DRAFT International Standard

ISO/IEC DIS 21617-3

Information technology — JPEG Trust —

Part 3: Media asset watermarking

ICS: 35.040.30

ISO/IEC JTC **1**/SC **29**

Secretariat: **JISC**

Voting begins on:
2026-07-14

Voting terminates on:
2026-10-06

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENTS AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

This document has not been edited by the ISO Central Secretariat.

Reference number
ISO/IEC DIS 21617-3:2026(en)

© ISO/IEC 2026



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2026

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ..... **v**
Introduction ..... **vi**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **2**
4 Media Asset Watermarking Framework **5**
4.1 Description 5
4.2 Overview 5
4.3 The framework 5
4.4 Evaluation criteria 6
5 Watermark embedding and detection **6**
5.1 Watermark signalling 7
5.1.1 Example 1 7
5.2 Algorithms 7
5.2.1 Semantics 7
5.2.2 Example 2 8
5.3 Referencing an external repository 8
5.3.1 Semantics 8
5.3.2 Example 3 8
6 Watermark structure **8**
6.1 Syntax 9
6.2 Semantics 9
6.3 Example 4 10
6.4 Payload calculation examples 11
6.4.1 Minimal viable payload 11
6.4.2 Payload with repository information 11
6.4.3 Payload with timestamp 12
7 Watermark embedding imperceptibility **12**
7.1 General 12
7.2 Embedding performance metrics 12
7.2.1 Mean squared error (MSE) 12
7.2.2 Peak signal-to-noise ratio (PSNR) 13
7.2.3 Weighted PSNR (wPSNR) 13
7.2.4 Just noticeable differences (JND) 13
7.2.5 Structural similarity index (SSIM) 13
7.2.6 Fréchet inception distance (FID) 14
7.2.7 Subjective quality measurement 14
7.3 Semantics 14
7.4 Example 5 14
8 Watermarking robustness performance **15**
8.1 General 15
8.2 Extraction performance metrics 15
8.2.1 Normalised correlation (NC) 15
8.2.2 Bit Error Rate (BER) 15
8.3 Robustness against attacks 15
8.3.1 Signal processing 16
8.3.2 Geometric processing 16
8.3.3 Removal 17
8.3.4 Compression 18
8.3.5 AI-based manipulation 18
8.4 Semantics 18
8.5 Example 6 19

© ISO/IEC 2026 – All rights reserved

9 Embedding and referencing **19**
Bibliography **20**

© ISO/IEC 2026 – All rights reserved

Foreword

ISO (the International Organization for Standardisation) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardisation. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organisation to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organisations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see https://www.iso.org/directives or https://www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at https://www.iso.org/patentsandhttps://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO-specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see https://www.iso.org/iso/foreword.html. In the IEC, see https://www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 29, Coding of audio, picture, multimedia and hypermedia information.

A list of all parts in the ISO 21617 series can be found on the ISO and IEC websites.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at https://www.iso.org/members.html and https://www.iec.ch/national-committees.

© ISO/IEC 2026 – All rights reserved

Introduction

Current technologies, especially with the rise of generative AI, have made the modification or synthetic creation of media assets easy for general users. While such developments offer new opportunities, particularly in creative industries, the proliferation of digital media asset content, coupled with the negligible cost of copying and redistribution, has significantly increased the risk of piracy, unauthorised replication and spread of misinformation, disinformation and mal-information.

In many application domains, creators may want or need to declare the type of modifications that were performed on the media asset, in contrast to other situations where the intention is to conceal the existence of manipulations. Media modifications are not always negative, as they are increasingly a normal and legal component of the production pipeline. Governmental organisations may consider new legislation, including the right to opt out of text and data mining, as well as the mandatory declaration of synthetic media and their manipulations. Companies, such as social media platforms and news outlets, may develop mechanisms that clearly detect and annotate manipulated media when it is shared, in support of establishing trustworthiness in media assets.

To facilitate globally interoperable media asset authenticity, integrity and provenance, JPEG (ISO/IEC JTC 1/SC 29/WG 1) developed and published an international standard: JPEG Trust, Part 1: Core Foundation (ISO/IEC 21617-1:2025). The JPEG Trust Part 1 standard defines a media asset as comprising its content, metadata, and a tamper-evident Trust Record. This Trust Record includes one or more Trust Manifests, which contain assertions about the asset's origin, device details, attribution, rights, edits, and related information. From this, Trust Indicators are derived and compiled into a Trust Indicator Set, which is evaluated using a Trust Profile to produce a Trust Report that assesses the asset's trustworthiness. Digital watermarking, in use for several decades, has been increasingly adopted as a method for embedding information directly into media assets in a way that can be both visible or invisible and robust. This technique, as illustrated in Figure 1, establishes a link between the media-related information, *e.g.,* metadata, and the content, one that is challenging to disrupt without compromising the intended usage of the media asset itself. Since the inception and rapid rise of generative AI media assets, watermarking has increasingly gained popularity, both within the industry and among policymakers, as a solution to signal whether the media asset is AI-generated or AI-manipulated content. Such watermarking is equally beneficial for media assets generated outside the context of AI (e.g., photographs and edited media assets). Furthermore, watermarking is also helpful to link other associated content provenance information, such as intellectual property rights, authorship, and ownership.

