Best Practice Manual for Digital Image Authentication

ENFSI-BPM-DI-02

DRAFT OF 16/04/2021 (FOR PUBLIC REVIEW)

ENFSI's position on Best Practice Manuals

ENFSI wishes to promote the improvement of mutual trust by encouraging forensic harmonisation through the development and use of Best Practice Manuals.
Furthermore, ENFSI encourages sharing Best Practice Manuals with the whole Forensic Science Community which also includes non ENFSI Members.
Visit www.enfsi.eu/documents/bylaws for more information. It includes the ENFSI policy document Policy on Creation of Best Practice Manuals within ENFSI (code: QCC-BPM-001).

BEST PRACTICE MANUAL FOR DIGITAL IMAGE AUTHENTICATION

DOCUMENT TYPE:	REF. CODE:	ISSUE NO:	ISSUE DATE:
BPM	**BPM-DI-003**	**001**	**16.04.2021**

CONTENTS

1. AIMS

This Best Practice Manual (BPM) aims to provide a framework for procedures, quality principles, training processes and approaches to the forensic examination. This BPM can be used by Member laboratories of the European Network of Forensic Science Institutes (ENFSI) and other forensic science laboratories to establish and maintain working practices in the field of forensic Image Authentication (IA) that will: deliver reliable results, maximize the quality of the information obtained and produce robust evidence. The use of consistent methodology and the production of more comparable results will facilitate interchange of data between laboratories.

The term BPM is used to reflect the scientifically accepted practices at the time of writing. The term BPM does not imply that the practices laid out in this manual are the only good practices to be used in the forensic field. In this series of ENFSI Practice Manuals the term BPM has been maintained for reasons of continuity and recognition.

2. SCOPE

This document addresses the forensic process for authentication of digital image files, i.e., assessing the extent to which supplied questions and claims concerning the genesis and life-cycle (provenance) of digital image data can be supported or answered. Therefore, this BPM deals with: context analysis, source analysis, integrity analysis, processing analysis and local manipulation detection, both through algorithmic methods or visual inspection. It covers the entire forensic process, from digital image file seizure to the presentation of evidence in court, and encompasses the specific aspects related to resources, validation, methodology, quality assurance, etc.

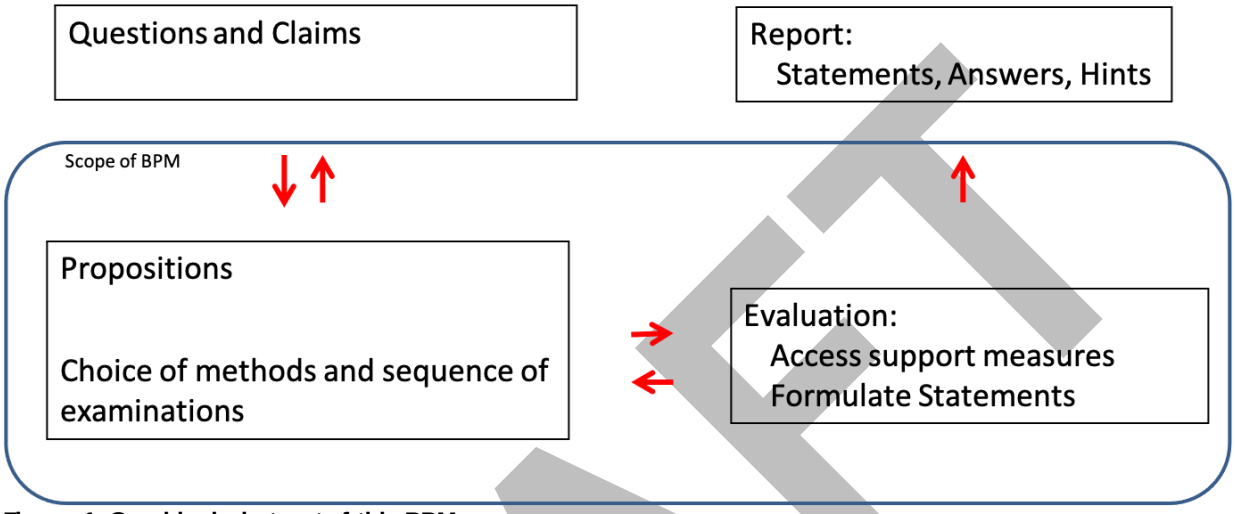

Figure 1. Graphical abstract of this BPM.

As indicated in Figure 1 this document describes:

1. The formulation of useful propositions from both the claims of the defendant and the questions supplied by the Customer (usually a judge, prosecutor, or police officer, and also private persons, where the jurisdiction allows it)
2. The wide selection of methods which one may use to evaluate each proposition, the principles of how to choose between them, and the sequence in which they should be applied.
3. The conflation of the results of each of these methods to evaluate the level of either support or rejection of the formulated propositions.

This BPM is aimed at experts in the field and assumes prior basic knowledge of digital image acquisition, processing and coding. It is not a standard operating procedure (SOP) and addresses the requirements of the judicial systems in general terms only.

This BPM focusses on:

- The technical aspects of digital image authentication.
- Passive image forensics techniques.
- Traditional sensor and camera technologies (consumer cameras, smartphones, CCTV systems, document scanners, etc.).

This BPM does not cover:

- Analysis relating to submitted video or moving image files.
- Active image forensics (digital watermarking, signature of block chain methods, etc.).
- General digital data authentication through digital signaturing.
- Methods related to investigation issues.
- Details of implementation of methods.
- Methods for determining whether a picture is the product of staging.

The effects of the following actions are mentioned but not described comprehensively in this BPM:

- Extraction of digital image data from other digital files like documents, presentations or data base files.
- Restoration of digital image files from e.g., unallocated space files.
- Device internal processing.
- Detection of artefacts that relate to an analogue source (e.g., photographic film, printed documents).
- Computer generation of images (generative neural network images, synthetised images, etc.).

3. DEFINITIONS AND TERMS

For the purposes of this Best Practice Manual (BPM), the relevant terms and definitions given in ENFSI documents, the ILAC G19 "Modules in Forensic science Process" (ILAC-G19:08/2014, 2014), as in standards like ISO 9000 (9000:2015, ISO), ISO 17020 (17020:2012, EN ISO/IEC) and ISO 17025 (17025:2017, EN ISO/IEC) apply.

The following definitions and terms have been used throughout this document:

Terms	Definitions
Active image forensics	Techniques making use of watermarking and digital signatures which have been included in a file for the purposes of authentication.
(Image) authentication	Assessing the extent to which supplied questions and claims concerning the genesis and life-cycle (provenance) of digital image data can be supported or answered.
Auxiliary data	The file system information of the file, any other external information about the image file and any data contained in the image file beside the pixel data.
Case Leader	Examiner who selects and prioritizes the tasks, assigns each task to one or more appropriate Examiners, and finally collects and interprets results before presenting them in court.
Chain of custody	A documentation that records the sequence of custody, control, transfer, analysis, and handing over, or destroying of items (physical or electronic data).
(Image) cloning	An image manipulation technique which consists in pasting a group of pixels coming from the same image into the image itself. This technique is also known as "copy-move attack" or "copy-paste attack".
Context analysis	The process of verifying that the context in which the image is placed is consistent and coherent with the image itself.
(Image) context data	The manifold/multiform information surrounding the questioned image, such as: the storage media, a webpage where the image was found, other images that are somehow related to the questioned image, etc.
Counter forensics	Techniques aiming to hinder the forensic analysis, by erasing or concealing traces left by some prior processing.
Customer	Person or organisation requesting an Image Authentication examination to be undertaken, and the beneficiary of the forensic report.
Deep learning	A machine learning approach based on artificial neural networks with several hidden layers (hence the word "deep").
Discriminating power	The discriminating power of an elementary methods relates to its ability to correctly separate elements based on some defined criterion.
Elementary method	A specific Image Authentication algorithm or technique for detecting traces left in the image pixels or metadata by some kind of processing. An elementary method is typically presented and described in details in a scientific publication.
Examiner	Person(s) undertaking the image authentication examination(s).
(Device) exemplar	A specific, unique instance of a device (typically identified by a serial number).
File format	The structure by which data is organised in a file.

File system information	Information about a file such as filename and extension, file path (directory path), MAC temporal information, security/access related information, versioning information.
Findings	Results of observations, measurements and classifications that are made on items of interest. They can be qualitative or quantitative. No result is also a finding.
Firmware	Software installed on an electronical device by the manufacturer that is essential for the basic functioning of the device.
Forensic Image	A bitstream duplicate of data contained on a device. An accurate reproduction of information contained on a device (physical or logical).
Global Analysis	Covering algorithmic methods that aim at unveiling traces of processing applied to the image during its lifecycle.
Hash value	The output string produced by a hashing function, that is, a function that maps an arbitrarily large digital input to a fixed-length (typically short) representation of it. It is commonly used as a means for verification that the input data has not changed from the point in time that the hash was first calculated.
Heat Map	A 2D false-colour representation of magnitude values, obtained by associating magnitude values to colours through a look-up table. Heat maps are often used to present the results of local image analysis methods.
Hex viewer	Tool to display binary data in hexadecimal format, is able to show arbitrary byte sequences, independent of their normal meaning/function.
Image file	Portrays a visual depiction of a scene and has additional ancillary data, not to be confused with a Forensic Image.
Integrity analysis	The process of examining for the presence (or absence) of traces that can be due to possible file modifications after the acquisition.
Likelihood ratio	A likelihood ratio is a measure of the relative strength of support that particular findings give to one proposition against a stated alternative.
Local Analysis	Covering algorithmic methods that aim at locating manipulated areas within the pixel data of the questioned image.
Local manipulation detection	The task of locating manipulated areas within a questioned image. By “manipulated area”, it is meant any region of the image that underwent some processing operation that was not applied to the rest of the image.
Lossy compression	A data compression technique which trades original image details for reduced storage memory. Examples of lossy image formats using compression algorithms are JPEG and HEIC (unless configured to work in a lossless fashion).
Method	A class of Image Authentication techniques for analysing traces left in the image pixels or metadata by some kind of processing. Examples include methods for “JPEG compression analysis”, “Shadow analysis”, “PRNU analysis”, etc. For each method, several specific analysis algorithms/techniques may be available, which are referred to as Elementary methods in this document.
(Image) metadata	Image metadata in this document includes file format (e.g., JPEG, BMP), image file internal metadata (e.g., Exif) and image decoding parameters.
Original image	An image whose integrity is preserved since its creation.
Passive image forensics	Techniques making use of metadata and digital artefacts which have not been intentionally included in a file for the purposes of authentication.

99

Pixel level analysis	Includes technical visual inspection (e.g., shadows, perspective, geometry, discontinuities) and techniques based on global features (e.g., compression level analysis, PRNU analysis) and local features (e.g., correlation map, clone detection).
Processing analysis	The process of examining for the presence (or absence) of traces that can be due to possible global or local modifications of the visual content of the image.
Propositions	Statements that are either true or false, and that can be affirmed or denied (Anderson (Anderson, Schuman, & Twining, 2005)). Propositions should be formulated in pairs (e.g., views put forward by the parties to the cases) and against a background of information and assumptions.
(Image) provenance	The life cycle and genesis of image data.
Quantization	A mathematical process, commonly used as part of compression algorithms, which maps a given set of input values to another discrete set of output values. Typically, this will result in loss of numerical accuracy due to rounding errors.
Questioned device(s)	See 'Questioned items(s)'.
Questioned image(s)	See 'Questioned items(s)'.
Questioned item(s)	All item(s) for which the customer has requested an image authentication examination. Questioned items could be digital images or devices, but does not include submitted Reference items.
RAW	Raw image files contain data from the image sensor which has typically undergone less processing operations (e.g., no CFA demoisacking, no lossy compression) than standard image files such as JPEG, HEIF, BMP.
Reference item(s)	All items that have been created or submitted so as to help the authenticity examination. Reference items could be digital images or devices.
Rolling shutter effect	An image distortion caused by its formation happening in a row/column-wise fashion and not being instantaneous - hence successive scanned lines capture the scene at different moments in time. This will only affect moving elements within the image, even when caused by a non-static camera. This effect is typical of CMOS imaging sensors.
Source analysis	The process of classifying, identifying, or verifying the source device.
(Image) splicing	An image manipulation technique which consists in pasting into a ("host") image a group of pixels coming from another ("alien") image.
Submitted item(s)	Questioned and reference item(s) provided for the examination.
Submitting party	Person(s) or organisation responsible for the delivery of the item(s) to the forensic laboratory.
Third Party	Person who acts as the interface between the customer and the Examiner(s) and therefore is able to review and redact any information supplied by the customer which could bias the Examiner.
Unallocated space	Areas of a storage medium that are not currently associated to any logical file or actively available data structure.
ZIP	File extension for files compressed with the *PKzip* algorithm.

