Temmermans *et al. EURASIP Journal on Image and Video Processing* (2017) 2017:68
DOI 10.1186/s13640-017-0216-z

EURASIP Journal on Image and Video Processing

REVIEW Open Access

JPEG Privacy and Security framework for social networking and GLAM services

Frederik Temmermans[1,2*], Touradj Ebrahimi[3], Siegfried Foessel[4], Jaime Delgado[5], Takaaki Ishikawa[6], Ambarish Natu[7] and Peter Schelkens[2,1]

Abstract

Current image coding standards provide limited support for privacy and security features. An exception is the JPSEC standard, which defines security extensions in JPEG 2000 specifications (part 8). Notwithstanding this shortcoming, the JPEG committee is currently defining a new JPEG Systems standard, which envisages privacy and security support across JPEG family of standards. In this manuscript, the main philosophy of this emerging specification is outlined along with typical use cases, main requirements as well as examples of potential technological solutions. The upcoming specification guarantees backward and forward compatibility with earlier standards and legacy implementations. Finally, we illustrate the introduced framework by two applications targeting secure photo sharing on social networks and IPR management in the GLAM sector.

Keywords: Image security, Image privacy, JPEG, JPEG 2000, JPSEC, JPEG Systems, Image coding, Encryption, Intellectual property rights, Social media, Ephemeral photo sharing, GLAM

1 Review

1.1 Introduction

In social networks, the widespread use of smart mobile devices with high-resolution cameras and user-friendly applications have made photo sharing an easy and therefore popular activity. Though almost all existing social networking services provide photo sharing capabilities, most of them lack a sound scheme to protect their users' privacy. A photo —'worth a thousand words' — contains a great amount of potentially privacy sensitive information both in the image data and in its associated metadata. Moreover, photos shared on online social networks can be accessed and commented easily and quickly by people and content analysis algorithms, resulting in most photos being tagged with additional information potentially disclosing further privacy sensitive information such as identification data.

Professional organizations, as those in the GLAM (Galleries, Libraries, Archives and Museums) sector, deal with a huge number of digital images and confronted with additional problems. In many cases, those images have associated IPR (Intellectual Property Rights), implying that their access and usage should be controlled. In this particular case, the challenge is focused on the fact that access to images needs to be controlled based on specific privacy policies or rules, as well as IPR conditions. Therefore, mechanisms are needed to both specify the policies and to enforce them.

Unfortunately, few structural solutions have been devised so far that can be deployed in an interoperable way such that privacy and security can be guaranteed and deployed in legacy image processing applications without breaking existing workflow. Particularly, signalling syntax needs to be provided that enables the communication and protection of privacy and security sensitive parts in the image data.

The majority of images exchanged nowadays on digital communication channels are in JPEG format defined by the Joint Photographic Experts Group (JPEG). JPEG activities are carried out within a Working Group under a Joint Technical Committee formed by the International Standardization Organization (ISO) and the International Electrotechnical Committee (IEC), formally known as

*Correspondence: ftemmerm@etrovub.be
[1]Imec, Kapeldreef 75, B-3001 Leuven, Belgium
[2]Vrije Universiteit Brussel (VUB), Department of Electronics and Informatics (ETRO), Pleinlaan 2, 1050 Brussels, Belgium
Full list of author information is available at the end of the article

ISO/IEC JTC 1/SC 29/WG 1 [1]. In this committee, standards are often defined in collaboration with the International Telecommunication Union. Prominent examples are the JPEG-1 (ISO/IEC 10918-1|ITU-T Recommendation T.81) and JPEG 2000 (ISO/IEC 15444-1 |ITU-T Recommendation T.800) standards [2]. More recently, standards addressing particular application domains such as high dynamic range imaging and low complexity, low latency coding have been defined, respectively, JPEG XT (ISO/IEC 18477) and JPEG XS (ISO/IEC 21122). The JPEG committee is currently seeking for solutions to embed support for privacy and security functionality in all its standards.