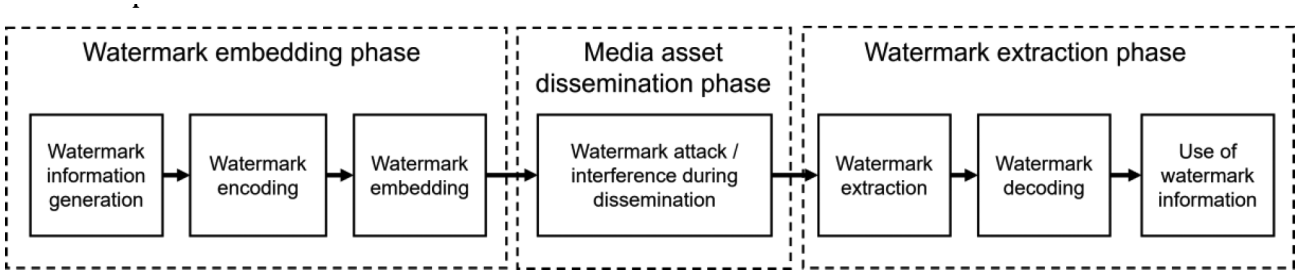


Figure 1 — A generic watermarking embedding and extraction workflow in the context of the media distribution or asset dissemination phase.

While growing efforts are noticeable in developing technologies, there is a need to have a standardised way to indicate the watermarking process, the structure of the watermarks, evaluate their performance and link them with metadata and other information. This document (JPEG Trust Part 3) ensures interoperability between a wide range of processes/algorithms dealing with media asset watermark embedding and extraction, providing a set of standard mechanisms to describe watermark structure and information relating to the watermarking process used.

Furthermore, a key aspect of understanding the effectiveness of the watermarking processes and the interpretation of the watermarks in establishing the trustworthiness of a media asset relies on the robustness and resilience of the watermark against adversarial attacks or unintentional modifications and retrieval of relevant information using the extracted watermark. Therefore, this document provides

© ISO/IEC 2026 – All rights reserved

a flexible framework through watermarking structure, a set of watermarking embedding and robustness assessment criteria, and user-defined watermarking profiles relevant to their trust requirements.

To facilitate a holistic approach for media trust, strengthening the overall media trust ecosystem, this document describes how media asset watermarking complements the annotation-based approach defined in JPEG Trust Part 1: Core Foundation.

This document (JPEG Trust Part 3) provides a comprehensive framework for individuals, organisations, and governing institutions interested in media asset watermarking and their use in establishing trust through provenance, authenticity, integrity, copyright, and identification of assets and stakeholders either in a standalone way or in conjunction with other mechanisms such as an annotation-based approach (e.g., JPEG Trust Part 1).

© ISO/IEC 2026 – All rights reserved

Information technology — JPEG Trust —

Part 3:
Media asset watermarking

1 Scope

This document extends the framework described in ISO/IEC 21617-1 (JPEG Trust Part 1 - Core Foundation) with watermarking capabilities for purposes such as content authenticity, provenance, integrity, intellectual property rights, and labelling. These extensions include aspects of an algorithm-agnostic embedding and extraction process, the signalling of the presence of a watermark, the structure of the watermark, evaluation criteria, and pointers to repositories containing additional information.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 10918-1:1994, *Information technology — Digital compression and coding of continuous-tone still images: Requirements and guidelines*

ISO/IEC 15444-1:2024, *Information technology — JPEG 2000 image coding system — Part 1: Core coding system*

ISO/IEC 19566-4:2020, *Information technologies — JPEG systems — Part 4: Privacy and security*

ISO/IEC 19566-5:2023, *Information technologies — JPEG systems — Part 5: JPEG universal metadata box format (JUMBF)*

ISO/IEC 19566-6:2019, *Information technologies — JPEG systems — Part 6: JPEG 360*

ISO/IEC 19566-7:2022, *Information technologies — JPEG systems — Part 7: JPEG linked media format (JLINK)*

ISO/IEC 19566-8:2023, *Information technologies — JPEG systems — Part 8: JPEG Snack*

ISO/IEC 18477-1:2024, *Information technology — Scalable compression and coding of continuous-tone still images — Part 1: Core coding system specification*

ISO/IEC 21617-1:2025, *Information technology — JPEG Trust — Part 1: Core foundation*

ISO/IEC 18181-2:2024, *Information technology — JPEG XL image coding system — Part 2: File format*

ISO/IEC 29199-2:2020, *Information technology — JPEG XR image coding system — Part 2: Image coding specification*