100

101 The following abbreviations have been used throughout this document:
102

Abbreviations	Expanded phrase
BMP	Bitmap Image File
BPM	Best Practice Manual
BRISK	Block Regional Interpolation Scheme for K-Space (algorithm)
CCTV	Closed-Circuit Television
CE(s)	Collaborative Exercise(s)
CFA	Colour Filter Array
CMOS	Complementary Metal Oxide Semiconductor
DCT	Discrete Cosine Transform
DIWG	Digital Imaging Working Group
DNA	Deoxyribo-Nucleic Acid
ENFSI	European Network of Forensic Science Institutes
EWG(s)	Expert Working Groups(s)
Exif	Exchangeable image file format
FITWG	Forensic IT Working Group
FPN	Fixed Pattern Noise
GPS	Global Positioning System
HDR	High Dynamic Range
HEIC	High Efficiency Image Coding
HEIF	High Efficiency Image File Format
IA	Image Authentication
ILAC	International Laboratory Accreditation Cooperation
ISO	International Organisation for Standardization
IT	Information Technologies
JFIF	JPEG File Interchange Format (see also JPEG)
JPEG	Joint Photographic Expert Group
LR	Likelihood Ratio
MAC	File date/time values for Modified, Accessed, and Created, respectively
NTFS	New Technology File System
OS	Operating System
PC	Personal Computer
PNG	Portable Network Graphics
PRNU	Photo Response Non-Uniformity
PT(s)	Proficiency Test(s)
QCC	Quality and Competence Committee (ENFSI)
SIFT	Scale-Invariant Feature Transform
SOP	Standard Operating Procedure
SURF	Speeded Up Robust Features
TIFF	Tagged Image File Format
XMP	Extensible Metadata Platform (Adobe proprietary format)

103
104

4. RESOURCES

4.1 Personnel

All personnel participating in an image authentication examination should be proven to be qualified to perform the examination. At each organisation, the local quality management system should clearly describe how such proof can or should be provided and documented. The periodicity with which this proof and documentation should be re-assessed and re-evaluated should also be described.

The level of knowledge and experience the personnel should have depends on the possible role the person has within the examination: Third Party, Case Leader or Examiner (required knowledge/experience defined below). In relatively simple cases a single person may perform all three roles, but as the complexity of the case increases, multiple persons may be needed to separate these three distinct roles. Multiple Examiners may also be required, due to either time constraints, or because a single individual may not possess competency in all the required methods.

The Third Party should be able to translate the customers investigation questions into competing propositions, and collect information about constraints and available resources from the customer.

The Case Leader should select and prioritize the tasks, assign each task to one or more appropriate Examiners, and finally collect and interpret results before presenting them in court. They must also have a technical understanding of all methods covered in their report.

Each Examiner, as a minimum, should be able to demonstrate a competence in:

- How images are created.
- How artificial images can be created from original image source(s).
- Image processing theory.
- Advanced technical understanding in the authentication methods used in their examination.

and up to date knowledge and experience in:

- Application of legal basics of the jurisdiction and established quality management rules of the organisation.
- Practical use of the organisation's IT environment.

4.2 Equipment

In order to be able to demonstrate reliable and repeatable casework performance, all relevant IT hardware, and software used in image authentication examinations should be set up in a well-defined and documented state.

The most important pieces of equipment that should be considered are:

- Computer hardware and software.
- Storage and archiving system.
- Graphical output devices like displays.

To be able to perform an authenticity examination, the following categories of software tools can be considered (see Section 5):

- Tools for performing image file structure analysis.
- Tools for performing embedded metadata analysis.
- Tools for viewing the content of image files.
- Tools for performing global analysis of the imagery.
- Tools for performing local analysis of the imagery.

It should be considered that performance and capabilities of tools can largely vary across different versions. The Examiner should be aware of the possible limitations that may incur by using an outdated tool.

Many tools can only be used safely for image authentication purposes in a strictly controlled manner. Standard operating procedures (SOPs) and validation reports (see Section 6) should give guidance on which software or elementary methods that should be used to realise a specific function on given source data.

4.3 Reference materials

A typical image authentication method extracts or computes features (single values, statistics, images, etc.) from the image to be examined. Hence, for some kind of examinations, suitable reference images should be used to compare and evaluate the obtained case results with those obtained for the reference materials. Such reference material can be either collected from publicly available and suitably documented datasets, or created for the specific examination (see Section 11).

4.4 Accommodation and environmental conditions

The general rules for IT laboratories should be applied; see ENFSI-BPM-FIT-01 (ENFSI-BPM-FIT-01 , 2015, version 01).

Special consideration should be given to:

- Lighting conditions (e.g., positions of building windows and artificial light sources vs. computer screens, etc.) when carrying out visual inspection related examinations, or visually interpreting 'heat maps' generated by tools.
- Confidentiality of displayed content (passers-by: positioning of displays and desks with the aim of preventing biassing issues if multiple Examiners are to be forming independent opinions).

4.5 Materials and Reagents

There are no specific technical specifications for image authentication materials; the general rules for digital evidence apply according to ENFSI-BPM-FIT-01 (ENFSI-BPM-FIT-01 , 2015, version 01).

Reagents are not used in image authentication.

5. METHODS

This section provides guidance on technical methods, strategy and peer review for handling different aspects related to passive image authentication (see Figure 2). This section presents four areas of analysis:

- **Auxiliary Data Analysis:** describing methods based on auxiliary data (all data except the pixel data of an image).
- **Image Content Analysis:** describing methods based on the image content (pixel data).
- **Strategy:** providing guidance on how to use these methods to perform typical authentication tasks.
- **Peer Review:** describing the application of peer review in an authentication process.

In this BPM general methods are described. For information about elementary methods, it is recommended to refer to their original papers and related successive literature. In the survey paper by P. Korus (Korus, 2017) and in the book by H. Farid (Farid, 2019), many of the methods mentioned in this BPM are discussed, also referencing to several elementary methods.

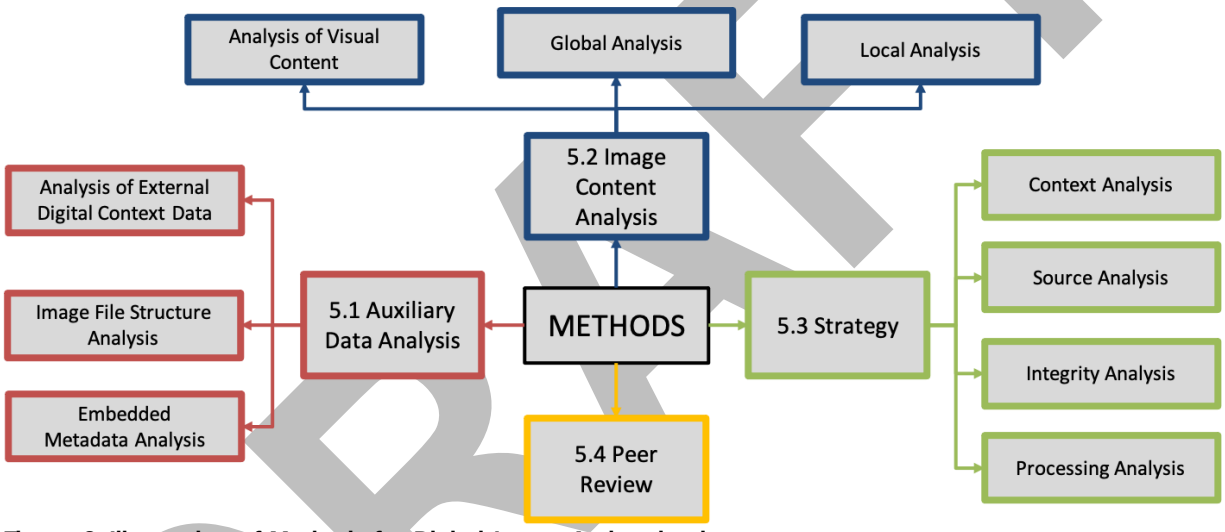

Figure 2. Illustration of Methods for Digital Image Authentication.

5.1 Auxiliary Data Analysis

The goal of this sub-section is to provide methods for analysis of auxiliary data (see Figure 3). These methods can be used for verification or comparison purposes within an image authentication examination. This sub-section presents the analysis of three different types of auxiliary data:

- **Analysis of External Digital Context Data:** auxiliary data related to the file, e.g., coming from the file system, other storage, or processing related data context.
- **Image File Structure Analysis:** auxiliary data that describes how the content of the file is organized.
- **Embedded Metadata Analysis:** auxiliary data describing the image, for example image width and height, quantization tables, Exif and XMP data, and additional data such as preview images.

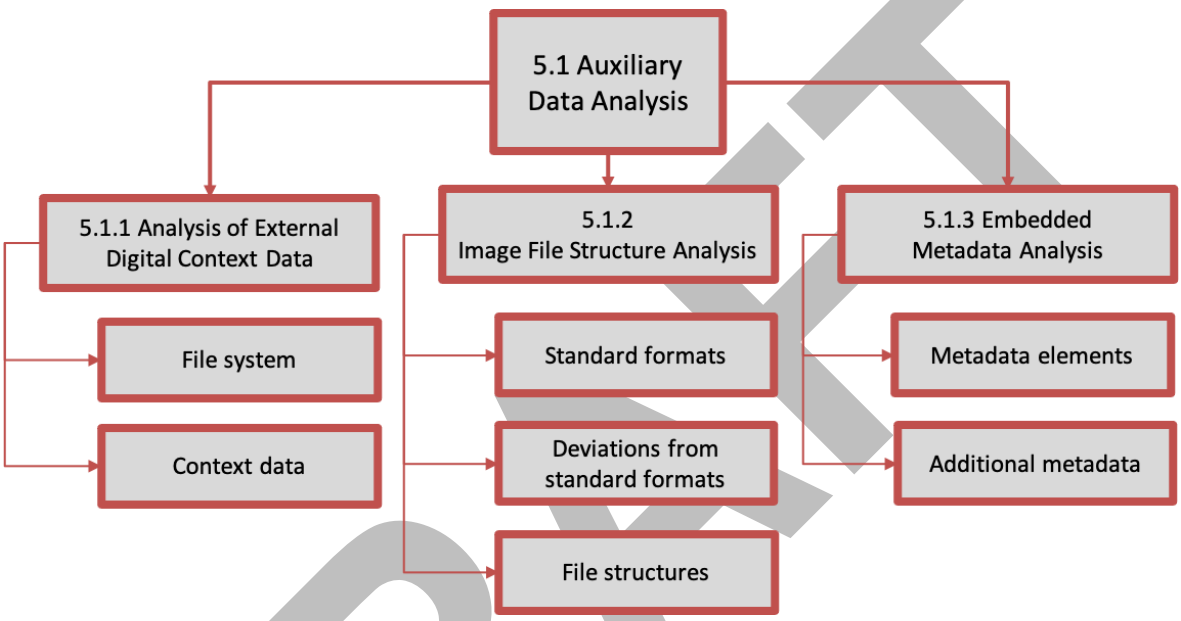

Figure 3. Illustration of Auxiliary Data Analysis methods for Digital Image Authentication.

5.1.1 Analysis of External Digital Context Data

If a questioned image file is submitted embedded within or alongside an evidence storage or processing container or context, this digital evidence context can be considered for more detailed analysis. If such a physical and/or digital evidence context is not readily available, an Examiner should consider if such context could possibly still be obtained from the Customer; see Section 9.

5.1.1.1 Standard file system metadata

Questioned image files often originate from a file system found on a submitted digital storage device. Examining the file system on this device may be important as it normally contains some standard information about the stored files which can be used for verification or comparison purposes within an image authentication examination. Examples are:

- Location in the directory structure
  The Location of a file on a file system path can give information about who or how a file was created. In particular it may be important to understand which software/app was used to create/resave/receive the file.
- Filename
  A filename can give an indication if a file has been created (sent or received) by a specific app/software and about date and time of creation. For example, "IMG_20210101_11-55.JPG" may belong to a picture taken at Jan. 1st 2021, or,

"DSC_00234.JPG" may be the name of image number 234 taken by a camera (since its last power/factory defaults reset or storage area (re)formatting).

- MAC (modified, accessed, created) date/time values.
  Date/time values can be used to position an image in a presumed timeline, and/or, to compare it to similar temporal metadata embedded within the imagery (e.g., Exif); see Section 5.1.3. File size; this information may give a first hint about manipulation if outside the expected range.
- File system feature flags (e.g., access restrictions should be similar for files in a sequence).

It should be noted that some of these values may be (inadvertently) changed by a normal user-copy or -extraction operation, so it may be important to understand or investigate, whether any provided questioned image data is/was obtained in a forensically sound way, i.e., whether the original storage and/or processing meta-data was accurately preserved or not. Moreover, it should be considered that date/time values normally depend on the system clock, whose reliability is often unknown.

More details about handling digital data can be found in Section 8.

5.1.1.2 Other storage or processing related context data

Besides traditional file system-based storage, other types of *direct* relationships between a questioned image file and its digital context may exist. For example, this relationship may be of a hierarchical nature (parent sibling like) when a questioned image has been submitted as part of an email message. Similarly, a questioned image may be submitted as part of a larger digital archive (e.g., a ZIP archive). In this case the email headers or archive metadata may contain relevant temporal or other metadata that may yield valuable information, or that can be compared with embedded metadata or other available auxiliary data; see Section 5.1.3.

