Exploration of media block chain technologies for JPEG privacy and security

Temmermans, Frederik, Bhowmik, Deepayan, Pereira, Fernando, Ebrahimi, Touradj, Schelkens, Peter

Frederik Temmermans, Deepayan Bhowmik, Fernando Pereira, Touradj Ebrahimi, Peter Schelkens, "Exploration of media block chain technologies for JPEG privacy and security," Proc. SPIE 11353, Optics, Photonics and Digital Technologies for Imaging Applications VI, 113530U (13 April 2020); doi: https://doi.org/10.1117/12.2556684

SPIE.

Event: SPIE Photonics Europe, 2020, Online Only, France

Exploration of Media Blockchain Technologies for JPEG Privacy and Security

Frederik Temmermans*[a,b], Deepayan Bhowmik[c], Fernando Pereira[d], Touradj Ebrahimi[e], Peter Schelkens[a,b]

[a]Department of Electronics and Informatics (ETRO), Vrije Universiteit Brussel, Pleinlaan 2, 1050 Brussels, Belgium; [b]imec, Kapeldreef 75, 3001 Leuven, Belgium; [c]University of Stirling, United Kingdom; [d]Instituto Superior Técnico - Instituto de Telecomunicações, Lisboa, Portugal; [e]Ecole Polytechnique Fédérale de Lausanne (EPFL), Switzerland

ABSTRACT

The need for efficient, widespread and reliable security and user privacy technologies is important more so than ever before. This is in particular crucial for workflows involving image data. Images can be easily edited to give a false impression of reality, leading to the growing challenges in the spread of fake news. But images are also creative works that are subject to copyright and integrity verification. Therefore, the ability to prove when, where or how a specific image was captured and tracing it through its workflow is crucial. To provide an answer to the above-mentioned challenges, the JPEG Committee has been working on a standard called JPEG Privacy and Security. In addition, more recently, the JPEG Committee has initiated an exploration activity to identify the needs for standardization in the realm of media blockchain applications. This paper presents the scope and implementation of the JPEG Privacy and Security standard and introduces the current state of the exploration study on standardization needs for media blockchain applications.

Keywords: privacy, security, copyright, integrity, fake news, blockchain, Distributed Ledger Technologies, DLT, media, image, JPEG, standardization

1. INTRODUCTION

Privacy and security, copyright violations and fake news are emerging challenges in digital media. Social media and data leaks increase the risk of user privacy violations [1]. Creative media, particularly images, are often susceptible to copyright violations which poses a serious problem to the media industry [2][3]. On the other hand, doctored images using photo editing tools and computer-generated components may give a false impression of reality and add to the problem of fake news. These problems demand solutions to protect images and associated metadata as well as methods that can prove the integrity of digital media. For these reasons, the JPEG Standardization Committee has been working on a new set of specifications called « JPEG Privacy and Security » that provides solutions to support privacy and security focused workflows. This standard defines tools to support protection or ownership rivets and integrity verification across a wide range of JPEG standards. Related to image integrity, blockchain technology has shown good potential to design solutions for creating tamper proof distributed ledgers. However, adopting blockchain technologies for digital image integrity verification poses several challenges at technological as well as at privacy related legislation levels. In addition, if blockchain technology is adopted to support media applications, it needs to be closely integrated with widely adopted standards to ensure broad interoperability. Therefore, the JPEG Committee has initiated an activity to identify standardization needs related to media blockchain and distributed ledger technologies (DLT). This paper presents the scope and implementation of the JPEG Privacy and Security standard and introduces the current state of the exploration study on standardization needs related to media blockchain applications.

[*] ftemmerm@etrovub.be

Optics, Photonics and Digital Technologies for Imaging Applications VI, edited by
Peter Schelkens, Tomasz Kozacki, Proc. of SPIE Vol. 11353, 113530U · © 2020 SPIE
CCC code: 0277-786X/20/$21 · doi: 10.1117/12.2556684