The remainder of this paper is organized as follows: Section 1.2 outlines a few use cases focused on social network and photo sharing, ephemeral photo sharing and IPR signalling for the GLAM sector. Section 1.3 discusses the scope of the JPEG Privacy and Security standardization framework, and Section 1.4 details JPEG Systems philosophy and technology in which the aforementioned framework will be integrated. Next, Section 1.5 illustrates the core principles of this framework in a secure transmorphing application and an IPR policy management service for the GLAM sector. Finally, conclusions are formulated in Section 2.

1.2 Privacy and Security use cases in image workflows

System-level and generic support for privacy and security protection features are of utmost importance for use cases ranging from image workflows such as image repositories with controlled access, publication and image annotation, medical imaging, privacy preserving search, video surveillance, social networking and photo sharing, ephemeral photo sharing, forensic image analysis, to countering terrorism [3].

As illustrated, some prominent use cases relevant in the scope of this special issue are highlighted in the following paragraphs, allowing for the identification of privacy and security requirements.

1.2.1 Social networking and photo sharing

Online social networking environments are sophisticated platforms connecting a large number of users and hence enabling complex social interactions. Information travels extremely fast on these networks, and therefore, they give rise to problematic privacy concerns. Proliferation of smart mobile devices with high-resolution cameras and user-friendly social network applications makes photo sharing an easy and therefore popular activity. Photos can potentially disclose a significant amount of privacy sensitive information, not only contained in the image data as such but also in the associated metadata. Moreover, on online social networking environments, shared photos can be accessed and commented or tagged easily by people as well as content analysis algorithms, potentially disclosing or enabling the disclosure of even more privacy-related information. Furthermore, this Personally Identifiable Information (PII) [4] may cause additional security issues in particular applications.

Almost all existing social networking services provide photo sharing capabilities, but most of them lack efficient privacy protection solutions for their users. After the reports of citizens being monitored by potential employers or governmental agencies and leakage of sensitive private photos online, people's concern about their online privacy is growing and a solution that would allow for access policy control and distribution is becoming highly desirable.

1.2.2 Ephemeral photo sharing

The enormous success of smart mobile devices has made communication between people extremely easy and fast. In particular, photo sharing raises much more privacy concerns — as indicated in the previous section — than that of traditional texts as a photo can contain or reveal rich privacy sensitive information.

Ephemeral information sharing, especially photo sharing, which allows a user to share photos in an ephemeral way choosing to have the photos disappear after a preset interval, has become increasingly popular. Users can preconfigure an interval during which other friends can access the original or cleared versions of their shared photo. In another scenario, a user can revoke the access right of certain users to a shared photo at any time as he or she prefers. Examples of such applications include the most famous Snapchat [5], Yovo [6], Privately [7] and Dstrux [8]. However, most current solutions to ephemeral photo sharing rely on a secure server to store the original image data and to enforce the access control. It would be very useful if image file formats could incorporate the ability of dynamic access control to image data such that any device and application can easily apply it as a solution for ephemeral photo sharing.

1.2.3 GLAM sector

The GLAM (Galleries, Libraries, Archives and Museums) sector often deals with high-value digital art reproductions. In this domain, it is crucial that such artefacts can be protected, both in an active as well as in a passive way. For example, correct IPR signalling is paramount. It is a common practice to embed IPR information within the image metadata. However, currently, the information is not always embedded in a uniform way. This situation makes it complicated for applications to inform their users in a clear and consistent way. In addition, active protection is sometimes desired. For example, some metadata might only be accessible to certain users, or similar to the ephemeral photo sharing use case, a visual

watermark can be added that can only be removed after proper authentication. GLAM Institutions might have within their collections images carrying 'privacy-sensitive' information, such as photographic material of identifiable individuals. For the exploitation of these images, the relevant legal framework concerning privacy and data protection must be taken into account. Finally, integrity and authenticity check should allow sharing as a trusted source as well as identification of potential modifications made to an artefact. An example framework targeting these scenarios is elaborated in the Section 'IPR management for GLAM sector' under 'Example Applications'.

1.3 JPEG Privacy and Security

In response to these market needs, the JPEG committee has initiated a standardization process to enable privacy and security support in its various standards. This activity is formally known as JPEG Systems part 4 'Privacy, Security and IPR features' or ISO/IEC 19566-4. JPEG Privacy and Security intends to provide a degree of trust while sharing image content and metadata. Simultaneously, it will allow the signalling of the associated policies. It targets technical solutions for resolving privacy and security issues, which are compliant with legacy technology in the domain, i.e. both image coding as well as metadata standards that signal information such as access policies and IPR conditions. The work on JPEG Privacy and Security is currently in progress and is expected to become an international standard in early 2019.