When sufficient additional digital storage or processing context for a questioned image is available, other type of *indirect* checks can be carried out as well. Typical examples of such checks are:

- Searching for, and reviewing identical or related imagery: Look for an identical image, a less processed version (which may be the original version) of the questioned image, another image giving information about the content of the questioned image, an image from a known source which contains the same camera ID (make/model) as that of the questioned source image, an image taken at the same time with the same camera.
- Looking for image processing software which might have been used to process the image and for traces of such a processing, e.g., log files, vestiges in associated temporary storage directories.
- Searching for entries in "recent" lists.
- Reviewing of internet browser caches.
- Reviewing of operating system caches, i.e., image thumbnails or preview imagery data may be available.
- Searching for old, invalidated directory entries to find traces of former locations of a file.
- Searching for extra information the file system may provide for a file which is normally not readily available to the user (e.g., NTFS index directory entries).
- Check consistency of file system block/cluster usage (no older file should have overwritten the content of a newer one).
- Searching for identical or possibly related file fragments by carving in free space.

If the locally available data provides hints to use of possibly relevant internet resources (e.g., online storage, backup or synchronisation services), the range of the search may also be extended in this direction, upon consultation with the customer.

A fully detailed analysis of each of the methods outlined above falls outside of the scope of this BPM. Additional guidance on the use of advanced digital forensic methods can be found in ENFSI guideline for evaluative reporting in forensic science (Willis, 2015).

5.1.2 Image File Structure Analysis

Most image files are structured according to a standard format. Examples of standard formats are:

- JFIF (JPEG File Interchange Format).
- TIFF (Tagged Image File Format).
- BMP (Microsoft Windows Bitmap).
- PNG (Portable Network Graphics).
- HEIF (High Efficiency Image File Format).

The structure of an image file is characterized by the number, type, sequence and size of the components (either required or optional). This delivers a lot of possibilities to compare the questioned image with other image files. Most standard formats provide a considerable number of compliant image file constructions that upon decoding may yield exactly identical image pixel data, even if only common choices for the variables of the standards are used. Many standards describe only the structural elements that could or should be present ("what"), however the standards do not describe in which order they must be encoded, nor how the encoding should be implemented ("how"). In principle this provides a good basis for methods trying to get information about processing history by using file structure analysis.

In practice however, the use of very popular and widespread code libraries leads to a reduced diversity in the image files created (default settings will provide a default structure). In the case that deviations with respect to such default structures are found; this would provide increased support to discriminate the software/device used.

The Examiner should take the following into account:

- For any file received, one should consider the version of the format which the file may be conforming to; e.g., one tool may produce a certain format version, another tool (for the same data) may produce another format version.
- Deviations from a specific image standard format (use of required or optional components) or the file structure (ordering of components) does not necessarily equate to the image having been tampered with, in fact this may provide an extra source of information for the purposes of authentication if the intermediate software is known. For example: a PNG file may contain so-called PNG chunks from Apple devices which do not conform to a strict interpretation of the PNG standard.
- Image processing tools normally do not try to preserve the structure of image files when saved by the tool after processing (or even simply load, display and resave, without any explicit changes), they use their own preferred format and structure. Even if the same file format is used the details of file structure may differ significantly. There are different policies for handling optional components in image files loaded for processing, they often can be governed to some extent by the options of the tools. Preservation of unknown/not interpreted components or modification of file structure may lead to inconsistencies in the resulting image file, e.g., if an APP1 field of a JPEG stream holding XMP (Extensible Metadata Platform, Adobe) data still contains descriptors to point to preview images which are no longer present or start at another offset.
- Tools exist which facilitate parsing and comparison of file structures. These are generally easier to use than analysis within a simple binary file or so-called "hex" viewer. A hex viewer is still useful as a trusted tool source as it permits access to the raw data, and permits checking of any interpretations made by other tools.

5.1.3 Embedded Metadata Analysis

Metadata of an image file can describe permanent and variable parameters of the imaging device. Some metadata is required for decoding and displaying the image while other metadata is not. An overview is provided in Table 1.

Table 1. Embedded metadata.

Metadata	Permanent	Variable
Mandatory	Pixel format	Resolution, Decoding parameters
Optional	Device make, Device model, ID/serial number	Date/time, GPS coordinates, Exposure settings, User comments, Position/direction of device, Software version, Technical parameters of optics, Picture mode

Some metadata fields may also depend on an initialization by the user, e.g., the owner's name or device internal date/time.

All aspects of metadata storage can be of interest for comparison purposes: not only a value itself, but also where it is stored in the file (order and offset) and the form of representation by which it is stored in the file (e.g., little or big endian and number of bytes allocated to the value). Deployment of multiple tools might be necessary to explore the full range of information, e.g., a high-level tool like an Exif parser to show the interpreted names and values of all metadata items and a low-level tool like a hex viewer to check the details of coding and storage. A lot of metadata items are stored in standardized structures and therefore are easy to handle, but also to manipulate, without causing inconsistencies, and therefore without leaving any obvious traces.

Hence, the evidential value of metadata analysis findings may not be strong for some questions. A special case (as they are not documented in any specifications) are proprietary elements like the so called “maker notes”: they often show an (at least in parts) unknown structure, coding and meaning, which makes comparison more difficult.

Aside from the primary image – modern devices like mobile phones may store within the file, additional associated proprietary data coding segments for:

- thumbnail and preview images,
- short video to illustrate the temporal evolution of the scene at shot time,
- depth of elements of the scene (e.g., with respect to 3D presentation),
- identifying areas of the image where faces are detected.

These may provide additional avenues for comparison against the primary image and reference image files for consistencies/inconsistencies.

Authenticity of metadata and image data in an image file may be different: image data may be altered without touching metadata and vice versa.

All image processing tools have to read and write the indispensable parts of metadata, but the handling of additional metadata is very divergent. There are different policies for handling metadata in image files loaded for processing and written as a resulting image file. They often can be governed to some extent by the options of the tools. Unknown metadata elements are often copied without any changes or omitted by the tools, known metadata elements may be used and modified. Metadata elements added by (a version of) an image processing tool can be quite distinctive (e.g., the quantization tables used by Adobe Photoshop). Metadata elements may also contain even more specific data, connecting the image file to external files (for example log files of an image processing software), which can be used e.g., for a search on a PC of a suspect.

5.2 Image Content Analysis

The goal of this sub-section is to provide methods that can be used for image content analysis (see Figure 3). Findings from these methods can be observations, measurements and classifications. This sub-section presents three areas of analysis:

- **Analysis of Visual content:** covering the analysis of features in a questioned image a human observer can perceive.
- **Global Analysis:** covering algorithmic methods that aim at unveiling traces of processing applied to the image during its lifecycle.
- **Local Analysis:** covering algorithmic methods that aim at locating manipulated areas within the pixel data of the questioned image.

These analyses can be performed independently from each other; however, some methods are more logical to apply before others. Usually, a local analysis must be conducted after global analysis in order to reveal the areas affected by manipulation. Some overlap may be observed between global and local analysis method names, because the features examined during global analysis may also be useful for local analysis.

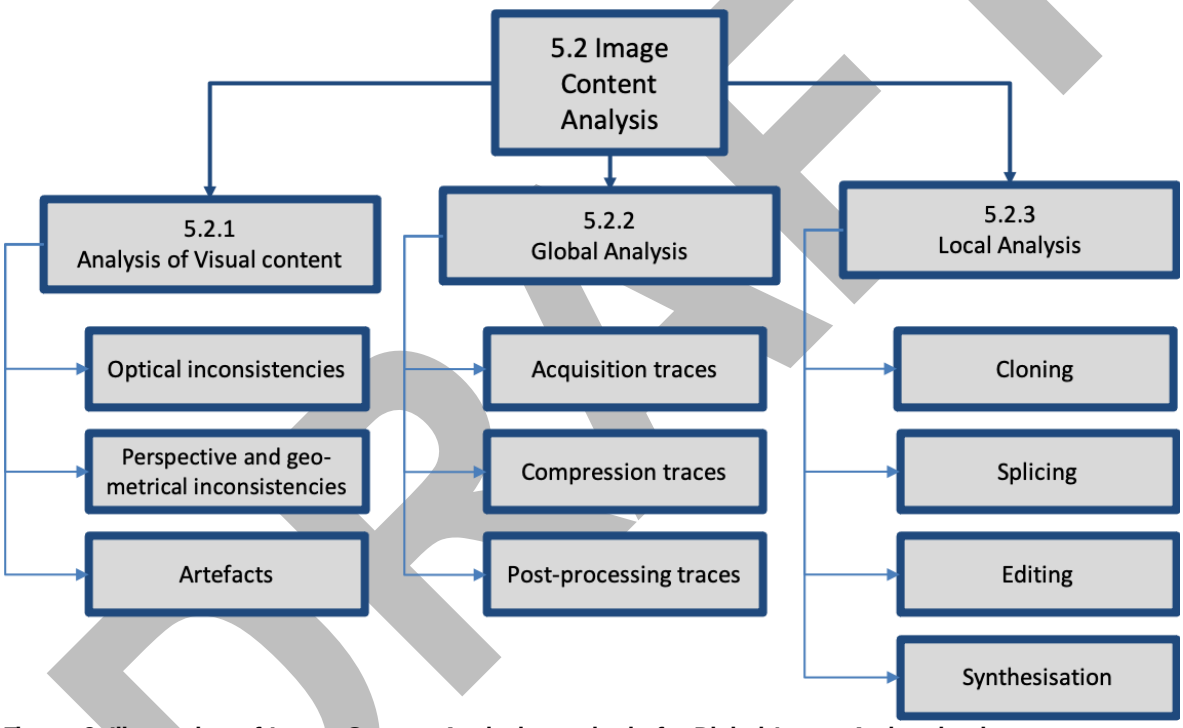

Figure 3. Illustration of Image Content Analysis methods for Digital Image Authentication.

5.2.1 Analysis of Visual Content

The intention of methods for detecting visual features is to check, whether the content of the image can be a capture of a real scene. Captures of a real scene must be consistent with physical constraints like size of rigid objects and the rules of optics and geometry. Information about the scene and the objects in the scene can be extracted from the image and compared with general knowledge, the results from other images and/or the results of 3D simulations. The provided list of methods is not exhaustive.

5.2.1.1 Optical inconsistencies

Different optical inconsistencies can be present in an image due to shadows, the presence of transparent objects, the presence of reflecting objects, and blurring. These inconsistencies are discussed below.

Shadows are dark areas cast upon a surface by a body intercepting the rays from a source of light. The following aspects of a shadow can be inspected: its direction, its shape/length and its contrast (hard- or soft-edged). To check the direction, shape and length of a shadow, the position of the light source(s) relative to the object must be known. In case of outdoor scenes, the Sun might be the dominant light source and if the time of recording is claimed or known, tools such as http://www.suncalc.org/ can be used to determine the position of the Sun and thus the direction and possibly the length of the shadow which then can be compared with the image under investigation. For indoor scenes, the position of light sources needs to be known. Checking the direction, shape and length can be done roughly from the image itself or more precisely by making reference recordings at the location of the recording. The edge of the shadow might be hard-edged or soft-edged. This depends on the used light source and/or weather conditions (cloudy versus bright sky). Other remarks with respect to shadow-analysis:

- If during a reference recording the shadow cannot be *exactly* reproduced, this does not automatically imply that the image is not authentic. The exact shape of a shadow depends on many factors and the exact reconstruction of shadows might be difficult.
- The direction of shadows of different objects do not need to be parallel, since the light source might be located in the neighbourhood of the different objects.

When a **transparent object**, for example a window, is part of the claimed manipulation, it is of interest to see if the information that is visible through the transparent medium (the background) is consistent with what is known or expected. The Examiner should take into account that the transparent medium could or should have deformed the view of the background scene. Reference recordings might be needed to verify the consistency of the background as seen through the transparent object.

When a **reflective object**, for example a mirror, is part of the claimed manipulation, it is of interest to see if the information that is viewable through the reflection is consistent with the rest of the scene. Of course, the Examiner must take into account that the reflective surface might not be flat, and thus that the scene seen through the reflection might be strongly deformed. Reference recordings might be needed to verify the consistency of the reflection.

The sharpness of objects in a photo depends (amongst other parameters) on the focal settings of the camera (e.g., focal distance and focal depth), the resolution of the image sensor and on the motion of the item itself. The Examiner could search for inconsistencies in the perceived sharpness but should take the following into consideration:

- Static objects at the same distance should have the same perceived sharpness. If not, this could be an indication for splicing. This can occur when the spliced images were of different resolutions.
- With the development of multi-lens cameras and software artificially blurring backgrounds, inconsistencies in the sharpness might not be caused by manipulations.
- Bluriness of a single object is also possible in the case of motion blur. i.e., when the object was moving during the exposure. The blur direction should be the same as the motion direction.
- Local blur is also possible when the lens is unclean (for example the presence of rain drops) or damaged (scratches). This local blur should be visible in other images taken with the same camera and lens around the same time period.
- If the camera was moving during the exposure, the complete scene might be blurred. The amount of blurring can differ for different regions of the image.

It should be noted that so-called *image re-lighting* advanced approaches exist, that allow insertion or removal of 3D objects in a scene. However, as indicated above, physical object properties can still be analysed for their possible visual or physical/geometrical inconsistency (e.g., transparency, reflective or light-diffusing object properties).

Other visual traces, object or scene properties may exist that also can be used to detect inconsistencies due to deep fake, computer graphics or computationally synthesised images.

5.2.1.2 Perspective and geometrical inconsistencies

Different perspective and geometrical inconsistencies can be present in an image as vanishing points, photogrammetry, etc. These inconsistencies are discussed below.