2. JPEG PRIVACY AND SECURITY

2.1 Background and context

JPEG Privacy and Security is a standard defined by JPEG (ISO/IEC JTC1 SC29 WG1). More specifically, it is Part 4 of the so-called JPEG Systems standard (ISO/IEC 19566-4). JPEG Systems defines a suite of specifications that provide additional functionalities in imaging workflows, independent of the underlying image coding solution used. Practically, this means that the functionalities can be adopted with all JPEG image coding standards, including the legacy JPEG, JPEG 2000, JPEG XR, JPEG XT, JPEG XS and the upcoming JPEG XL standards. In addition to the privacy and security features, JPEG Systems also defines tools to embed metadata (Part 5), 360 support (Part 6) and linked images or image sets (Part 7). Other system level extensions might be added in the future. Activities on JPEG Privacy and Security standard started in 2015 with the organization of several workshops to collect use cases and requirements from stakeholders [5][6][7][8]. Based on the outcome of these workshops, a call for proposals was issued in April 2017 [9]. Several responses were received that ultimately led to the JPEG Privacy and Security International Standard, which is expected to be published in April 2020.

The JPEG Privacy and Security standard focuses on two main sets of features related to protection and authenticity. For protection, the standard supports tools to protect (encrypt) parts of images and/or associated metadata. This is done in such a way that backward and forward compatibility are retained. In practice, this means a legacy decoder will not be able to decode the protected information, but it will still be able to process and to render the file as a normal image. Access control can be managed independently for various regions in the image or various metadata instances. For authenticity, the standard mainly focuses on the use of signatures or hashes to check integrity. Again, this can be done for specific image regions and for associated metadata, independently. This enables functionalities such as identification and assessment of the master file, tracking of changes and provenance, versioning control, etc.

2.2 Standardization approach

While many of these functionalities could already be implemented by stakeholders independently, the aim of the JPEG Privacy and Security standard is to provide a framework capable of supporting protection and authenticity workflows in a standardized way. Hence, existing technologies are adopted where possible. For example, the JPEG Privacy and Security standard does not define any new encryption algorithms. Rather, it focuses on the signaling syntax to embed encrypted information in JPEG files. To this end, the standard focuses on the definition of generic boxes. While most JPEG standards use box-based file formats, this is not the case for the legacy JPEG format, which supports extensions via APP marker segments. APP marker segments are chunks of data (limited to 64Kb) that are skipped by a decoder if it cannot interpret the embedded information. JPEG XT defines a file format to wrap boxes in one or more APP11 marker segments [4]. Hence, the JPEG Privacy and Security standard and other system level extensions can focus on the definition of boxes and adopt the JPEG XT file format for compatibility with the JPEG image coding standard. Metadata based functionalities, such as embedding access rules or provenance information, adopt the JPEG Universal Metadata Box Format (JUMBF). JUMBF is Part 5 of the JPEG Systems standard and provides a universal mechanism to embed any type of metadata (textual or binary) in images coded with JPEG standards. In addition, it adds functionalities such as referencing between metadata instances and image data, and a URI scheme for references and requests.

2.3 Protection functionalities

Protection of image content and/or metadata is supported by two boxes: the Protection box and the Replacement box. Both are detailed in the following subsections. In practice most use cases will combine both boxes. A usage example is given in subsection 2.3.3.

2.3.1 The Protection box

To support protection, the JPEG Privacy and Security standard defines a (JUMBF) Protection box. This box wraps encrypted information and signals additional information such as the used encryption algorithm and access rules. Legacy decoders will not recognize this box and hence will skip it entirely. Updated decoders can act in two ways depending on the scenario. If the used encryption method is unknown, or if the user doesn't have access rights, the entire box will be ignored. If the content can be decrypted, the entire Protection box is replaced with the decrypted content. This implies that the protected content should be a box or APP marker segment (or sequence of them) to make sure that the resulting file is still valid. The resulting file is then decoded as usual, this flow is illustrated in Figure 1. In many scenarios, the Protection box will not be used on its own but rather in combination with other boxes. More specifically, many use cases will combine the Protection and Replacement boxes. The latter is detailed in the next section.