ISO/IEC 21122-1:2024, *Information technology — JPEG XS low-latency lightweight image coding system — Part 1: Core coding system*

ISO/IEC 6048-1:2025, *Information technology — JPEG AI learning-based image coding system — Part 1: Core coding system*

ISO/IEC 14496-12:2022, *Information technology — Coding of audio-visual objects — Part 12: ISO based media file format*

© ISO/IEC 2026 – All rights reserved

C2PA Technical Specification, *C2PA Technical Specification 2.3, Coalition for Content Provenance and Authenticity*, [1)]

RFC 8746, *Concise Binary Object Representation (CBOR) Tags for Typed Arrays.*

ECMA-404, *The JSON data interchange syntax,*[2)]

W3C *Extensible Markup Language (XML)*, https://www.w3.org/XML/

ITU BT.500-15, *(05/2023), Methodologies for the subjective assessment of the quality of television images*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardisation at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org

To ensure a correct understanding of the JPEG Trust documentation, this document defines terms and concepts as they are used in this context. In this section, the terms and definitions used are listed in alphabetical order with a reference to their original source wherever applicable.

3.1
assertion
data structure which represents a statement asserted by an actor concerning the media asset

3.2
capacity
maximum amount of information that can be embedded by a watermark on a media asset under preset conditions of robustness and for a given impact on its visual quality.

3.3
disinformation
information that is false and deliberately created to harm a person, social group, organisation or country

[SOURCE: ISO/IEC 21617-1]

3.4
embedding
method to insert certain information (e.g., a watermark) into a media asset.

3.5
extraction
method to extract certain information (e.g., a watermark) that was previously inserted into a media asset.

3.6
generative AI media asset
synthetic media asset
media asset created by means of artificial intelligence (AI) and machine learning (ML)

[SOURCE: ISO/IEC 21617-1]

3.7
imperceptibility
measure of watermark embedding that indicates the similarity between the original (non-watermarked) and watermarked media asset according to human perception.

1) https://c2pa.org/specifications/specifications/2.3/specs/C2PA_Specification.html

2) https://ecma-international.org/publications-and-standards/standards/ecma-404/

© ISO/IEC 2026 – All rights reserved

3.8
intellectual property rights (IPR)
exclusive right of the actor (3.1) to the intellectual work of their creation

[SOURCE: ISO/IEC 21617-1]

3.9
invisible watermark
watermark that is not visible to human perception.

3.10
JPEG 1
common image compression data format and means of reference to ISO/IEC 10918-1:1994

3.11
JUMBF
universal format to embed any type of metadata in any box-based JPEG file format and means of reference to ISO/IEC 19566-5:2023

3.12
mal-information
information that is based on reality, used to inflict harm on a person, social group, organisation or country

[SOURCE: ISO/IEC 21617-1]

3.13
manipulated media asset
manipulated media
media asset that has been changed with the intention to induce misinterpretation

[SOURCE: ISO/IEC 21617-1]

3.14
media asset
digital assets including images, videos, audio or text

[SOURCE: ISO/IEC 21617-1]

3.15
media asset content
portion of a media asset that represents the actual content, such as the pixel data of an image, along with any additional technical metadata required to understand or render the content (e.g., a colour profile or encoding parameters)

[SOURCE: ISO/IEC 21617-1]

3.16
media asset integrity
lack of corruption of a media asset

[SOURCE: ISO/IEC 21617-1]

3.17
media asset metadata
portion of a media asset that represents non-technical information about the media asset or its content, such as location, creator, annotations or IPR information

[SOURCE: ISO/IEC 21617-1]

© ISO/IEC 2026 – All rights reserved

3.18
media asset original
media asset produced by a device or method without any modifications

[SOURCE: ISO/IEC 21617-1]

3.19
media asset provenance
set of information about a media asset, including the trail of modifications starting from an actor

[SOURCE: ISO/IEC 21617-1]

3.20
media asset source
non-human actor that created the media asset original

[SOURCE: ISO/IEC 21617-1]

3.21
misinformation
information that is false but not created with the intention of causing harm

[SOURCE: ISO/IEC 21617-1]

3.22
payload
data carried by the watermark.

3.23
robustness
measures of successful watermark extraction from the media asset, which may or may not have gone through certain processes such as filtering, compression, cropping or modification.

3.24
visible watermark
watermark that is visible to human perception.

3.25
watermark
data that has been encoded for the purposes of embedding into media assets. It may be visible/perceptible or invisible/imperceptible.

3.26
watermark decoding
process of converting the watermark that was extracted from media assets back into its original format.

3.27
watermark encoding
process of converting the watermark into a form suitable for embedding into media assets.

3.28
watermarked media asset
media asset that carries a visible or invisible watermark.

3.29
watermarking
technique that embeds data into a media asset. It also provides the technique to extract the data back from the watermarked media asset.

© ISO/IEC 2026 – All rights reserved