Vanishing point is the point at which receding parallel lines viewed in perspective appear to converge. The main principle behind perspective is that parallel lines, that is, lines that are parallel in all three dimensions, will have the same vanishing point in non-deformed images. In general, vanishing points do not have to be on the horizon of the image and more than one vanishing point can be present in an image.

If a perspective analysis shows that a group of parallel lines do not have the same vanishing point this could be an indication for manipulation. When applying the perspective method, it is crucial that the Examiner should also take into account the following considerations:

- The perspective line principle can only be used if it is known that the lines are truly parallel in the real world. In images of natural scenes, this might be difficult to estimate especially when the image content shows moving objects recorded under uncontrolled circumstances.
- The appearance of elements of the image may not be perfect. Lines that are parallel in the real world could be (strongly) deformed in the image. Effects that can introduce these deformations are:
    - Lens distortion.
    - Intermediate transparent and reflective objects between object and camera such as windows, screens or mirrors.
    - The Rolling Shutter Effect.
    - Interlacing.
    - Compression artefacts.

These deformations can make it more difficult or even impossible to determine the correct position of a vanishing point. The determination of the vanishing point is very sensitive to fluctuations in the provided input (e.g., due to the selection of line segments by a user). This estimation is even more difficult when the line segment is barely visible due to limited resolution, motion blur, bad lighting conditions, or compression artefacts. The error made in the position of the vanishing point strongly depends on such estimations especially when the lines are short and located close to each other. From the above given considerations, it follows that there exist a great number of possible explanations for an apparent inconsistency in the position of a vanishing point besides the fact that the image has been manipulated.

Photogrammetry allows determination of the position of the camera which captured the questioned image, and measurements of the environment, objects and persons depicted in the image content. In order to verify that a questioned image is a genuine recording of the scene, various analyses can be performed. For instance:

- Using a single image (reverse projection) or multiple images (multi-image photogrammetry) from a scene with objects of known shape and dimensions, their relative positions, shape and sizes on the image can be measured and checked for consistency.
- The measured positions/photographs of the scene may highlight possible discrepancies with the scene configuration or expected recording conditions.

Photogrammetry adjustment algorithms are sensitive to various sources of errors, such as the camera parameters (focal length, distortions, etc.), the placement of:

- image points by the Examiner.
- 3D points on objects whose position changes between different images.
- reference measurements which define the scale of the model.

In the assessment of their results, the Examiner should consider the expected sources of errors and the errors coming from image transformations or content manipulations. Even if images come from an unknown source or show obvious signs of manipulation, the geometrical analysis can yield reliable information on the camera positions, lighting conditions, shadows' angles and length as well as the positions and sizes of elements of the subject. In this regard, it complements other analyses of the visual content described in this section.

5.2.1.3 Artefacts

Image artefacts are noticeable distortions in the image. These could be caused by the acquisition chain (e.g., optical distortion, optical blur, graininess), manipulations applied to the image, artefacts from the image synthesis (e.g., deep fakes) as well as by lossy compression (e.g., blocking, ringing, contouring) or corruption. A possible way to understand whether an artefact has arisen due to the normal image generation process (e.g., acquisition and compression) or due to some manipulation or corruption, one may check whether the artefact is similarly present in authentic reference images.

The Examiner should consider the following:

- At the edge of objects colour mixing may occur. If significantly more or less inconsistencies than expected are observed in these regions, this should be considered for evaluating propositions.
- Lines that are parallel in the real world could be deformed in the image based on compression artefacts (block artefacts).
- Objects that in the real world have a rounded form could be deformed in the image based on compression artifacts (block artefacts).

5.2.2 Global Analysis

Global analysis aims to unveil traces of processing applied to the image during its lifecycle; exploiting the fact that manipulations can leave traces within the processed image. Normally, global analysis methods provide a compact description, e.g., a single value, a plot, or some aggregated statistics, and has to be interpreted by the Examiner.

Global analysis is often helpful for steering further analyses at the local level (e.g., detecting traces of double JPEG compression at a global level may suggest to prioritize the use of JPEG-based methods for the local analysis).

In the following, we classify methods based on the kind of traces they leverage: acquisition traces, compression traces and post-processing (e.g., resize, cropping, level adjustments) traces.

- Manipulation detection based on image capture/acquisition traces:
  - **Chromatic Aberration Analysis**: Camera lenses are imperfect, and exhibit increasing degrees of chromatic aberration as you move from the centre to the edge of the lens. Global chromatic aberration analysis aims at detecting the presence of such artefact in the image, and possibly fit a mathematical model to the measured/detected artefact. E.g., a frequency plot of the average angular error can be computed. It should be noted that chromatic aberration traces are easily concealed by lossy compression.
  - **Photo Response Non-uniformity (PRNU) Analysis**: PRNU is the variation in the photo-response between the individual sensor pixels, which through research has been found to be stable over time. Given a set of suitable reference images, a camera sensor's PRNU pattern can be estimated. The correlation between the PRNU-pattern of the questioned image and the sensor's PRNU pattern can provide an indication on whether the questioned image was acquired with that sensor.
  - **Colour Filter Array (CFA) Analysis:** Most colour cameras use a colour filter array to capture different colours on different physical pixels, and the resulting mosaic images are then interpolated to obtain a full colour image. The arrangement of the colour filter array (e.g., Blue-Green-Green-Red), the interpolation algorithm, or the induced local correlation can be analysed, e.g., as a way to obtain information about properties of the originating device. It should be noted that traces left by demosaicking are not robust to lossy compression.
  - **Fixed Pattern Noise (FPN) Analysis**: As an effect of mass production of camera sensors, they may include defective pixels whose responses are noisy or fixed – irrespective of scene lighting – also called "dead" or "hot" pixels. This fixed pattern noise can be used to provide an indication of whether the questioned image was acquired with a particular sensor. Internal camera processing may attempt to conceal FPN, but such processing may in turn leave detectable traces. Besides that, the Examiner should be aware that the FPN of a sensor can change over time and is temperature dependent.
- Manipulation detection based on compression traces
  Compression analysis methods are an important asset in the toolbox of the Examiner. These methods aim to reveal traces of (possibly multiple) lossy compression steps applied to the image. It should be noted that the first compression step is often carried out inside the camera. Examples of algorithms based on this approach include:
  - **Discrete Cosine Transform (DCT) Analysis**: When compressing an image with the JPEG standard algorithm, the image is split into 8-by-8 blocks, and these blocks are transformed to the DCT domain. The obtained coefficients are then divided by the values of the quantization tables. This quantization step leaves statistical traces in the coefficients, which can be exploited to detect single or multiple compressions (e.g., by analysing the histograms of coefficients separately for each spatial frequency). It is to be noticed that

processing between the quantizations (e.g., cropping, resizing, levels adjustment) may complicate the analysis, calling for specialized/dedicated detection methods.
    - **JPEG Ghosts Analysis**: By computing the global difference between the questioned image and several recompressed versions of it, it may be possible to expose traces of previous compressions while simultaneously estimating the quality factor of such compressions.
    - **JPEG Dimples Analysis**: Some imaging devices which output JPEG images show a specific JPEG artefact, present in each JPEG compression block, called "dimple". They manifest themselves as a grid of slightly brighter or darker pixels, spaced by 8 pixels in each dimension. Presence of such artifact throughout the whole image can be used as a verification/consistency check that the questioned image is produced by an alleged model of source device (not at the unique device level). The image must be at the original scale (or restored to this scale) in order for JPEG dimples analysis to be applicable.
- Manipulation detection based on post-processing traces
  Beside the features involved in capturing the image, there are other global analyses which may be used in detecting image manipulations. For example:
    - **Histogram Analysis**: When a significant number of pixel values in an image are redistributed, for example by contrast enhancement, different input values may collapse onto the same output value, and leave other output values unused, which leads to statistical traces in the histogram of the image or some colour channels of it. It should be noted that such traces may be erased by further processing or even mild compression.
    - **Fourier Analysis**: When an image is modified and resaved, new periodic patterns might have been introduced. These patterns can be made visible in the output of a 2D Fourier Transform of the image. Typical modifications that might introduce periodic patterns are resizing, rotation and re-capture of a digital image. The latter case also includes manipulations through an analogue processing chain, such as by printing the image followed by scanning or by taking pictures of it from a display (monitor or projector screen). It should be noticed that peaks in the 2D Fourier spectrum could be due to presence of periodic elements in the visual content of the image (e.g., a grid, fence); moreover, when an image is strongly JPEG compressed, or is affected by the JPEG dimples artifact, this may also cause peaks in the 2D Fourier spectrum.
    - **Pixel Correlation Analysis**: Some image processing functions such as rotation (other than multiples of 90-degrees), resizing or even CFA-demosaicking and JPEG compression may introduce local correlation between neighbouring pixels throughout the whole image. Such local correlations may be well exposed through a statistical analysis, which may reveal the presence and even the parameters of the applied processing (e.g., estimate the resizing factor). It should be noted that correlations due to different causes may conceal or interfere with one another - the latter making detection harder but possibly even more informative.

5.2.3 Local Analysis

Local analysis aims at locating manipulated areas within a questioned image. Examples of local manipulation include:

- Image splicing.
- Image cloning.
- Editing a group of pixels to change their appearance (e.g., colour, sharpness), their size (e.g., by up- or down- scaling), or orientation (e.g., by rotating them).
- Synthesisation of pixels to edit or replace a region of the image (e.g., inpainting, content generation or adaptation with deep neural networks, or use of Computer Graphics methods).

5.2.3.1 Approaches to locate manipulated areas

The general idea exploited by elementary methods for local analysis is that localized manipulations may introduce inconsistencies or anomalies in pixels, for example:

- Manipulated pixels retain some (visual or statistical) property that is not retained in the rest of the image or, vice-versa, manipulated pixels lose some (visual or statistical) property that is retained in the rest of the image. Noticeable examples of methods based on this approach include:
  - **Local correlation analysis**: when a region of the image is rotated or scaled, affected pixels may retain strong correlation due to interpolation.
  - **Colour Filter Array demosaicking analysis**; when pixels are pasted from an alien image having traces of interpolation due to CFA demosaicking, the pasted pixels may have stronger local correlation than the rest of the image. On the contrary, there may be cases where the pasted pixels expose significantly lower local correlation compared to pixels of the host image.
  - **Blocking artifact analysis:** pixels from an alien image which are pasted may retain inconsistent blocking artifacts or compression noise than pixels in the rest of the host image.
  - **Local JPEG compression analysis** (e.g., JPEG Ghost Analysis and Error Level Analysis): when a JPEG image is tampered with locally and re-saved to any format, computing the difference between the final image and a re-compressed version of it could reveal which regions were not tampered with, so that manipulated regions stand out.
  - **Aligned and not-aligned double JPEG compression analysis:** when a JPEG image is tampered with locally and re-saved as JPEG, pixels in untouched regions may hold traces of double quantization, while manipulated pixels only hold traces of one quantization (due to the final JPEG compression).
  - **Chromatic aberration analysis:** when the alien image suffers from chromatic aberration, pasted pixels may retain an aberration pattern which does not fit into the global aberration model of the host image.
  - **Generical noise analysis:** pixels from the alien image may contain a different noise level (e.g., due to different ISO settings, different sensor quality, different compression quality, etc.) than pixels in the host image.
  - **PRNU local analysis:** manipulated pixels no longer retain the sensor noise pattern that characterizes the originating device.
  - **Local JPEG dimples analysis:** in images affected by the JPEG dimples artefact, the local absence of such an artefact may indicate that pixels have been manipulated in that region.
  - **Rich model analysis:** the different provenance of alien and host regions is sometimes reflected in subtle variations in pixels, which are well exposed in high-order image statistics.
  - **Machine learning-based analysis:** artefacts introduced by local manipulations can be detected or localised using trained machine learning models. It has to be noted that performance of this kind of analysis is usually influenced by the composition of the training dataset.

- In case of cloning, two (or more) regions of the image become identical or visually similar (net of geometrical transformations such as rotation, flipping, scaling). Noticeable examples of algorithms based on this approach include:
  - **Keypoint-based clone detection:** keypoints (e.g., SURF, SIFT, BRISK) are extracted from the image and their descriptors are compared to locate clusters of matches. A large cluster of matches may indicate that part of the image has been cloned. This kind of analysis is typically more robust to geometrical transformation of cloned pixels, but becomes less reliable when a flat object is cloned (e.g., the sky or a wall, which contain little or no keypoints).
  - **Block matching clone detection:** the image is divided in blocks and descriptors are computed for all blocks, then matching clusters of descriptors are searched for. A large cluster of matches may indicate that part of the image has been cloned. This kind of analysis is typically less robust to geometrical transformation but works even when the cloned region is flat.

It should be noted that some of the methods already presented in the Visual Inspection section may also be used to locate manipulations (e.g., analysis of blur inconsistency). They are not repeated here for conciseness.