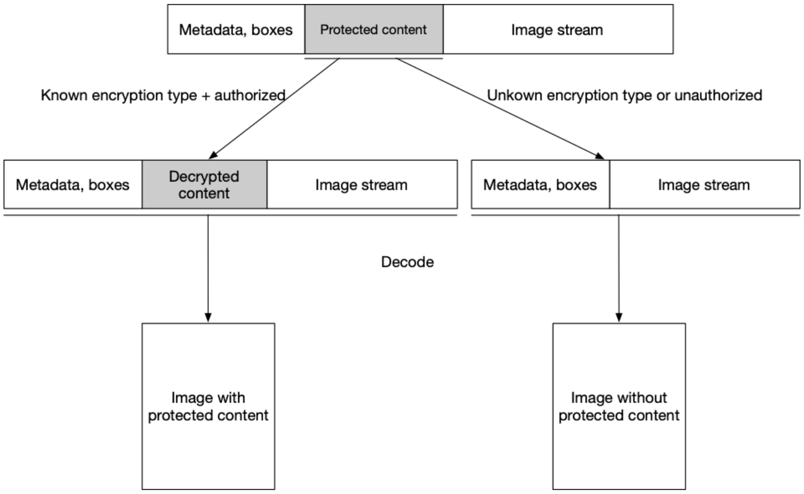
Metadata, boxes
Protected content
Image stream
Known encryption type + authorized
Unkown encryption type or unauthorized
Metadata, boxes
Decrypted content
Image stream
Metadata, boxes
Image stream
Decode
Image with protected content
Image without protected content

Figure 1. Decoding process for image files that embed protected content.

2.3.2 The Replacement box

In many protection use cases, there are two versions of certain information, a public and a private (protected) version. Some metadata such as location and timestamp might be removed from a public metadata instance but present in a private instance. In these cases, the private content replaces the public content for authorized users. This is exactly the idea of the "Replacements" concept in the JPEG Privacy and Security standard: some content is - under certain circumstances - replaced with other content. The Replacement can be protected in order to make it only accessible to privileged users. Similarly to protected content, replacements are embedded in an image as a JUMBF box, more precisely a JUMBF Replacement box. A replacement signals that some content in the file should be replaced with the content embedded in the Replacement box. Multiple types of replacements are supported:

- **Box type**: an entire box is replaced with the embedded content. The box that will be replaced can be referenced with a JUMBF reference or by its position in the file.
- **APP type**: an APP marker segment is replaced. The segment that will be replaced is referenced by its position in the file. This type can be used, for example to replace EXIF metadata in legacy JPEG images.
- **ROI type**: a region of interest in the image is replaced with the embedded image stream. In addition to the image stream also the target coordinates are signaled. In this case, both image streams should be decoded prior to executing the insertion of the region of interest.
- **File type**: the entire file is replaced with the embedded file. An example use case is the scenario where a low-resolution version of an image is replaced with a high resolution version.

Figure 2 gives an overview of the different replacement types and decoding flows.

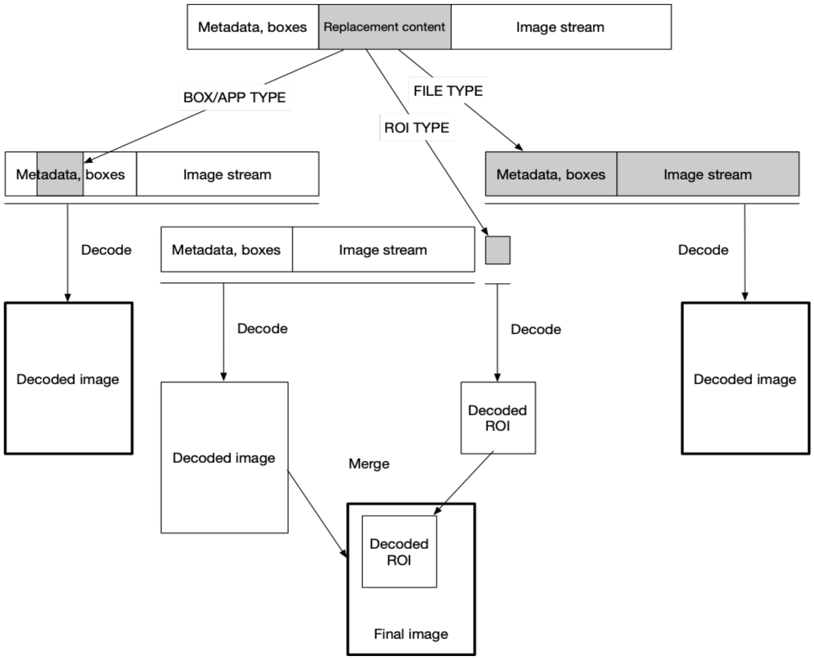

Figure 2. Overview of the different replacement types and decoding flows.

