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

Coding of Still Pictures

JBIG

Joint Bi-level Image
Experts Group

JPEG

Joint Photographic
Experts Group

TITLE:	Fake Media: the JPEG Stake
SOURCE:	WG 1
PROJECT:	General
STATUS:	
REQUESTED ACTION:	For publication on SC29 and JPEG website
DISTRIBUTION:	Public

Contact:
ISO/IEC JTC 1/SC 29/WG 1 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

Fake Media: the JPEG Stake

Context and Motivation

Recent advances in media manipulation, particularly deep learning based approaches, can produce near realistic media content that is almost indistinguishable from authentic content to the human eye. These developments open opportunities for production of new types of media contents that are useful for the entertainment industry and other business usage, e.g., creation of special effects or artificial natural scene production with actors in the studio. However, this also leads to issues relating to fake media generation defying the integrity of the media (e.g., deepfakes), copyright infringements and defamation to mention some. Misuse of manipulated media can cause social unrest, spread rumours for political gain or encourage hate crimes. In this context, the term 'fake' is used here to refer to any manipulated media, independently of its 'good' or 'bad' intention.

In many application domains, the 'media manipulators' may want to declare the type of manipulations performed, in opposition to other situations where the intention is to 'hide' the mere existence of such manipulations. This is already leading various Governmental organizations to plan new legislation or companies (especially social media platforms or news outlets) to develop mechanisms that would clearly detect and annotate manipulated media contents when they are shared. While growing efforts are noticeable in developing technologies, there is a need to have a standard for the media/metadata format, e.g., a JPEG standard that facilitates a secure and reliable annotation of fake media, both in good faith and malicious usage scenarios. Therefore it is important for the JPEG Committee to better understand the fake media ecosystem and needs in terms of standardization through an in-depth analysis of fake media use cases, naturally independently of the 'intentions'.

Key Capabilities of a Potential Standard

In order to have an in-depth understanding of fake media use case, it is important to identify some of key capabilities that would be required in a potential standard addressing this use case:

- Secure signal if media content has been modified.
- Description of the type of modification, i.e., use of deep learning.

- Indication of the likelihood of modification and corresponding region where it might have been applied.
- Record and protection of metadata information relating to specifics of the modification, i.e. purposes, copyright, etc.
- Identification of the source of the media content.
- Verification of the integrity of the media content.
- Keeping track of the media content changes.

While the above list is non exhaustive and requires further study, it is also important to understand in more depth the usage scenarios which will require input from relevant industries, public bodies (responsible for legislations), technology providers and end-users. Therefore the JPEG committee has the intention to engage with stakeholders in this use case in order to develop a clearly defined roadmap for standardization.

Objectives

It is envisaged that JPEG initiates a standardization activity in order to ensure interoperability between a wide range of applications dealing with fake media. To reach this goal, and as a first step, stakeholders are invited to join this effort by helping to better understand applications and scenarios relevant to fake media use cases. This will allow the JPEG Committee to then identify key requirements for a standard in fake media. Initial findings suggest that a set of standard metadata to signal fake media content along with relevant information on the latter are needed. In addition, standard mechanisms for security and protection of integrity both metadata and fake media content are desired. The latter is closely related to issues highlighted in *media blockchain under progress in the last two years* in JPEG and therefore is considered as a natural continuation of that effort.

Next steps

During its 88th online meeting (July 2020), the JPEG Committee has created a public Ad Hoc Group (AHG) on Fake Media as a first concrete action toward the above mentioned objectives. The mandates of the AHG are to:

- Collect fake media use cases and requirements.
- Survey on relevant industry and government initiatives.
- Engage with stakeholders and attract them to contribute.
- Define an action plan.

resulting in the following deliverables:

- Initial use cases and requirements
- List of relevant initiatives
- Action plan

Interested parties are invited to join the above AHG through the following URL: http://listregistration.jpeg.org.