5.2.3.2 Interpretation of the output produced by local analysis methods

Elementary methods for local analysis usually produce a digital image as output. The meaning of pixels in the output image strongly depends on the specific elementary method. In general, at least three different categories of methods can be identified based on the kind of output:

- Some methods produce a processed version of the input image, conceived to make possible inconsistencies more visible for the Examiner. Examples include computing a simple prediction error map from the questioned image pixels (as done by some algorithms for **Local correlation analysis**) or subtracting a recompressed version of the image from the input image (as done by the **Error Level Analysis** algorithm). Being essentially "raw data", this kind of output maps normally requires a higher level of interpretation by the Examiner.
- Some methods produce a forgery localization map, obtained through a statistical analysis of the image; this kind of map usually shows the probability/likelihood score with which each (region of) pixel(s) belong to the manipulated or non-manipulated statistical model, and are often presented in false-colours for better visibility. Examples in this category are methods for: **Aligned and non-aligned double JPEG compression analysis**, methods for detecting inconsistencies in **CFA demosaicking**, methods for measuring the local presence or absence of the expected sensor noise pattern (**PRNU Local Analysis**), and methods for **Local JPEG dimples analysis**.
- Some methods produce a clone detection map, where regions of the image that are classified as clones are visually linked (e.g., connected by lines or coloured in the same way). Normally, these methods do not classify which of the linked regions is the source or clone, calling for additional analysis via different means.

Given the wide variety presented above, it is impossible to define a general rule for the interpretation of the output maps produced by local analysis methods. However, the Examiner should consider that most forgery localization methods produce an output which measures/shows the local presence or absence of some trace in each image region, which does not directly imply a classification of that region as manipulated or non-manipulated.

For all local analysis methods, it is the Examiner's responsibility to interpret the meaning of presence/absence of some trace in a specific region, also considering the information obtained through different analyses (e.g., Global analysis). When interpreting the output of a local analysis method, the Examiner should be aware of the limitations and weaknesses of the method. Some noticeable examples are provided:

- Methods for PRNU local analysis are normally less reliable in dark and light-saturated regions.
- Methods based on statistical analysis of DCT coefficients, such as Aligned and non-aligned double JPEG compression, Blocking Artifacts, Error Level Analysis, and JPEG

Ghost are negatively affected by exceptionally uniform or textured regions as well as by black- and white- saturated regions.

- Strong JPEG compression applied after manipulation hinders the performance of most local analysis methods.
- Global up- or down-scaling negatively affects most methods for Aligned and non-aligned double JPEG compression analysis.

Local analysis tools are usually designed to reveal the presence of manipulated regions, and as such, they can only provide support towards the hypothesis of the image being locally manipulated. However, there are some cases where a local analysis tool can also provide support towards the hypothesis that the image is locally pristine. Noticeable examples of the latter category are:

- **PRNU local analysis**: detecting presence of the expected camera's sensor noise provides support to the hypothesis that pixels were not tampered with;
- **JPEG dimples analysis**: presence of aligned JPEG dimples artifact lends support to the hypothesis that pixels are not tampered with;
- **CFA demosaicking analysis:** local compatibility of pixels with the expected CFA interpolation filter provides support to the hypothesis that pixels were not tampered with.

5.3 Strategy

In the previous sub-sections, this BPM presented several technical methods for handling different aspects related to image authentication.

The goal of this sub-section is to provide a strategy for using the presented methods to address the propositions in a structured manner. Since different propositions may need different analysis workflows (see Figure 4), this sub-section presents four areas of analysis:

- **Context Analysis**: the process of verifying that the context in which the image is placed is consistent and coherent with the image itself.
- **Source Analysis**: the process of classifying, identifying, or verifying the source device.
- **Integrity Analysis**: the process of examining for the presence (or absence) of traces that can be due to possible file modifications after the acquisition.
- **Processing Analysis**: the process of examining for the presence (or absence) of traces that can be due to possible global or local modifications of the visual content of the image.

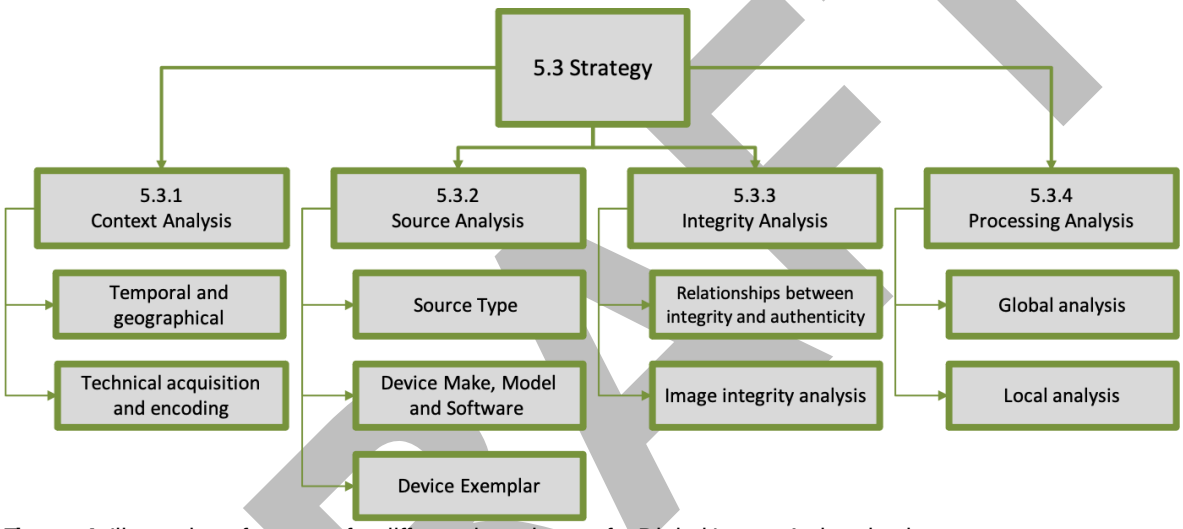

Figure 4. Illustration of strategy for different hypotheses for Digital Image Authentication.

An image authentication task may not necessarily require all four areas to be considered. In the following sections, these four areas are explored in more detail.

5.3.1 Context Analysis

Context Analysis aims to discover all possible elements which are inconsistent with the temporal and geographical context along with technical acquisition and encoding context. In the following tables (Table 2 and Table 3) a list is proposed which is meant to be general and exhaustive, however there may be some additional elements, not considered here, available in special cases. Examples are provided to clarify the concepts. The right column of the tables contains examples of checks. Possible pitfalls or fallacies in using the methods were mentioned in the Methods section and are not repeated below.

Please note that information mentioned in the table about time and position mostly relies on camera settings; therefore, the information could be misleading if the camera was not configured properly at the time of acquisition.

846 **Table 2. Analysis methods and examples for temporal and geographical context analysis.**

Analysis methods	Examples of checks
DATE/TIME Checks between temporal information associated to the image and purported date and time. Methods: internal metadata, file system and external metadata, time indications from content or technological developments	• Consistency of Exif data with claimed time/period. • Compare purported date and time with email header information (on hard drive). • If the image provided is claimed to be the original, and is presented on what is claimed to be the original storage device, then consider if the media and format were available at the expected date of image creation • Examine for objects within the image which did not exist at the purported date and time of acquisition
LOCATION Checks between geographical information associated with the image and purported geographical information Methods: internal metadata, file system and external metadata, location indications from content, visual inspection	• Consistency of photos being taken at a specific location • Examine Exif data to be consistent with purported location • Consistency of image content with the camera/operator position, as obtained through photogrammetric analysis
DATE/TIME & LOCATION Checks between temporal information associated to the image and purported temporal information & location Methods: internal metadata, file system and external metadata, time and location indications from content, visual inspection.	• Temporal information from shadows is consistent with purported time of acquisition & location • Consistency of imagery with weather reports at purported time of acquisition & location. • Examine for buildings/streets/ monuments within the image which did not exist at the purported date and time of acquisition & location, e.g., comparing against satellite images
SCENE AND OBJECT GEOMETRY Check between how the scene and objects appear in the image and their actual properties in the real world. Methods: photogrammetric analysis, location indications from content, visual inspection	• Examine image archives from different sources (satellite, aerial, drone, surveillance, witnesses, social media, etc.) to get measurements of the subject and check whether or not a questioned image is consistent with these measurements. • If the scene depicted in the questioned image still exists and has not changed completely, perform a photogrammetric survey of the scene to get reference measurements of the subject and assess if the image content is consistent with these measurements. • Consistency of the size of static objects in the image (photogrammetric analysis) with the real size of objects that are still present at the scene
PASSAGE OF TIME Check the image content and consecution with a sequence of temporally spaced images (visual verification of consistency of content). Methods: internal metadata, file system and external metadata, time and location indications from content, visual inspection.	• Examine a sequence of images for inconsistencies in appearance, motion and position of objects. Greater confidence can be attributed to an observation if seen in multiple images.

847 **Table 3. Analysis methods and examples for technical acquisition and encoding context analysis.**

Analysis methods	Examples of checks
CODING ARTEFACT Check if the object in the image a result of an optical illusion or an artifact of the image generation (i.e., rolling shutter, compression)? Methods: Visual inspection	• Examine if for example an insect is passing very close to the camera, mistaken for UFOs ("blurfo"). • Examine if objects that are expected to have a certain shape could be deformed because of acquisition or compression artefacts. Examples include: blocking artefacts, interlacing, rolling shutter, etc.
FILE NAME/LOCATION Check if the name and location of the file (i.e., folder location) are named and structured consistently with its expected source Methods: internal metadata, file system and external metadata	• Examine if a file with a name typical from social media applications is inside the camera app folder in a smartphone • If a picture from a series is found in a folder and the file name not is consistent with the other file names in the folder; e.g., PIC1000 is located together with PIC0001-PIC0050
FILE STRUCTURE Check if there any inconsistencies between MAC times, file size and other file system metadata and the image metadata? Methods: internal metadata, file system and external metadata	• If among other pictures there is one with very different features, this may imply something may have happened
RECAPTURE Check if the imagery includes traces that indicate that the image has been recaptured? Methods: Global analysis (Fourier Analysis, Aliasing, Blurring, Colour-contrast non-uniformity, Double JPEG compression, Noise etc.), Visual inspection.	• Examine if a file has been created as a screenshot, screen-capture, printed-capture or printed-scanned image or if it is a "original image".

848
849

5.3.2 Source Analysis

The process of classifying, identifying, or verifying the source device is hierarchically divided in levels, since every step is a specialization of the previous and involves the analysis of the:

1. Source Type (camera, scanner, computer graphic).
2. Device Make, Model and Software (with possibly different camera applications, different versions of the same application or different firmware version),
3. Device exemplar (unique device).

5.3.2.1 Source Type

This level aims at determining the class of the device which has created the image (digital camera, scanner, computer graphics software). The analysis is performed, analysing common traits of images belonging to one of these classes, using the following methods:

- Embedded metadata: metadata and file format features can be used to evaluate the kind of device, for example if the name of the device or software used are saved in the respective metadata sections.
- Global analysis: images from different classes of devices will show different traces, for example:
    - an image from a digital camera should show certain noise and demosaicking artefacts.
    - an image from a scanner should show scanner artefacts (pattern noise).
    - an image from a computer graphic software should not have noise or demosaicking patterns unless digitally added.

5.3.2.2 Device Make, Model and Software

This level is about determining the make, range of models, model, revision, firmware version, software version, of the device which has created the image. The corresponding analysis methods usually needed are:

- If no reference device is available, metadata and file format structure can be used to evaluate the make, model and software version of the device, e.g., by comparing them against specifications or reference databases.
- If pictures from a device of the same alleged make and model are available (see Section 11), their metadata, file structure and global statistics can be compared with the questioned imagery in order to corroborate the make, model or software identification.

Note regarding reference images either acquired from databases or taken using a reference device:

- if the images were captured using a different software or firmware version, the results could be unreliable.
- Even if you are in possession of a device with the same software or firmware (in order to take reference images), it is usually necessary to explore and compare several combinations of settings and parameters (some of which controlled by the user, some other self-adjusted by the camera), see Section 11.2.

In this process, the availability of the manual and datasheet of the (supposed) acquisition device is valuable.

5.3.2.3 Device Exemplar

This level involves verifying whether a specific device exemplar has created the questioned image. The analysis is performed using distinctive traits which should be able to identify as unambiguously as possible the source device.

If pictures from the alleged device exemplar are available (or can be taken), then this possibly may provide support towards or against the proposition that the device is the exemplar. This can be achieved in two possible ways:

- By comparing unique identifiers within the metadata (e.g., the serial numbers). Note: when establishing the support level, the Examiner should consider that such metadata is easily editable, or removable.
- By comparing some features of the reference images with the questioned image. Usually, this involves the analysis of the unique sensor defects, such as fixed pattern noise (FPN), or, more specifically, Photo Response Non-Uniformity (PRNU).

5.3.3 Integrity Analysis

During the verification, it may be necessary to establish if the image is original or not, and which processing steps in the questioned image formation and history are expected to have an impact on the analysis result.