2.3.3 Protection usage example

As mentioned before, in practice, many use cases will combine the protection and replacement tools. Figure 3 illustrates the process to protect a region of interest of an image such as a face. In the image stream of the master file, the face has been replaced with a placeholder, in this example a smiley face. This is the public image that will be rendered by legacy decoders or shown to unauthorized users. The original region of interest is wrapped in a Replacement box along with its positioning information in the master image. In its turn, the Replacement box is encrypted and wrapped in a Protection box. A decoder with correct authorization rights will first decrypt the content of the Protection box. The result is a Replacement box which replaces the Protection box. Finally, the region of interest embedded in the Replacement box is inserted in the master image and the result is then rendered to the user.

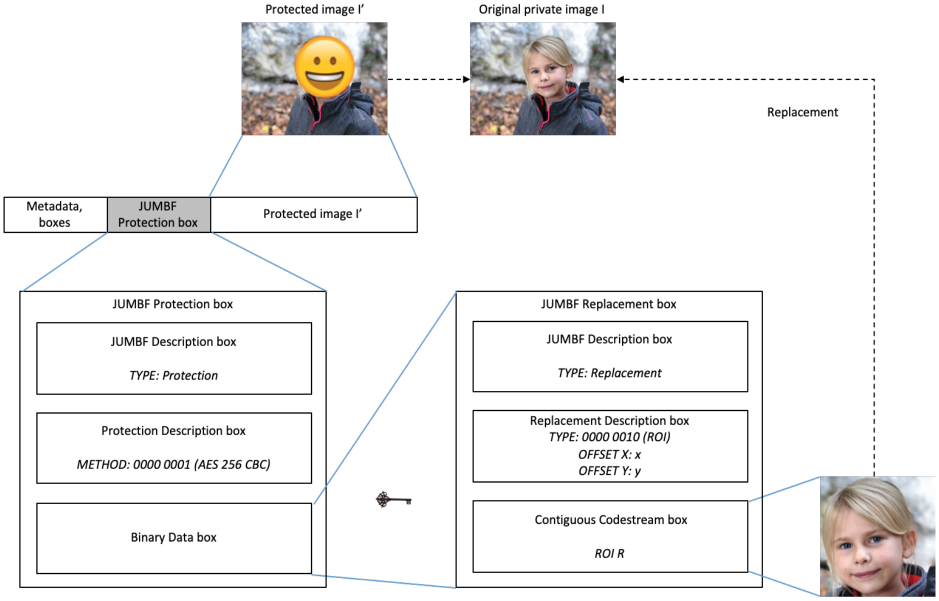

Figure 3. Example structure of an image containing a protected region of interest.

2.4 Authenticity functionalities

Many use cases related to authenticity and integrity rely on the usage of signatures or checksums to validate if the content is authentic or untouched. To this end, JPEG Privacy and Security builds again on the JPEG builds on JUMBF. JUMBF allows to embed a SHA-256 checksum to validate embedded content such as metadata instances or image regions. However, since a checksum could be updated along with the associated content, there is always a need for an additional validation mechanism. For example, encryption techniques, invisible watermarking or a registration authority can be used. Unfortunately, all of these have their specific drawbacks. For example, even though invisible watermarking techniques are invisible to the human eye, they still make modifications to the original image content. Registration authorities provide a great alternative, but the implication is that the user relies on a third party. This is exactly the issue that could be resolved by adopting blockchain technology. For that reason, in January 2018, the JPEG committee initiated a new activity to explore the usage of blockchain and distributed ledger technologies in a media context.

3. MEDIA BLOCKCHAIN

3.1 Background and context

Media distribution through online platforms is the de facto solution recently and a popular form of interaction amongst Internet users, whether from a social or financial perspective. As discussed earlier, protecting intellectual property rights (IPR) is crucial in digital distribution as copying, doctoring and redistributing any content is far easier due to the availability of large and cheap storage, sophisticated content editing software, and broadband networks. While this is important since the amount of illegally consumed material without authorization is rising, it is increasingly difficult for any user to discern if the media was edited or doctored and if so by whom. Hence, a mechanism to distribute media in a transparent way is required with the functionality to protect content’s integrity.