The earlier described use cases were gathered by the JPEG committee during three workshops in Brussels [9], La Jolla [10] and Chengdu [11]. These workshops involved the participation of stakeholders of the different addressed markets. Stakeholders included academia, not-for-profit organizations, government agencies, lawyers and news agencies. Based on these interactions with stakeholders a set of key desired functionalities has been identified. Supported functionality in JPEG Privacy and Security includes access to partial or complete image data and metadata, independent protection of image data and metadata, hierarchical levels of access, support for privacy policies, provenance signalling, authenticity checking, signalling mechanisms to avoid stripping off metadata and support for file carving.

Every use case needs specific dedicated protection tools. For example, in some cases, invisible watermarks or fingerprints could be more suited than traditional encryption. However, it is important to note that JPEG does not intend to standardize any of the underlying technologies but rather aims to formalize the way these are signalled and applied to JPEG images. As such, users will have the flexibility to choose and adopt the tools best suited for their specific scenarios. When defining the signalling syntax, backward compatibility with legacy JPEG and JPEG 2000 code streams will be provided as well as with other existing standards and frameworks (e.g. those by SC 27, SC 29, and W3C).

Based on the identified use cases and requirements, a list of targeted tools to be included in the standard was created [12]. These tools are classified into two main domains: protection and authenticity.

1.3.1 Protection features include

- Protection tools to protect parts of any type of JPEG images and/or associated metadata independently, while ensuring backward and forward compatibility with JPEG coding technologies;
- Handling of hierarchical levels of access and multiple protection levels for metadata and image protection;
- File carving systems (e.g. resynchronisation points).

1.3.2 Authenticity features encompass

- Integrity check of image data and/or embedded metadata;
- Avoidance of stripping off metadata, especially IPR information;
- Versioning and/or tracking changes of an image and/or associated metadata and solutions to support embedding provenance information;
- Embedding of traceable information to allow identification and assessment of the master image and identify derived or modified versions of the master image.

To understand how these functionalities can be integrated and supported in current and future JPEG standards, it is important to comprehend the philosophy behind the system architecture of JPEG standards outlined in the next section.

1.4 JPEG Systems

The JPEG committee, in the last 30 years, has developed several methods that add new features to its core coding solutions. The first and most used image coding standard JPEG-1 (ISO/IEC 10918-1) with its file format JFIF (ISO/IEC 10918-5) allowed for the inclusion of additional features by using a so-called APP markers mechanism. An example of a commonly used APP marker is APP1 with EXIF metadata. However, the number of APP markers was limited and many features offered through them were not widely adopted.

Together with the JPEG 2000 standard (ISO/IEC 15444-1), the method of a box-based file format was introduced in 2000. This is a very flexible syntax where objects for additional features in the file were encapsulated within a binary structure as illustrated in Fig. 1.

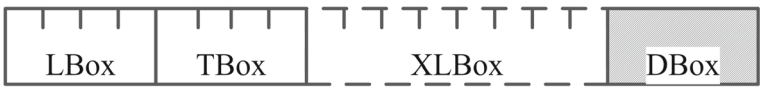

Fig. 1 Illustration of a box-based file structure

The key elements of this structure are as follows:

- The 32bit wide LBox field, which defines the length of the box structure;
- The 32bit wide TBox field, which defines a unique box type identifier (the feature);
- An optional extended length field XLBox, when the box is larger than $(2^{32} - 1)$; and,
- An optional DBox field, which contains the payload of the box, if necessary.

This method was widely used not only in JPEG 2000 but also in other standards like JPEG XR (ISO/IEC 15444-2:2004/AMD3:2015) or in the ISO Base Media File Format (ISOBMFF) in MPEG-4 (ISO/IEC 14496-12). Many features were already added to these standards using the same syntax.