5.3.3.1 Relationships between integrity and authenticity

Integrity and authenticity are different concepts and one does not imply the other. Note that the image integrity being compromised does not imply it is inauthentic, or the other way around. When facing image integrity regarding if a file is an original or not, the Examiner generally must deal with four different kind of scenarios:

1. Integrity is compromised, while authenticity is maintained.
    - An image which has undergone a set of post processing operations, regardless their purpose and kind, if these processing steps do not change the informative content of questioned imagery.
    - Producers of devices can provide tools to import and convert files and metadata from their proprietary format. Images exported or converted by such tools, even if the informative content of the image is unaltered, are considered “non-original” image files.
    - In some cases, processing steps are applied to the image in the form of documented, post production steps. If these processing steps do not change the informative content of questioned imagery (e.g., resizing, compression, level adjustment), authenticity is maintained.
2. Integrity is compromised and authenticity is uncertain
    - An image which has undergone a set of post processing operations, regardless their purpose and kind, which change the informative content of questioned imagery.
    - Synthesised images, as deepfake images.
3. Integrity is maintained and authenticity is uncertain.
    - By recapturing an image, a new original image is created whose authenticity remains uncertain, since it depends on the content of the captured image.
    - In addition to the native camera software, an increasing number of alternative camera applications are available for mobile devices. Some of these are explicitly designed to modify the image in real time (e.g., changing the background or replacing or modifying faces) and thus possibly with a heavy impact on the visual content of the image. Noticeably, most recent devices natively allow generating images in portrait or bokeh mode.
    - In addition, some social networks offer the possibility, by using their own app, to upload images directly on their web platform right after they have been captured, thus allowing the image to not be memorised inside the device. Given that such an image file, hosted remotely by social network platforms, may be the only image version available and, as such, the closest to the camera original image file, the reliability of such images should be evaluated according to the specific case circumstances.
4. Integrity and authenticity are both maintained.
    - An image providing a truthful description of an event is captured and never processed. The Examiner may not be able to prove that both the integrity and authenticity are both maintained

5.3.3.2 Strategy for image integrity analysis

When facing image integrity verification, the Examiner generally must deal with three different kinds of scenarios, with increasing level of difficulty, and with decreasing level of strength of the result:

1. The original version of the questioned image is available
    - The Examiner can easily state whether any modification was applied to the image file, e.g., using a hash comparison.
2. The original version of the questioned image is unavailable but the questioned device is available or the model of the source device is known:
    - Make (or use available) reference images with a reference device or the questioned device
    - Perform checks for information related to make, model and software (see Section 5.3.2.2).
    - The comparison of image file structure (see Section 5.1.2) and embedded metadata (see Section 5.1.3) will give an indication about the integrity of the questioned file.
3. No original reference image is available and the source device type is unknown. In this case, a so called “blind integrity verification” can only be performed:
    - If a totally blind integrity verification has to be carried out, proving the originality is usually impossible. However, the non-originality can still be proved (e.g., detecting presence of a photo editing software name in the Exif software tag.) Some properties of the image may indicate in a less strong way that the image is likely not original (e.g., absence of thumbnail)
    - If a set or database of possible source devices is available. The comparison of the questioned image file structure (see Section 5.1.2) and embedded metadata (see Section 5.1.3) will give an indication as to whether some device is able to create an image with the same format features and metadata.

The main challenges in Image Integrity analysis are:

- Some features can be optional, can have a single possible value, a set of possible values or an almost infinite set of values (e.g., JPEG quantization tables and parameters, JPEG Huffman tables, or other optional metadata), can be poorly documented.
- Different firmware on the same device can lead to different features being observed.

5.3.4 Processing Analysis

A large number of analyses methods are available. To deal with this, prioritization can be carried out following the criteria discussed in Section 10.3. An initial minimisation of the available methods can be achieved based on the image format (e.g., there are methods that only work on JPEG files). Although trying all available methods is an accepted practice, it should be considered that information obtained during previous analyses may help prioritizing or excluding some analysis methods. For example:

- if Metadata analysis suggested presence of digital zoom from the Exif data, this could provide an explanation for some traces found by Global Analysis methods.
- if traces of multiple JPEG compressions were found during the Global Analysis, local methods based on double quantization analysis should be prioritized;
- if the image is strongly JPEG compressed, using methods based on CFA demosaicking traces is likely pointless, since such traces are known to be sensitive to compression.

Elementary methods often require the Examiner to set some input parameters. When possible, the choice of such parameters should be guided by the information obtained during previous analyses. For example, if the image is strongly JPEG compressed, information in higher DCT frequencies is probably limited, and JPEG-based local analysis tools should be configured accordingly.

Table 4 and Table 5 show the classification of the various kinds of analysis which can be performed on an image with the goal to find traces of processing. These methods are listed according to the scope of the analysis.

Table 4. Methods and examples of checks for Global Processing analysis.

Analysed characteristic/methods	Examples of checks
ENCODING Does the image show traces of a previous encoding/compression?	DCT Analysis JPEG Ghosts Analysis
INTENSITY AND COLOUR Does the image show traces of contrast, brightness or colour modification?	Histogram Analysis
CROPPING Does the image show traces of cropping?	Visual Analysis
INTERPOLATION Does the image show traces of a resize or other geometric transformation (rotation, perspective)?	Pixel Correlation Analysis
NOISE Is the image noise profile incompatible with the reference device?	PRNU Analysis FPN Analysis

Table 5. Methods and examples of checks for Local Processing analysis.

Analysed characteristic/methods	Examples of checks
VISUAL CONSISTENCY Is there any visual inconsistency in the image (possibly taking advantage of basic, documented, image enhancement, e.g., level adjustment)?	Visual Analysis
PERSPECTIVE Is there any inconsistency in the perspective of the image?	Shadow Analysis Perspective Analysis Sharpness Analysis
LIGHTING Is there any inconsistency in the lighting of the image?	Visual Analysis
SHADOWS Is there any inconsistency in the shadows of the image?	Shadow Analysis
CLONING Is there any trace of cloned parts within image?	Keypoint-based Clone Detection Block matching Clone Detection
SIZE OF PARTS Is there any inconsistency in the size of parts of the image?	Analysis of perspective constraints
ENCODING Is there any inconsistency between compression traces within the image?	Blocking Artefacts Analysis JPEG Compression Analysis Double JPEG Compression Analysis
CORRELATION Is there any inconsistency in the correlation between pixels within the image?	Local Correlation Analysis Colour Filter Array Demosaicking Analysis
NOISE Is there any inconsistency in the noise within the image?	PRNU Local Analysis Generical Noise Analysis

It is important to be aware that whatever approach is applied, anything found could be the result of either:

- Processing operations that have been applied during the image generation process, e.g., colour filter array demosaicking, interpolation due to camera digital zoom, colour adjustment due to camera internal white balancing, JPEG compression performed by the camera, etc.;
- Processing operations that have been applied after the image generation process, e.g., any global editing performed with image editing software (resize, cropping, level adjustment, median filtering, etc.). When findings suggest that the image has been processed after its generation, it is important to try to characterize the possible source of modifications: for example, a specific social media platform could be associated with a fixed image size and compression strength, specific processing software could be associated to a fixed set of JPEG quantization tables, etc.

Logically, in an authenticity examination the focus lies on the processing operations that have been applied after the image generation process.

5.4 Peer Review

Human-based interpretations play a central role during the whole process of Image Authentication. Therefore, peer review is a useful method to improve objectivity and increase reliability of results. Its use should not necessarily be limited to the final check; peer review can be used during the whole process and should be used for all critical steps and according to the Examiner's needs,

6. VALIDATION AND ESTIMATION OF UNCERTAINTY OF MEASUREMENT

6.1 Validation

General guidelines about validation can be found among others in:

- ISO 17025 (17025:2017, EN ISO/IEC), Section 7.2 'Selection, verification and validation of methods'
- ISO 17020 (17020:2012, EN ISO/IEC), Section 6.2 'Facilities and equipment' - 6.2.11
- QCC-VAL-002 (QCC-VAL-002, 2014), The ENFSI Guideline for the Single Laboratory Validation of Instrumental and Human Based Methods in Forensic Science

The application of these for related fields can be found in:

- ENFSI-BPM-FIT-01 (ENFSI-BPM-FIT-01 , 2015, version 01), "Best Practice Manual for the Forensic Examination of Digital Technology"
- ENFSI-BPM-DI-02 (ENFSI-BPM-DI-02, 2018, Version 01), Best Practice Manual for Forensic Image and Video Enhancement

The requirements for performing a method validation in IA should as a minimum include:

- An outline of the applied methods and their use cases (e.g., for PRNU: a general description of PRNU-based source camera identification and when it is applicable).
- A detailed description of the process, such as in which order, which tools and functions are applied and with which settings (e.g., for PRNU: a description of how the camera's sensor pattern was extracted, how the correlation threshold was determined).
- A collection of rules to ensure that known restrictions, errors and flaws of the used tools do not adversely affect the results, and that the quality of results is optimised according to the given conditions (e.g., for PRNU: specifying the minimum number of reference images required, how to handle saturated images, details of limitations on the supported geometrical transformations, and potential issues related to multiple-camera devices).
- A dataset with known source, recording conditions or processing operation should be used as standards to check if the method gives the expected results (for instance to check that different software give comparable results).
- A validation report.

Some methods may require validation with case-specific example files with expected results (ground truth) and known provenance, covering sufficiently well the range of appropriate sources and typical Customer requirements, such that limitations may be revealed (e.g., for PRNU: by making new reference recordings with cameras of the same type and model to demonstrate that the method performance is acceptable in the specific scenario addressed in the analysis).

Re-validation is needed whenever:

1) the current situation is different from the situation of the validated method, for example:
   - Applying some method on a JPEG image although it was validated for BMP.
   - Using a method that was proposed for analysing digital images to analyse a frame of a video.
   - Using a method for forgery localization based on Colour Filter Array artefacts that was only validated on uncompressed images to analyse a JPEG compressed image.

2) the performance deviates significantly from that expected, for example:
   - PRNU source device identification relies on the assumption that each imaging sensor leaves a unique noise pattern in the image. Technological developments may someday falsify this assumption, e.g., because devices may remove the PRNU noise, or introduce some kind of non-unique artefacts that increase the correlation, thus leading, respectively, to a much larger false negative or false positive rate.

3) significant field related technologies are newly developed which may affect performance of the validated method, for example:

- The technique for double compression analysis may be validated for assisting with detection of double JPEG compression of images. In the case of a HEIC format - presented to the Examiner as a JPEG file; a double JPEG compression analysis would detect the single JPEG compression, which could give rise to false negatives for detecting double compression.

6.2 Estimation of uncertainty of measurement

General guidelines about uncertainty of measurement can be found among others in:

- ISO 17025 (17025:2017, EN ISO/IEC), Section 7.9 'Evaluation of measurement uncertainty' in the ISO 17025 standard'
- QCC-VAL-002 (QCC-VAL-002, 2014), The ENFSI Guideline for the Single Laboratory Validation of Instrumental and Human Based Methods in Forensic Science

The uncertainty within image authentication measurement is mainly caused by:

- Tool inaccuracies: e.g., inherent uncertainty to the design and implementation of the elementary methods within the tools. Inaccuracies are to be checked on a regular basis, by (re)validation.
- Operator inaccuracies: uncertainty caused by the way the methods were applied, e.g., the appropriateness of the tool being selected for the given scenario, and settings of the required parameters;
- Data inaccuracies: reference imagery (reference images chosen for comparison purposes may lack similarity to the questioned image) and databases (e.g., out of date or incomplete database of quantisation matrices), etc.

Given the intricate dependencies which could exist between uncertainties that arise at various points during the image authentication analysis procedures, the uncertainty attached to a specific measurement cannot always be quantified.

If possible, the impact of such uncertainty sources on the image authentication result should also be reported, preferably as evaluated during the method validation for each tool used (e.g., if in a PRNU examination, other reference devices were not examined in order to evaluate discrimination capability of such method in the specific case).

7. QUALITY ASSURANCE

7.1 Proficiency Testing/Collaborative Exercises

Proficiency tests should be used to test and assure the quality of Image Authentication (IA) BPM specific processes. A list of currently available PT/CE schemes as put together by the ENFSI Quality and Competence Committee (QCC) is available at the ENFSI Secretariat and via the ENFSI website. "Guidance on the conduct of proficiency tests and collaborative exercises within ENFSI", QCC-PT-001 (QCC-PT-001, 2014, version 001), provides information for the ENFSI Expert Working Groups (EWGs) on how to organize effective proficiency tests (PTs) and collaborative exercises (CEs) for their members.

There are no accredited European proficiency tests currently available for image authentication investigation covering the whole process addressed within this BPM.

PTs for PRNU based source identification have been provided by NFI. More information and access to the PTs can be obtained by contacting NFI (bob@holmes.nl).

Usually, the Digital Imaging Working Group (DIWG) mailing list provides information about ENFSI PTs/CEs when they occur. It can also be used as a forum to enquire about externally organized PTs/CEs. To be added to the mailing list of the working group, contact the chairperson, as identified via the webpage:
https://enfsi.eu/about-enfsi/structure/working-groups/digital-imaging/

In the absence of available PTs, construction of lab internal test materials, collaborative exercises, or interlaboratory tests with well- known provenance/ground truth can provide an alternative for forensic labs with sufficient resources. Another possibility is to design experiments using data from publicly available data sets like those proposed in scientific publications.

7.2 Quality Controls

It is recommended that procedures are in place in order to mitigate against bias within the examination. The following suggestions should be considered in order to achieve this:

- Delegate initial assessment and communication with the customer and examination to different persons (Third Party, see Section 9).
- Have a second Examiner for conducting the examination independently or for conducting critical findings checks.
- Assigning an arbitrator to deal with any differences of opinion between Examiners.
- Establish a Peer review system for the reports (see Section 5.4).