Blockchain and distributed ledger technologies (DLT) have recently gained popularity outside the financial market and cryptocurrency as they offer a means of executing permanent, secure transactions. Application of blockchain in the media and entertainment industry have also attracted serious interest, especially for trusted content distribution and digital rights management. In this context, it was natural that the JPEG committee initiated an activity to explore and to identify standardization needs with regards to media blockchain and distributed ledger technologies.

A blockchain is a distributed ledger of blocks that make use of peer-to-peer transmissions and provides a platform to record and share data in a distributed manner [10]. The platform itself is a combination of decentralized networks, meaning no central organizations oversee or process transactions. This is important, as it implies that no organization can claim ownership of the blockchain network, thus offering full trust and transparency. The concept was first introduced by one or more anonymous authors using the pseudonym Satoshi Nakamoto in 2008 during the development of Bitcoin [11]. Blockchain contains a particular type of data structure that allows data storage and transmission in the form of blocks, linked to each other in a digital chain. It facilitates the use of cryptographic and algorithmic methods to record and synchronize data across all participating nodes in the network in an immutable manner. This is important to make any transaction, such as media distribution, to remain transparent and trustable.

A number of applications areas outside cryptocurrency have emerged in the recent past that use blockchain as their core infrastructure. These applications include financial management, healthcare, government and public sector (e.g., taxes, voting, land registry, intellectual property management etc.), manufacturing, energy, retail, supply chain management, etc. Media and entertainment domain have also identified new applications that use blockchain as their core technology offering solutions to existing problems, particularly related to copyright and authentication as indicated in the previous sections. For example, Fujimura et al. [12] proposed to add the copyright information as part of the blockchain transaction. A multimedia blockchain framework was proposed [13] that keeps all records of the media transactions (e.g., ownership, licenses etc.) and offers a mechanism for tamper-proof verifiable integrity of the media enhancing trust among stakeholders. In addition, a number of industry-led initiatives, mostly in form of software as service, have surfaced that leverage blockchain as their core infrastructure to provide solutions to the media and entertainment sector. Therefore, it was a sensible move for the JPEG committee to explore this space and identify the standardization needs. In this paper, selected solutions and use cases are presented to allow better understanding of the scope and requirements for a potential future standard.

3.2 Selected examples of media blockchain solutions

This section presents selected examples solutions in the current media and entertainment industry that use blockchain as underlying technology. These solutions largely aim to address some of the challenges relating to multimedia distribution and digital rights management.

3.2.1 KODAKOne and KODAKCoin

One of the first industry entrants in media blockchain has been KODAKOne [14]. It introduced a blockchain based platform for digital rights management for photographers which also helped them to post licensing terms and conditions. This platform claimed to address the issue through post licensing when images are being used without permission. KODAKCoin, a cryptocurrency used in this solution, was a photo-centric cryptocurrency aimed at empowering photographers and agencies who target to take greater control in image rights management using blockchain technology.

3.2.2 Multimedia blockchain framework

Bhowmik and Feng [13] proposed a blockchain based framework to facilitate tamper proof distribution of media assets. This framework allows to preserve copyright related information within the blockchain whereas a self-embedding watermarking algorithm allows the detection of any tampering with the media asset in question. The framework claims to be important to many application areas and stakeholders in the creative industry including digital archives and GLAM services (galleries, libraries, archives, and museums) to identify misinformation, and preserve valuable artwork and its digital rights.

3.2.3 IBM blockchain for accountability in media and entertainment

IBM explores a blockchain infrastructure, targeting the media and entertainment (M&E) industry for three specific goals [15]: a) more effective media asset management; b) controlled copyright management to reduce disputes; and c) advertisement fraud reduction. IBM teamed up with Mediaocean to create a blockchain based media supply chain for the advertisement industry. This framework is intended to offer accountability in the advertisement industry and combines smart contracts in the ad ecosystem.

3.2.4 eWitness: media authentication for evidentiary purposes

While the examples above are heavily biased towards copyright management tasks, eWitness [16] intends to make use of blockchain for authentication, targeting evidentiary purposes. The idea is to register any digital media taken from smart phones and cameras, following a hash or signature of the same media along with its EXIF metadata to be registered through an Ethereum based blockchain infrastructure. It is claimed to provide the provenance and an authentication mechanism to create trust and detect fake/doctored media for journalists, civil liberty units and other similar non-government/government entities.