In the last years, the JPEG committee has worked on a systematic review and consolidation of all of its file formats, functionalities and code stream syntax. The goal was and is to define an overall framework — called JPEG Systems — for future and legacy standards to ensure interoperability and functionality exchange between all JPEG family standards. As a first result, the principles for the system layer structure of JPEG standards are now defined in part 1 of JPEG Systems — 'packaging of information using code streams and file formats' (ISO/IEC TR 19566-1:2016) and part 2 — 'transport mechanisms and packaging' (ISO/IEC TR 19566-2:2016).

As the box-based approach was identified as future-proof, a method was developed to add boxes not only to the newer standards in the JPEG family but also to the JPEG-1 standard, for example to allow for extensions for High Dynamic Range (HDR), extended bit depths, privacy and security features, universal metadata or 360° images.

The concept of the method was first introduced in the recently developed JPEG XT standard (ISO/IEC 18477-3) [13], which is part of a forward and backward compatible suite of standards to JPEG-1. New extensions include HDR, up to 16-bit integer coding, HDR floating-point coding, lossless and near-lossless coding and alpha channel coding. The main principle of the concept is to cut a box structure into parts smaller than 64 k byte as this is the limitation of an APP marker segment and to include these parts into multiple instances of APP11 marker segments (see Fig. 2). The packet sequence number identifies the specific part of the box. For more details please refer to ISO/IEC 18477-3 JPEG XT: Box File Format [13].

It is important to stress that such approach inherently enables backward and forward standard compliance. Backward compatibility refers to the capability of a decoder to interpret correctly both the older standard, in particular JPEG-1, and the newly added functionality. Forward compatibility refers to the capability of the older standard or its legacy implementation to still being able to interpret and decode the information it is assumed to recognize in the expanded file format specification but to ignore all new components that are connected to the more recent standard specification such that it does not breakdown. The latter capability is extremely important since it will guarantee that existing applications using legacy codecs are not jeopardized.

Next steps for JPEG Systems are the implementation of system layer extensions in part 4 — 'Privacy, Security and IPR features' (ISO/IEC 19566-4) and part 5 — 'JPEG Universal Metadata Box Format (JUMBF)' (ISO/IEC 19566-5).

An illustration for the use of the APP11 marker in the legacy JPEG-1 standard is given in Fig. 3, which shows also the compatibility to legacy JPEG-1 and newer JPEG decoders.

1.5 Example applications

1.5.1 Secure transmorphing

Secure transmorphing can be used to protect privacy of pictures in many applications, including in social media

0xFFEB	Le	CI	En	Z	LBox	TBox	*XLBox*	DBox
APP11 marker	Size of marker segment	Common Identifier for specific APP11 marker	Box Instance Number	Packet Sequence Number	Box Length	Box Type	*Box Length Extension*	Payload Data

Fig. 2 Organization of the APP11 marker segment for boxes

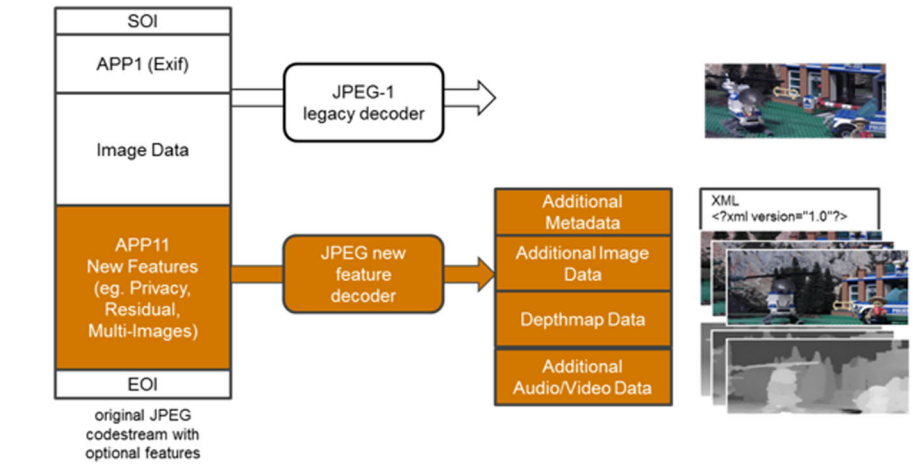

Fig. 3 JPEG Systems - APP11 usage with box-based data

where access to the original can be restricted to authorized recipients only, while allowing access to a pleasant but privacy protected version of the image. Examples of transmorphing are illustrated in Fig. 4 and can range from the well-known scrambling to inpainting. Most existing approaches are storing and transmitting both original and processed versions of an image individually, which requires more bandwidth and storage usage and management efforts. In this section, we discuss an algorithm called JPEG transmorphing [14, 15], which morphs an image to its processed version while preserving sufficient information about the original image in the processed image so that the original image can be recovered later.