Assuring the use of valid methods is an important task of the quality management system (see Section 6). To perform validation, datasets of images with known source, recording conditions and processing history have to be maintained covering the whole range of IA tasks of the lab. The performance of new methods on the appropriate datasets has to be checked and documented as well as the performance of already validated methods on new, additional data. A fault management system should be implemented to guarantee that new information about features or defects of devices, algorithms or methods used, as well as the discovery of flaws in IA processes and their effects on (intermediate) results are documented, communicated to and discussed with the customers of the affected current and former cases.

7.3 Data Collection for control, monitoring and trend analysis

High speed development of devices and technology demand for a high pace in adapting the methods and the corresponding documents (standard operating procedures, checklists, test data sets, etc.). Therefore, it is necessary to maintain and review statistics about the applicability and success of methods in different situations.

8. HANDLING ITEMS

Digital imaging is part of IT and therefore the general rules for digital evidence apply, according to:

- ENFSI-BPM-FIT-01 (ENFSI-BPM-FIT-01 , 2015, version 01), "Best Practice Manual for the Forensic Examination of Digital Technology".
- The requirements of the local legal system (e.g., about privacy and data protection considerations, chain of custody and retention expiration).
- The local quality management system (e.g., about documentation, use of hash values to prove identity of file content and backup procedures).

8.1 At the scene

There is no specific consideration for handling items at scenes for Image Authentication. The more the digital context (data and devices) is preserved and collected at the scene, the more possibilities may exist to check questioned imagery against that data and to produce additional reference material.

8.2 In the laboratory

8.2.1 Data stored on examination systems

All submitted data (questioned files, forensic image, reference files) should be stored write-protected on storage resources accessible by the examination system, the examination(s) taking place on copies. Alternatively, a forensic image of the primary data can be made to preserve it prior to any subsequent examination being carried out on that copy. Files should be stored in a way that clearly distinguishes copies from the originals, without altering the original filenames.

8.2.2 Devices

The general rules for handling devices are described in ENFSI-BPM-FIT-01 (ENFSI-BPM-FIT-01 , 2015, version 01), sections 8 and 9. In image authentication, the handing of questioned devices differs from how a device would normally be treated forensically; because they may be used to produce reference images (see Section 11). Active use of the imaging capabilities (using the device to take new images) requires taking some precautionary measures, depending on the device type and the circumstances of the use:

1. Devices needed for production of reference material must be kept operational as long as needed to take adequate images for the examination, it must be possible (and safe) to turn the device on, access, and use it for image capture.
2. Mobile phone devices belonging to a suspect/witness may require a standard forensic examination (for texts, images etc) by other areas of the laboratory prior to being authorised for being used to generate reference material.
3. It might be necessary to avoid external modifications of the systems (e.g., updates of the software or firmware via wireless connections), because the version may have influence on captured images. Even if a connection to an internet resource (like Instagram, Snapchat or WhatsApp) is needed to create reference material, updates should be blocked reliably.
4. The content of internal storage must have been saved in an adequate way (e.g., by making a forensic image, specifying a physical image if unallocated space is of interest). Note: the capture procedure may change the internal storage (not only picture folders but also image galleries, thumbnail databases, recent lists etc.).
5. New external storage items (e.g., memory cards) should be used to take new images on the device.

Points 1 and 3 of the above list apply also to reference devices of the same type and version as the questioned ones.

Considerations related to using a questioned device are mentioned in Section 11.2.

9. INITIAL ASSESSMENT

9.1 Introduction

Recall that this BPM is mainly focussed on the technical issues related to Image Authentication (IA). Initial gathering and assessment of potential IA evidence at a crime scene is therefore not covered in detail in this document. Further guidance on collecting evidence at scene can be found, e.g., in ENFSI-BPM-FIT-01 (ENFSI-BPM-FIT-01 , 2015, version 01) in sections 8 (Handling Items) and 9 (Initial Assessment).

Any work carried out will be to best answer the requests of the Customer. At each stage, it is important that the course of action is selected based on (i) an assessment of both the requests put forward by the Customer and (ii) the possible alternative(s), thus mitigating the effects of bias.

9.2 Reviewing the Customer Requirements

It is essential before starting any examination in the laboratory to understand, or agree with the Customer, the purpose of the examination requested. First of all, an assessment should be made to establish what is technically possible and worthwhile in order to meet the Customer requirements. For IA, reviewing the Customer requirements may involve several important steps, including but possibly not limited to:

- Steps recommended to be carried out by a Third Party:
  - Checking whether the Customer requirements are clear (i.e., what is exactly claimed or questioned).
  - Checking whether there are limitations on cost and timing.
  - Checking if there are any matters of confidentiality to be communicated to the Examiner(s) (e.g., vulnerable witness or informant may need to be anonymised in all images and/or reports).
  - Determining the Customer's priorities for the information requested.
  - Translating the Customer's questions and claims (concerning the provenance of the image) into relevant competing hypothesis (ENFSI Guideline for Evaluative Reporting in Forensic Science (Willis, 2015)) for the Case Leader.
  - Enquiring about any additional information pertaining to the case, for performing or prioritizing relevant technical examination methods - e.g., documentation check and provenance information (see sections 9.4 and 9.5), or the level of relevant knowledge - in the fields of imaging, IT, law, forensics etc. of the person who originally produced the images (see Section 10).
  - Anonymization of case details which may be biasing to the Examiner(s) (e.g., previous convictions of suspect, results of forensic examinations unrelated to the authentication task, etc.).
  - Deciding which case information will be made available for the Examiner(s).
- Steps which may be carried out by either the Case Leader or a Third Party:
  - Making enquiries regarding privacy and security requirements, in addition to those required of the local standard legal framework (data protection, anonymisation of individuals within imagery in reports produced, etc.).
  - Establishing what constraints or other considerations may exist, e.g.:
    - Preservation of material for other purposes such as fingerprint examination, or DNA.
    - Custody and reporting deadlines.
    - Future examinations that will be based or depend on the results of this examination.

9.3 Scope of examination

It is recommended that the following steps will be carried out by the Case Leader:

1. Estimating the width of the examination, i.e., which technical examination methods may be feasible and relevant, and/or required.
2. Estimating which additional evidence, information or digital data may be required from the Customer; e.g., the device needed for collecting reference pictures or examining its memory or data storage, or other possibly relevant storage media or devices (e.g., a suspect's PC, mobile phones, etc.).
3. Initially estimating the depth of each of these possible examination steps, including in particular how much resources and effort could or should be invested into each examination and revisiting what could be the resulting Customer cost and reporting time. Such depth estimation may also include, e.g., the amount of new reference imagery or comparison devices that may be collected and investigated, the amount and number of variations in parameter settings of used tools, etc.
4. Performing an overall risk assessment, taking into account, e.g., the risk of destruction of (other or yet unknown) evidence, or causing irreversible changes to relevant data or items.

9.4 Documentation Check

Documentation should be complete with respect to the chain of custody (from point of seizure by the authorities) including details of the method of retrieval and conveyance (including, e.g., system time information, passwords used or needed, etc). Ideally the handling and/or processing steps carried out before seizure should also be provided and traceable to the individual who carried them out.

If sufficient information is not provided, the Customer should be contacted requesting this. If this information cannot be provided, the Customer should be informed about the possible effects or impact on the findings (see Section 12). Such interaction (including the impacts, and the reporting of these to the customer) should also be included in the report (see Section 13).

9.5 Preliminary Check of Purported Provenance

The purported provenance of the imagery should be assessed. The suspect (from which the Customer has acquired the imagery) may have a story of provenance for the imagery. The Customer may also provide additional information as to how they themselves have handled/acquired this imagery. If the manner in which the Customer has acquired the imagery from the suspect does not appear to be consistent with the imagery that has been supplied (e.g. the Customer state they have sent an original, and it is evident that you have been supplied with a screen capture), or if insufficient information has been supplied regarding the origin of the data, the Customer should be contacted for resolving these issues.

If no or limited information regarding provenance has been supplied, this should be reported on (see Section 13). If such information was not provided, the Case Leader should attempt to establish the provenance of the imagery during the in-depth technical examination, using appropriate analysis methods (see Section 5, for further guidance).

Reasonable steps should be taken to obtain previous or alternative version(s) of the imagery. The examination of earlier versions in parallel with the supplied imagery may be useful as it may for instance demonstrate what has been changed and when.

When multiple versions of the same image are available, then some of these versions may be excluded from the examination (see Section 10.1). For example, if the only difference between the images is that they have suffered data loss due to the way the images have been seized and submitted to the forensic laboratory (e.g., implicit degradation which has occurred due to transcoding, low quality scanning of documents, photography, or screen capturing software used to acquire images displayed on a computer screen).

The lifecycle of the imagery can be divided into the following stages:

- Before seizure (not within jurisdiction of law enforcement).
- During seizure (methods used to seize may impact on quality).
- During handling/selection/submission (methods used to convey, store and process data may impact on quality).

Care should always be taken that no implicit, i.e., hidden or non-obvious loss or addition of information may have occurred during any of the stages listed above, e.g., changes in image metadata, image recompression or image format conversion. If this cannot be avoided, tested and/or verified, then a complete processing history should ideally be provided alongside the provided imagery.

10. PRIORITISATION AND SEQUENCE OF EXAMINATIONS

The starting point of any examination should always be composing an initial overview of the available items and resources, and estimating the evidential value that could be obtained from each item.

10.1 Preparation

In cases where a large number of questioned items is submitted, Third Party and the Customer need to select some specific items on which the examinations primary will be performed on. This selection can be performed by random sampling or by the Customer.

If a selection not is possible the Examiner need to establish if there is any evident connection between the submitted items. Cursory inspection of the data is based on easy-to-get features like visual content, hash values, file names, file formats and simple metadata (image sizes, device type identifiers, etc.). Typical connections of interest are “taken independently under similar conditions” and “seem to have a common ancestor”. They allow to subdivide the items into categories, facilitating prioritisation and scheduling of examinations. A more detailed description can be found in the workflow example below.

10.2 Prioritisation

Prioritisation tries to optimize benefit/cost ratio by the ordering of examinations. Prioritisation is essential if the expected effort to reach comprehensive results exceeds the limits set for the examination process. In this case prioritisation tries to reach optimal results under fixed limitations. Otherwise, the goal is to minimize the effort to get comprehensive results.

The prioritisation will depend on:

- the item(s),
- the request(s),
- the available resources (Examiner(s), devices, tools), and
- constraints like the Customer’s timeframe and cost limitations.

Hence, the possible criteria for the Case Leader to determine priority, taking into consideration the prioritisation requested by the Customer and availability of resources, are:

- Expectation that examination of a questioned item may yield very strong support towards one of the propositions.
- Evidential value versus estimated complexity.
- Evidential value versus estimated cost.
- Evidential value versus estimated time.

Note: High evidential value can relate to either support or opposition for a given proposition. In case several connected (e.g., near duplicates) images were submitted, it may not be necessary to examine all of them if strong support towards one of the propositions is already reached early in the examination for one of the images (there may be no value in examining inferior copies of the image).

10.3 Sequence of examinations

Strict rules for the sequence of examinations, applicable for the whole range of possible authentication examination tasks, can’t be given. In general, the sequence of examinations of a single image is based on a layered approach from less to more technical complexity. It may not be necessary to perform all potential examination methods if strong support towards one of the propositions is reached early in the examination (there may be no value in carrying out other methods which at best would only provide limited additional support for the same proposition).

The following areas of examination should be considered starting with basic approaches, to more advanced if required at a later stage:

- Initial Assessment (see Section 9).
- Reconstruction (see Section 11)
- Methods
  - Analysis of External Digital Context Data (see Section 5.1.1)
  - Image File Structure Analysis (see Section 5.1.2)
  - Embedded Metadata Analysis (see Section 5.1.3)
  - Image Content Analysis - Analysis of Visual Content (see Section 5.2.1)
  - Image Content Analysis - Global Analysis (see Section 5.2.2)
  - Image Content Analysis - Local analysis (see Section 5.2.3)
- Evaluation and Interpretation (see Section 12)
- Presentation of Evidence (see Section 13)

10.4 Example authentication workflow

Stage 1: Preparation of examination process:

a) Rough survey of questioned items and reference items, grouping into categories based on similarities in content and/or metadata, prioritizing further examinations based on these findings.
b) If a forensic image of the questioned device has been supplied, carry out a rough survey to find reference items (e.g., to check for consistency of metadata, between questioned and other items on the device).
c) If reference devices are provided, test each device, create or gather, inspect and classify some sample images per device – having awareness that network-enabled (e.g., mobile phones) imaging devices may have more easily received software updates since the creation date of the questioned image(s).
d) Compare reference images properties and metadata against the questioned image(s) metadata, so as to determine whether the questioned images(s) could be compatible with one or more of the provided reference devices. This comparison could be conducted on a hierarchical basis (e.g., first compare more broad properties such as image format and Exif metadata, then subtler elements such as JPEG markers order).
e) Otherwise, obtain specifications for device(s) believed to have created the questioned image(s).
f) Similarly, if no or not enough reference images are available, start search for alternative sources:
   - Request additional material from the customer as far as available (e.g., access to other images from a mobile phone data extraction, to provide information regarding images made under different OS versions).
   - Start procurement to get (a) suitable reference device(s).
   - Do more intensive searches on the forensic image of the questioned device(s) (e.g., for deleted images which may show unedited versions of questioned itme(imagery).
   - Perform searches on internet resources for reference files recorded by the example device or processed by a specific software version.

