ISO/IEC JTC 1/SC 29/WG1 (ITU-T SG16)

Coding of Still Pictures

JBIG
Joint Bi-level Image Experts Group

JPEG
Joint Photographic Experts Group

TITLE: JPEG Trust White Paper

SOURCE: WG1

EDITORS: Sabrina Caldwell (sabrina.caldwell@anu.edu.au)
Frederik Temmermans (Frederik.Temmermans@vub.be)
Philippe Rixhon (philippe@rixhon.net)

STATUS: Final

REQUESTED ACTION: Publish

DISTRIBUTION: Public

Contact:
ISO/IEC JTC 1/SC 29/WG1 Convener – Prof. Touradj Ebrahimi
EPFL/STI/IEL/GR-EB, Station 11, CH-1015 Lausanne, Switzerland
Tel: +41 21 693 2606, Fax: +41 21 693 7600, E-mail: Touradj.Ebrahimi@epfl.ch
Today's images arise from many sources: digital cameras, film photo scans, photo editing software, artificial intelligence, and combinations thereof. These technological innovations allow us to produce novel new imagery and even new knowledge derived from our media assets, but at the same time, they can confuse and even deceive us. To take advantage of the beneficial outcomes of modern digital media production technologies while lessening the negative outcomes, we need to know if and how we can trust the media we encounter.

To facilitate global interoperable media asset authenticity, JPEG (ISO/IEC JTC 1/SC 29/WG 1) initiated the development of a new international standard: JPEG Trust. JPEG Trust arises from an exploration that started five years ago of requirements for addressing mis- and dis-information in digital media. JPEG Trust provides a comprehensive framework for individuals, organizations, and governing institutions interested in establishing an environment of trust for the media that they use and supporting trust in the media they share online. This framework addresses aspects of provenance, authenticity, integrity, copyright, and identification of assets and stakeholders.

The JPEG Trust framework is built in compliance with well established JPEG standards as well as other widely adopted industry standards to ensure a smooth integration into existing digital media ecosystems. The framework can be integrated into ecosystems that use any of the JPEG family of standards (including JPEG 1, JPEG 2000, JPEG XS, JPEG XL and JPEG AI). In addition, due to its generic nature, many aspects of the framework can also be applied to other image file formats or other media modalities such as video or audio.

**Establishing Trust**

Trustworthiness of media is subjective and dependent on context. JPEG Trust does not explicitly define trustworthiness but rather provides a framework and tools for individuals, organizations, and governing institutions to establish trust in accordance with the conditions they specify. For example, when a photograph of a damaged car is shared among family members, they would not question the veracity of the photograph. However, when this same photograph is shared with an insurance company, additional indicators of authenticity would likely be required. The context-dependent and often subjective nature of trust is accommodated by the JPEG Trust framework.

**The JPEG Trust Framework**

Currently JPEG Trust consists of one part, the Core Foundation (ISO/IEC 21617-1). This foundation handles three main areas:

1. annotating provenance information,
2. extracting and evaluating trust indicators, and
3. handling privacy and security concerns.

The following three sections elaborate upon these aspects in more detail.
Annotating provenance information

JPEG Trust standardizes means to link media assets together with their associated provenance annotations in a tamper-evident manner. The presence or absence of this information provides the contextual information needed for the establishment of trust in the media asset. The model for storing and accessing media asset provenance information is aligned with the industry supported Coalition for Content Provenance and Authenticity (C2PA) specification\(^1\). The C2PA specification defines the technical means for combining statements of fact together with a digital signature. Some of these facts include cryptographic bindings, information about human, non-human, and AI-based actors and the actions (creation, editing, type of editing etc.) that were performed in the creation or modification of the media asset. Hence, existing media assets that have C2PA-compliant provenance information are fully compatible with the JPEG Trust framework. JPEG Trust also adds additional provenance functionality such as signaling the extent of modifications.

Extracting and evaluating trust indicators

The JPEG Trust framework (Figure 1) specifies how to extract an extensive array of Trust Indicators from any given media asset. These indicators can originate from the metadata, the media content or provenance information. Subsequently, specific conditions for trustworthiness, expressed in Trust Profiles, allow individuals, organizations, and governing institutions to evaluate relevant trust indicators according to the requirements for their specific usage scenarios. The resulting evaluation can be expressed in a Trust Report to make the information easily accessed and understood by the end user.

Some examples of Trust Indicators are:

- From the metadata: presence of EXIF metadata or value of any of the EXIF metadata fields.
- From the media content: results of an external AI Generated Content (AIGC) detector, such as the probability that the asset is generated by AI according to this particular algorithm.
- From the provenance information: information about the camera that was used to capture the image and that signed the asset.

\(^1\)https://c2pa.org/specifications/specifications/1.4/index.html
Handling privacy and security concerns

The JPEG Trust framework provides a mechanism to annotate media assets with information about their trustworthiness. In many scenarios, it is important that this information can be protected from exposure. JPEG Trust also provides the means to protect that information using means based on the provisions of JPEG Privacy and Security (ISO/IEC 19566-4). Privacy provisions allow for the protection of information about an image when appropriate. For example it can be used to protect the identity of a field photographer capturing an image in a conflict zone. In this example, the agency distributing the photograph could sign the media asset instead of the photographer. End users would not be able to identify the photographer and it is up to them to decide whether they consider this particular image trustworthy based on the reputation of the agency.

Next steps

The JPEG Trust Part 1 - Core Foundation (ISO/IEC 21617-1) is currently a Draft International Standard and is expected to be published as an International Standard later in 2024. This first part is the starting point of the JPEG Trust framework that will evolve over time and be extended with additional functionalities in the future. Currently the JPEG Committee is working on features to better support media tokenization such as declaration of authorship, ownership and terms of use. In addition a new Part 2 “Trust Profiles Catalogue” was initiated to provide dedicated Trust Profiles for specific common usage scenarios. Finally, reference software is being developed and will be published as a new Part of JPEG Trust in the future.

More information

For the latest information about JPEG Trust and other JPEG activities please regularly consult jpeg.org.

The Joint Photographic Experts Group (JPEG) is a Working Group of ISO/IEC, the International Organisation for Standardization / International Electrotechnical Commission, (ISO/IEC JTC 1/SC 29/WG 1) and of the International Telecommunication Union (ITU-T SG16), responsible for a wide range of standards including the JPEG 1, JPEG 2000, JPEG XS, JPEG Pleno, JPEG XL and JPEG AI families of standards.