Let us assume that a digital image has been processed by one or a series of image processing operations, for example masking human faces in the picture with smiley faces. The transmorphing process, illustrated in Fig. 5, can be described by the following operations:

- Calculation of a Mask matrix, by first taking the difference between the original and processed pixels and generation of a binary image by applying a thresholding operation on the image difference. The values equal to 1 in the binary image are dilated to match the Minimum Coded Unit (MCU) block boundaries and then downsampled such that each element points to a corresponding MCU block. Therefore, the values equal to 1 in the Mask matrix corresponds to a region or MCU blocks where the image is modified, called modification region(s) or modification blocks. The calculation of the Mask matrix is performed for each of the three colour channels in the image followed by merging the three Mask matrices with logical OR operations.
- Creation of the sub-image according to the Mask matrix, where the sub-image denotes pixels in the original image corresponding to the modified regions. The sub-image is encoded as a JPEG image, by setting all DCT coefficients outside of the modified regions in the original image to zero. If the original image is already in JPEG format, this can be easily done by transcoding the modified regions of the original image to the sub-image.
- Embedding data in APPn markers by inserting the byte stream of the JPEG sub-image, along with the

Fig. 4 Examples of secure transmorphing operations applied to an image

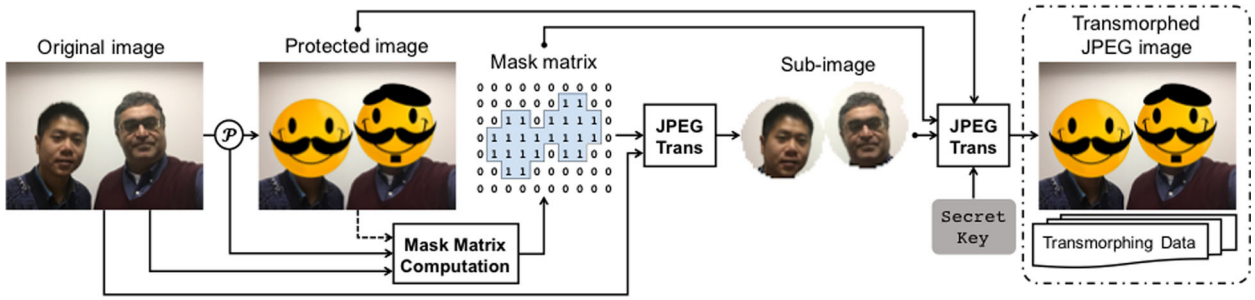

Fig. 5 Privacy protection of a JPEG image with secure transmorphing

metadata about the sub-image, in one or several application marker segments (APPn Markers) of the JPEG file of the processed image. Specially, a security option is available in the JPEG secure transmorphing algorithm to meet the needs for image security and privacy protection applications. The Secure JPEG [16] framework is applied to the sub-image with a selected image security tool, which can be either AES (ISO/IEC 18033) or scrambling. The embedded metadata signals three types of information: (i) the size of the sub-image in bytes, (ii) the method by which the sub-image is secured, and (iii) the Mask matrix.

The recovery process, illustrated in Fig. 6, aims at restoring the original image from the transmorphed image by reversing the above-described transmorphing process:

- Extraction of the sub-image bytestream and metadata from the APPn markers, and reconstruction of the sub-image and Mask matrix followed by replacement of the DCT coefficients corresponding to the modification blocks of the morphed image with that of the sub-image.
- In cases where the sub-image is secured, a secret key needs to be provided to decrypt or descramble the extracted sub-image.

A secure transmorphing algorithm involves four inputs: the original image, the processed image, a mask threshold, and a secret key. The original and processed images can be in any format but are assumed to have the same pixel resolution. The output transmorphed image and the reconstructed image are all in JPEG format.