Stage 2: Loop of examination process:

- Choose the highest prioritized question and then the category of images most likely to advance answering this question. Within that category then choose a typical image and the elementary method estimated to have the highest evidential value / cost ratio.
- Optimize parameters of this elementary method being used, apply it to reference image(s) for comparison.
- Expand to other related questioned images of that category and suitable other categories. This may help to increase the reliability of the obtained results, or it may serve to adjust the classification.
- Try to find explanations for the observed effects and evaluate the impact of such explanations on the provided propositions (when needed, new propositions may be

created). Look for suitable methods to raise or diminish the support toward such new propositions.

- Loop to a) until all questions in the request can be answered with sufficient certainty or all available resources (time, manpower, methods, cost, etc.) are exhausted.

11. RECONSTRUCTION

11.1 Introduction

Creation, detection and use of reference items play a central role in image authentication. Reference items are equipped with some information about their source and/or processing history. A typical image authentication method extracts features (single values, statistics, images, etc.) from the image to be examined and (a) suitable reference image(s) with the same elementary method and involves a comparison between the results obtained. A high similarity of features would support the propositions that the images share common elements in source or processing history and vice versa.

In order to carry out a reconstruction, an understanding of the alleged history (either provided or hypothesized) of the creation of the image is needed i.e., the interrelation between source and processing steps and the features of the resulting image. In general, the sequence of processing steps may not always be apparent (leave obvious/unique detectable traces). Note: trace artefacts may be revealed by elementary methods, arising as a side effect of non-malicious processing steps (e.g., transmission). Additionally, you may not expect to find indicative traces following all manipulations/processing steps (especially if counter forensic methods have been used).

Reconstruction can deliver reference images with highest level of reliability. To perform a reconstruction is however not always necessary; it depends on the claims or propositions to be tested in the case and the possibilities and need to perform a reconstruction at all. Based on the specific case, reconstruction may involve creating new images using the suspected source device(s) and/or by applying the suspected image processing chain. Further considerations are detailed in sections 11.2 and 11.3.

11.2 Considerations with respect to using devices

To create reference images, one should use (in order of preference) either the questioned device or some reference device of the same make, model and firmware version. Important:

- When using the questioned device make sure not to destroy any data stored on the device which may be still needed. If required by local jurisdiction, seek relevant authorisation prior to making any changes to the device (including making images).
- Try to set the parameter settings corresponding to the questioned image, documenting all values and any changes made (for example: zoom factor, camera mode and geo-localization features).
- Depending on the choice of methods (see Section 5) and on the intended use of the images, it might be advisable to capture similar scene, movement and content (attempting to match in a technical sense, such as mimicking presence of saturated areas, texture, brightness, etc.).

Note:

- Modern imaging devices like mobile phones may update their software rather frequently which can have some influence on images taken (Operating system version and version of applications - which may play a significant role in determining the properties of generated images).
- Two devices of a specified make and model may have different hardware components.

11.3 Considerations with respect to processing chain

Image processing functions can introduce certain traces in an image. The markedness of these traces may depend on:

- Acquisition: Characteristics of the questioned image data (e.g., saturation, resolution, shooting mode).
- In-camera processing: Implementation details and parameters of the processing function(s), i.e., filter settings, High dynamic range (HDR) techniques.

- Post-processing phase: Other parts of the processing chain, especially typical post-processing functions applied to the image data before examination (like compression, conversion, resizing, etc.)

When creating reference images, it is important to try reproducing the whole hypothesized lifecycle, starting from acquisition and following with in-camera processing and compression steps, as well as any possible post-processing steps.

Note:

- There are many possible ways to achieve a certain modification. It is therefore not always possible to discover the actual image processing chain.
- It is important to create a validation of the above methods to check that the proposed processing steps conform to the assumed processing steps of the original.

12. EVALUATION AND INTERPRETATION

The ENFSI Guideline for Evaluative Reporting in Forensic Science (Willis, 2015) provides forensic Examiners with a framework for formulating evaluative reports. This guideline should be consulted for specific guidance on formulating logical, evaluative opinions. This BPM provides details of some of the factors that can influence evaluation in Image Authentication (IA) and should be read in conjunction with the ENFSI Guideline.

12.1 Interpretation of individual findings

The degree of support of a finding towards a pair of propositions depends on the discriminating power of the elementary method used. To illustrate this, an example is given below:

An elementary method based on Local Noise Analysis is employed to analyse an image containing a cat. The customer wants to know whether the cat has been pasted into the image or not. Upon examining such question, the Third Party formulates two competing propositions:

- *H1: Cat X has been pasted into image A after the file was captured by a camera.*
- *H2: Cat X was in the scene when image A was captured by a camera.*

If in this situation a Local Noise Analysis elementary method produces a map where the cat "stands out", the Examiner should consider the possible reasons why this happens. The Examiner may be facing a true positive result (the region containing the cat actually has a noise pattern which is not consistent to the rest of the image) or a false positive result (e.g., because the elementary method is sensitive to the cat's hair texture, so that the cat would stand out anyway, regardless of possible manipulations). The degree of support towards propositions H1 and H2 depends on the discriminating power of the Local Noise Analysis elementary method. It should be noted that, in this case, the method involves the interpretation by the Examiner.

In image authentication, establishing the discriminating power of an elementary method is often challenging. While the performance of each elementary method is often evaluated and reported in the corresponding scientific paper, the testing conditions in such experimental evaluations are typically very different than those encountered in casework. Therefore, it is necessary for the Examiner to understand the discriminating power of an elementary method in the circumstances of the particular case. In order to accomplish this, an Examiner could:

1. Create a suitable testbed (see Section 11) which reflects as close as possible the current examination, and establish performance of the method on such testbed.
2. Investigate the performance of the elementary method on available datasets and gather information on its discriminating power. This investigation should reveal the influencing conditions (e.g., parameter settings of this method or properties of the image) that may give rise to false negative and false positive results.
3. Examine the behaviour of the elementary methods with respect to findings from other similar features within the questioned image (e.g., for local analysis methods).

12.2 Overall interpretation of findings and formulation of conclusions

During the evaluation stage all findings from the different elementary methods are evaluated by the Case Leader, resulting in a conclusion that states the evidential weight as a level of support for each one of the competing propositions. Some results of operations on images can be assessed independently, but many results have to be compared with other results to deliver evidential value.

In this stage the Case Leader should also consider the background information (see Section 9) regarding how the imagery was handled since it has been placed in the custody of law enforcement till its IA examination, as any processing steps encountered (e.g., due to downloading or transfer by e-mail) may have had a causal effect towards the observed

findings. At the same time the Examiner should avoid any possible or known risk of introducing bias into the overall process (see Section 9).

The final conclusion of an authentication examination states the evidential weight of (all) the findings as a level of support for one of the competing propositions. Support levels are typically reported using a graded scale. Currently, there is no universally accepted scale for reporting IA conclusions and there is a wide range in scales used by different agencies. The ENFSI member laboratories are expected to comply with the ENFSI Guideline for Forensic Evaluative Reporting (Willis, 2015), which recommends both to use the likelihood ratio (LR, that is, likelihood of findings given the proposition divided by the likelihood of findings given the alternative proposition) as an indication for the level of support (often referred to as the strength of evidence), and a graded scale to associate verbal expressions to numerical values, where required.

The assignation of a precise quantitative likelihood to any of the examination findings in IA is often impossible; mainly because:

- The findings of some elementary methods only admit qualitative evaluation, (e.g., only high or low probabilities of findings under the competing propositions).
- The lack of adequate reference databases to allow evaluating the likelihood of the findings under one of both the competing propositions.
- Probabilities are sometimes subjective in their nature, even though the rules for their combination may be valid.

For this reason, the formulation of conclusions largely relies on the training, knowledge and experience of the Case Leader.

In order to reach a numerical value (or an interval) as close as possible to the evidential weight of the findings, the contribution of findings from each analysis conducted should be considered. In doing so, either the degrees of support (under each of the two propositions) should be combined, or the likelihood of the whole set of findings would be used. According to the value of the likelihood ratio computed based on the likelihoods of the findings under the two competing propositions, a textual form of the conclusion could be:

- The findings from the examination lend a strong support **for** the proposition rather than to the alternative proposition, or
- The examination findings provide strong support **against** the proposition rather than to the alternative proposition.

If the estimated LR for the example given in section 12.1 would be 2000, the textual form of the conclusion (according to ENFSI Guideline [9]) could be:
The forensic findings provide strong support for that the cat has been pasted into the image after it was generated by the camera, rather than the cat was in the scene when the questioned image was captured by a camera.

13. PRESENTATION OF EVIDENCE

When the examination is done, the evidence can be presented to court either orally or in writing. In both cases the evidence should be provided with honesty, integrity, objectivity and impartiality.

General guidelines about the presentation of evidence can be found among others in ENFSI-BPM-FIT-01 (ENFSI-BPM-FIT-01 , 2015, version 01), ENFSI-BPM-DI-02 (ENFSI-BPM-DI-02, 2018, Version 01), the ENFSI Guideline for Evaluative Reporting in Forensic Science (Willis, 2015) and ISO 17025 (17025:2017, EN ISO/IEC) (Section 7.8 'Reporting of results') and ISO 17020 (17020:2012, EN ISO/IEC) (Section XX “”). The way of reporting may vary depending on national legal stipulations or requirements. Nevertheless, the overall reporting process should still enable independent review or reproduction of the reported results.

When the evidence of an image authentication examination is presented in writing, the report should state whether or to which degree, case specific questions can be answered. It usually includes the main observed image authentication related features of the image, in accordance with its purported context, source, integrity, and processing history. If an evaluative conclusion is made based on relevant population data, the source of the data should be made clear. If the evaluative opinion is based upon subjective knowledge, training and experience, this should be stated also. All the supporting data should at least be retained by the laboratory, or depending on jurisdiction, supplied with the report – in order to permit repeatability.

If imagery is included in the report (e.g., to communicate the region which is suspected to be locally modified), it should not invite non-experts to form their own interpretation (e.g., by attempting to interpret a noise map of the data). A possible solution is to include a copy of the original unprocessed image, annotated to indicate the feature of interest (or a sketch used instead). It should be made clear that the quality of included imagery may be reduced depending on the reporting format or method. For example, quality loss may occur due to subsequent printing onto paper, or rescaling/compression etc. If imagery is included in the report, and superior quality digital versions are available, a reference to these files should be provided.

When the evidence of an image authentication examination is presented orally, the expert witnesses should resist or refrain from responding to questions that take them outside their field of expertise unless specifically directed by the court, and even then, a declaration as to the limitations of their expertise and possible risks involved should be made.

14. HEALTH AND SAFETY

Health and safety considerations will depend upon the operational requirements of the agency or organization for whom the Examiner works and the types of casework undertaken.

The general health and safety rules for handling digital evidence should be applied according to the laboratory quality management system and standard operating procedures (SOPs).

Certain issues mainly arise when extracting data from devices, e.g., specific health and safety measures should be considered when handling hazardous materials (including objects with sharp edges), possibly contaminated objects (e.g., biohazards), toxic materials etc.

Psychological health risks may arise due to exposure to indecent or disturbing imagery. An organization should implement proper provisions and procedures to mitigate or counteract these risks whenever staff are required to work with such imagery.

When viewing imagery for prolonged periods of time Examiners should take regular screen breaks - and be aware of the effects of prolonged exposure to blue light.

15. REFERENCES

17000:2020, EN ISO/IEC. (n.d.). *Conformity assessment — Vocabulary and general principles.*

17020:2012, EN ISO/IEC. (n.d.). *Conformity assessment — Requirements for the operation of various types of bodies performing inspection.*

17025:2017, EN ISO/IEC. (n.d.). *General requirements for the competence of testing and calibration laboratories.*

9000:2015, ISO. (n.d.). *Quality management systems — Fundamentals and vocabulary.*

Anderson, T., Schuman, D., & Twining, W. (2005). *Analysis of Evidence* (Second Edition ed.). Cambridge Unversity Press.

ENFSI-BPM-DI-02. (2018, Version 01). *Best Practice Manual for Forensic Imge and Video Enhancement.* European Network of Forensic Science Institutes.

ENFSI-BPM-FIT-01 . (2015, version 01). *Best Practice Manual for the Forensic Examination of Digital Technology.* European Network of Forensic Science Institutes.

Farid, H. (2019). *Photo Forensics.* MIT Press.

ILAC-G19:08/2014. (2014). *Modules in a Forensic Process, section 4.2.3.*

Korus, P. (2017). Digital image integrity–a survey of protection and verification techniques. *Digital Signal Processing 71*, pp. 1-26.

QCC-PT-001. (2014, version 001). *Guidance on the conduct of proficiency tests and collaborative exercises within ENFSI.* European Network of Forensic Science Institutes. European Network of Forensic Science Institutes.

QCC-VAL-002. (2014). *Guidelines for the single laboratory Validation of Instrumental and Human Based Methods in Forensic Science.* European Network of Forensic Science Institutes.

Willis, S. M. (2015). *ENFSI guideline for evaluative reporting in forensic science: Strengthening the Evaluation of Forensic Results across Europe.* European Network of Forensic Science Institutes.

16. AMENDMENTS AGAINST PREVIOUS VERSION

Not applicable (first version).