3.2.5 Privacy-preserving photo sharing using blockchain

Sharing photos online has become an extremely popular activity, raising a wide concern on privacy issues related to the shared content. ProShare, is a photo-sharing solution similar to Instagram that addresses some of the privacy issues often encountered in social media by relying on a trusted third party different from the sharing platform operator [17]. However, depending on a central authority requires users to blindly trust it and is a single point of failure. While the original architecture in ProShare relied on a central server that behaved as a semi-trusted intermediary between the owner of a picture and the recipient with whom the original picture is shared, those characteristics are vulnerabilities that can compromise user privacy. Features of blockchain technology can be used to transform ProShare in a purely peer-to-peer and decentralized privacy-preserving system. Recently, ProShare architecture has been extended to accommodate a blockchain and hence eliminate the need for a trusted third-party in the sharing process between sender and recipient [18].

3.2.6 Other example solutions

Other example solutions include Current [19] which is an incentivized media blockchain ecosystem and allows incentives to its user, or Po.et [20] which proposes a decentralized protocol for content ownership, discovery and monetization in media through its blockchain framework. While there are other examples emerging frequently, the JPEG committee found these examples to offer valuable insight for further exploration towards a potential future media blockchain standard.

4. JPEG EXPLORATION ON MEDIA BLOCKCHAIN

From the inception in January 2018, the JPEG Committee, through an Ad-hoc Group (AhG), has explored the potential of media blockchain in consultation with industrial, academics and other stakeholders through discussions and a series of four workshops during the JPEG standardization meetings. A white paper [21] on media blockchain and distributed ledger technologies captured and analyzed these discussions and the outcome of the workshops and made recommendations for further work within the scope of JPEG standardization activity. Evidence suggested that media contents are increasingly managed on blockchain and DLTs and therefore the issue of interoperability, tracking and exchange of such contents become important and could be addressed by the JPEG Committee. Additionally, the Committee is also engaged with other standardization groups, notably ISO/TC307 Blockchain and Distributed Ledger Technologies [22], to complement the activities in media related applications and to better respond to media specific needs.

4.1 Use cases

Selected solutions that are discussed in the earlier section provide a better understanding of such scenarios. Based on a critical evaluation of the existing solutions, two main categories of potential requirements were identified: a) means to enable trust, privacy and security in the media consumption chain and b) provisions to empower transparent and trusted media distribution ecosystem in the creative sector. The first category advocates that the media blockchain can provide an efficient solution to issues related to trust, privacy and security in the consumption chain, while the latter proposes the media blockchain can provide a transparent and trusted media distribution ecosystem empowering creative content creators or publishers. Along with these two categories four user groups have also been identified: a) content creators; b) publishers; c) consumers; and d) digital archives. Example use case scenarios are envisaged in constructing a set of potential requirements for JPEG explorations on media blockchain:

- **Pictures without permissions**: Content creators, e.g., photographers, photojournalists/bloggers, or fashion photographers create content that has potential for monetization. Once appeared online (a legitimate version), other users potentially use that content for their own purposes (commercial or free posts) without endorsing the creator of the original content.
- **Authentication and integrity verification for forensic evidence**: Easy availability of sophisticated image editing software makes it possible for anyone to doctor the content or tamper evidence. Scenarios of such usage include a) crime scene evidence tampering; b) spreading of fake news/misinformation through social media for spreading hatred, terrorism, scaremongering or gaining political advantages; or c) tampering surveillance footages that have potential use for legal purposes.
- **Advertisement fraud and advertisement copyright infringement**: Ad frauds are a major concern and therefore considered as a potential use case. The scenarios include: 1) advertising platforms restrict advertisement performance data to advertisers and hence can falsify the data to their customer and 2) fraudsters simulate clicks, mouse activity and fake social network accounts using bots to inflate the numbers.
- **Security of medical image content**: Medical images are crucial and confidential assets for national health trusts or any clinic. Thus, security and reliability of such content at large scale is important for fundamental patient needs, legal purposes and protection from cyber-attacks.
- **Authenticity and copyright protection in the GLAM sector**: The Galleries, Libraries, Archives and Museums, often known as GLAM, deal with a large amount of digital content. GLAM services face issues related to intellectual property rights (IPR) for access and usage control to authenticity including fake images and tampering.
- **Content ownership and monetization**: Content creators and publishers both like to manage their digital rights and licensing information in a reliable way to avoid fraudulent activities. It also expects a mechanism for easy and flexible exchange of licensing agreement with the end user. Both the publishers and creators may have an archive of existing content and like to reach out to larger audiences and monetize in an automated way.
- **Collaborative work environments / Stakeholder recognition**: Commercial artworks or professional media content often involve various stakeholders, e.g., photographer, scene writer, models, makeup artists, designers, post processing experts, distributor, publishers, etc. Often their contributions are not recognized once the content is distributed. In this scenario, the stakeholders desire to claim royalty in the form of micropayment (such as bitcoin) and/or be recognized.