This algorithm can be deployed in a social network setting enabling the secure exchange of image data. Applications exist nowadays that do enable this functionality. An example is ProShare that was developed by EPFL [17]. This application allows to post protected images to Facebook, Twitter, WhatsApp .... Users need to register via the ProShare app enabling them to assign (partially), protect images and define access rights. Thereafter, protected images are posted to the respective social network. Protected images can subsequently be rendered again by other users using the ProShare app if they were assigned the appropriate rights by picture owner. If users are not registered on ProShare, they will not be able to view the protected (parts of the) images uploaded via ProShare. The secret key handling is done via this app and not via the social network. In the particular case of ProShare, an attribute-based encryption along with conventional public key cryptography is used to achieve secure transmission of secret keys and a fine-grained control over who may view shared photos [14, 15].

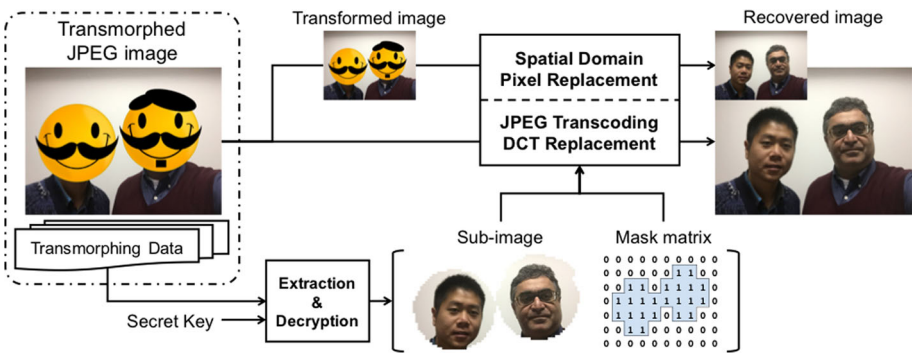

Fig. 6 Recovery of the original from a secure transmorphed JPEG image

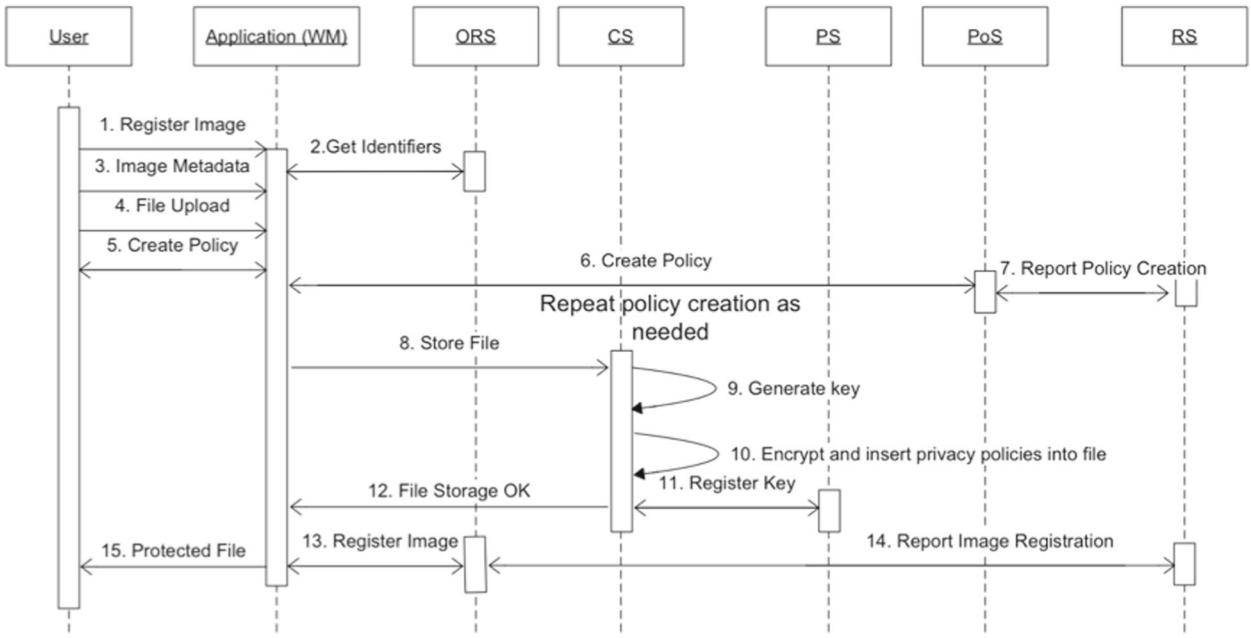

Fig. 7 Image protection

This framework of course does not deliver full protection as it is the case in an analog world as well. People can for example always take snapshots of the screen, which is a weak point of every application reconstructing digital content. What is important though is that the advocated system allows for secure exchange of image content between the right holders. If end-users are deliberately overruling, the assigned rights they are placing themselves in a vulnerable legal situation.

1.5.2 IPR management for GLAM sector

As mentioned in the introduction, the GLAM sector is dealing with images that have associated Intellectual Property Rights (IPR). In this particular case, the access to the images needs to be controlled based on specific privacy policies or rules and IPR conditions. Therefore, mechanisms are needed to both specify the policies and enforce them. To be more specific, we consider here an example implementation of controlled access to images owned by a museum.

One relevant issue is who defines the policies. Two main options are either the service provider or the image owner, assuming the case in which the image owner is not the one that provides access to the image. In our example, the service provider (the museum) could define the rules, but they should be based on the original intellectual property rights set by image owner.