- **Provenance / Copyright verification**: End user wants to verify the provenance, copyright or ownership before making a purchase / licensing.

4.2 Requirements

The use cases, in fact, aid the JPEG Committee to develop a list of requirements for a potential media blockchain standard. As mentioned in the previous subsection, the requirements are divided into two main categories. These are further expanded using a range of fine-grained categories, such as:

- **Digital rights management**: The standard shall provide mechanisms to create and manage rights of media assets through blockchain. This shall ensure to generate and maintain digital rights of the asset at a global scale conforming laws of the land. This includes certificate/license generation, distributions and management.
- **Copyright protection**: The standard shall provide provisions to securely preserve copyrights information.
- **Integrity**: The standard shall provide mechanisms to verify the integrity of the media in question.
- **Authenticity**: The standard shall provide means to support source verification and ownership authentication.
- **Traceability**: The standard shall provide a mechanism to trace the modifications and involve stakeholders or identify sources of piracy.
- **Privacy compliance**: The standard shall provide means to comply with privacy laws.
- **Asset distribution and monetization**: The standard should envisage the need for tools that can cater for seamless asset distribution and monetization, manage smart contracts, content versioning and micropayments.

While the JPEG Committee considers a media blockchain may provide a comprehensive solution to support the identified requirements, it is important to define the scope in a disciplined manner to identify the core technologies for a holistic JPEG Privacy and Security standard.

4.3 JPEG activities in media blockchain

Past and current activities within the JPEG exploration on media blockchain include a) engagement with relevant stakeholders, b) collection of diversified use cases and industry applications, c) in-depth assessment of the collected use cases to identify the key features of the media blockchain, both from business and technical perspectives, d) defining the requirements for a potential standard and c) initiating the standardization process. At the time of writing of this paper, the Committee has identified a diversified set of use cases and related requirements which are planned to be published during the next Committee meeting in April 2020. It is anticipated that some of these requirements are already addressed in the existing JPEG standards, such as within the JPEG Privacy and Security, some will be outside the scope of JPEG remit and rest will require a new standard to be developed. However, a standardization of media blockchain will pose technical challenges which the Committee is keen to explore further. While it is still under the exploration stage, it is also envisaged that a formal call for proposals may be issued, should there be justifiable requirements to be addressed by JPEG.

5. CONCLUSIONS AND NEXT STEPS

The JPEG Privacy and Security standard provides a set of tools to protect image content and metadata as well as tools to support image authenticity, integrity, copyright and provenance workflows. Blockchain and distributed ledgers are promising technologies that can provide solutions to several challenges in media applications, including avoiding dependence on third party registration authorities. However, applications of blockchains in a multimedia context also come with several challenges that need to be addressed and efficiently resolved. Therefore, the JPEG Committee has started an exploration activity on standardization needs related to media blockchain. This paper discussed the scope and implementation of the JPEG Privacy and Security standard and presented the current state of the blockchain exploration activity, notably a number of illustrative use cases and their corresponding requirements. The JPEG Committee continues to publicly disseminate these use cases and their requirements to further refine them based on community feedback. Thereafter, a decision will be made on the standardization steps. This might include extending existing JPEG standards such as the JPEG Privacy and Security specifications, defining new JPEG standards and/or making suggestions to other standardization committees that are more focused on the core blockchain and distributed ledger technologies.

REFERENCES

[1] M. Smith, C. Szongott, B. Henne and G. von Voigt, "Big data privacy issues in public social media, 6th IEEE International Conference on Digital Ecosystems and Technologies (DEST), Campione d'Italia (2012).

[2] Frederik Temmermans, Fred Truyen, Ann Dooms, Peter Schelkens, Bruno Vandermeulen, "Integrity of Still Images", Image and Research (2018).

[3] Frederik Temmermans, Touradj Ebrahimi, Siegfried Foessel, Jaime Delgado, Takaaki Ishikawa, Ambarish Natu and Peter Schelkens, "JPEG Privacy and Security framework for social networking and GLAM services", EURASIP Journal on Image and Video Processing, 2017, 68 (2017).

[4] Thomas Richter, Alessandro Artusi, Touradj Ebrahimi, "JPEG XT: A new family of JPEG backward-compatible standards", IEEE Multimedia Magazine, Issue of July/Sept 2016.

[5] "1st JPEG Workshop on Media Blockchain Proceedings", ISO/IEC JTC1/SC29/WG1, wg1n81033, Vancouver, Canada, October 16th, 2018.

[6] "2nd JPEG Workshop on Media Blockchain Proceedings", ISO/IEC JTC1/SC29/WG1, wg1n82017, Lisbon, Portugal, January 22nd, 2019.

[7] "3rd JPEG Workshop on Media Blockchain Proceedings", ISO/IEC JTC1/SC29/WG1, wg1n83044, Geneva, Switzerland, March 20th, 2019.

[8] "4th JPEG Workshop on Media Blockchain Proceedings", ISO/IEC JTC1/SC29/WG1, wg1n84024, Brussels, Belgium, July 16th, 2019.

[9] "Privacy and Security Final Call for Proposals", ISO/IEC JTC1/SC29/WG1, wg1n75035, 2017.

[10] Natarajan, H., Krause, S., & Gradstein, H. "Distributed ledger technology and blockchain", World Bank, 2017.

[11] Nakamoto, S. (2019). Bitcoin: A peer-to-peer electronic cash system. Manubot.

[12] S. Fujimura, H. Watanabe, A. Nakadaira, T. Yamada, A. Akutsu and J. J. Kishigami, "BRIGHT: A concept for a decentralized rights management system based on blockchain," in IEEE 5th International Conference on Consumer Electronics - Berlin (ICCE-Berlin), Berlin, 2015.

[13] Bhowmik, D., & Feng, T. (2017, August). The multimedia blockchain: A distributed and tamper-proof media transaction framework. In 22nd International Conference on Digital Signal Processing (DSP) (pp. 1-5). IEEE.

[14] KODAKOne | Image Rights Management Platform, WENN Digital Inc., [Online]. Available: https://kodakone.com/. [Accessed 20 February 2020].

[15] Enforcing accountability in media | How blockchain technology can work for media and entertainment, IBM, [Online] https://www.ibm.com/downloads/cas/6146Z4JE. [Accessed 20 February 2020].

[16] eWitness: Seeing Can Be Believing Again, CUNY Academic Commons, [Online]. Available: https://ewitness.commons.gc.cuny.edu/. [Accessed 20 February 2020].

[17] L. Yuan; D. Mc Nally; A. Küpçü; T. Ebrahimi, "Privacy-Preserving Photo Sharing based on a Public Key Infrastructure", Applications Of Digital Image Processing XXXVIII, August 2016.

[18] P. Pfister, T. Ebrahimi, "Privacy-preserving photo sharing based on blockchain", Applications of Digital Image Processing XLIII, August 2020.

[19] An Incentivized Blockchain Enabled Multimedia Ecosystem, Current Inc., [Online]. Available: https://cdn.current.us/whitepaper.pdf. [Accessed 20 February 2020].

[20] The decentralized protocol for content ownership, discovery and monetization in media, po.et, [Online]. Available: https://www.po.et/. [Accessed 20 February 2020].

[21] "JPEG White paper: Towards a Standardized Framework for Media Blockchain and Distributed Ledger Technologies", ISO/IEC JTC1/SC29/WG1, wg1n84038, 2019.

[22] ISO/TC 307 Blockchain and distributed ledger technologies, ISO, [Online]. Available: https://www.iso.org/committee/6266604.html. [Accessed 20 February 2020].