The next issue is how to define the rules (policies); i.e., on which kind of information we should base the conditions to verify in order to decide if the access is granted. Examples could include information on user, image, action, context, etc. A specific example of a rule to

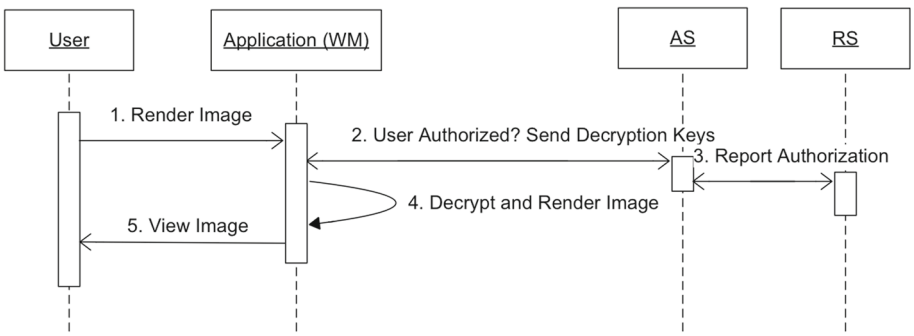

Fig. 8 Authorization of access to a protected image

illustrate this could be only museum employees can view the painting photo album during this month. In this case, users are the museum employees, images are the specified photo album, action is view and context is this month.

The third and final issue we consider is where to store the rules and the images to which they apply. Images could be even referenced in their repository. Rules could be included as protected metadata in the image itself — using JPEG Privacy and Security signaling syntax — or in external systems.

The possible solution presented here provides all these features [18]. The privacy policies are described with XACML [19], which facilitates the possibility of having different levels of granularity in the rules. As mentioned before, this information can be included (or linked to) within the image file, i.e., the APP11 marker segment in case of a JPEG-1 file format. In our specific implementation, based on MIPAMS [18], the privacy policies are included in the image with only a reference to an external system that will handle everything (access to the privacy policies, authorization of access to the images, protection of the image, creation of the privacy policies, etc.).

The creation phase (Fig. 7, or how to protect an image for further distribution and access, includes registering the image (with the Workflow Manager WM and the Object Registration Service ORS), adding the metadata, uploading the image (to the Content Service CS), creating its privacy rules (with the Policy Service PoS), encrypting if requested and adding privacy information. These processes are complemented with the key management (Protection Service PS) and some reporting (Reporting Service RS).

In turn, the access phase or how to authorize access to a protected image (Fig. 8), starts when a user intends to render a privacy protected image. If authorization is given by the Authorization Service (AS), the decryption keys are sent to the user and the Application Workflow Manager WM decrypts the protected image (parts) and renders the image.

2 Conclusions

Integrating support for privacy and security functionality in existing image representation formats without breaking legacy applications was until recently a quite cumbersome activity. In this paper, it is demonstrated how — while respecting backward and forward compatibility with legacy implementations of image decoders — this functionality can be integrated in the family of coding technologies standardized by the JPEG committee. More particularly, we focused on JPEG-1 technologies and explained how by exploiting and expanding its file format and code stream syntax this could be achieved. The proposed solution in the process of integration in the JPEG Systems part 4 — 'Privacy, Security and IPR features' (ISO/IEC 19566-4) and part 5 — 'JPEG Universal Metadata Box Format (JUMBF)' (ISO/IEC 19566-5) standards. We illustrated the exploitation of this syntax in two application contexts targeting completely different markets, namely secure transmorphing in social networks photo sharing and IPR management in GLAM applications.

Acknowledgements
Not applicable.

Funding
Work presented in this paper has been partially supported by the Spanish Government under the project Secure Genomic Information Compression (GenCom, TEC2015-67774-C2-1-R) and the European Union's ICT Policy Support Programme as part of the Competitiveness and Innovation Framework Programme, under GA no. 621037 (Europeana Space).

Availability of data and materials
Not applicable.

Authors' contributions
All authors are member of the JPEG committee and involved in shaping and defining the JPEG Privacy and Security standardization activities. TE proposed the Secure Transmorphing solution and JD the MIPAMS architecture. All authors read and approved the final manuscript.

Ethics approval and consent to participate
Not applicable.

Consent for publication
Not applicable.

Competing interests
The authors declare that they have no competing interests.

Publisher's Note

Author details
[1]Imec, Kapeldreef 75, B-3001 Leuven, Belgium. [2]Vrije Universiteit Brussel (VUB), Department of Electronics and Informatics (ETRO), Pleinlaan 2, 1050 Brussels, Belgium. [3]Ecole Polytechnique Fédérale de Lausanne (EPFL), Multimedia Signal Processing Group (MMSPG), EPFL/STI/IEL/GR-EB, ELD238, Station 11, 1015 Lausanne, Switzerland. [4]Fraunhofer Institute for Integrated Circuits IIS, 91058 Erlangen, Germany. [5]Universitat Politècnica de Catalunya (UPC), Campus Nord D6, Jordi Girona 1-3, 08034 Barcelona, Spain. [6]Waseda University, no.66-401, 3-14-9 Okubo, Shinjuku-ku, 169-0072 Tokyo, Japan. [7]Australian Government, Canberra, Australian Capital Territory, Australia.

Received: 12 June 2017 Accepted: 19 September 2017
Published online: 29 September 2017

References

1. JPEG. https://www.jpeg.org/. Accessed 25 Sept 2017
2. P Schelkens, A Skodras, T Ebrahimi, *The JPEG 2000 Suite*. (Wiley, Chichester, UK, 2009)
3. T Ishikawa, J Delgado, A Natu, P Schelkens, F Temmermans, JPEG Privacy and Security scope use cases and requirements version 1.3 (WG1N74006) (2017). ISO/IEC JTC 1/SC 29/WG 1
4. ISO/IEC JTC 1/SC 27, ISO/IEC 29100:2011 – Information Technology – Security Techniques – Privacy Framework (2011). ISO/IEC JTC 1/SC 27
5. SnapChat. https://www.snapchat.com. Accessed 25 Sept 2017
6. Yovo. https://yovo.me/. Accessed 25 Sept 2017
7. Privately. http://www.privately.eu/. Accessed 25 Sept 2017
8. Dstrux. https://dstrux.com/
9. P Schelkens, T Ishikawa, A Natu, F Temmermans, S Kim, A Hinds, A Skodras (eds.), *Privacy and Security Workshop Proceedings, (wg1n70033)* (ISO/IEC

JTC 1/SC 29/WG 1, Brussels, 2015). https://jpeg.org/items/20151109_privacy_security_proceedings.html
10. P Schelkens, T Ishikawa, A Natu (eds.), *JPEG Privacy and Security 2nd Workshop Proceedings, (wg1n71026)* (ISO/IEC JTC 1/SC 29/WG 1, La Jolla, 2016). https://jpeg.org/items/20160307_privacy_security_2_proceedings.html
11. Y Zhao, J Lu, A Natu, T Ishikawa, P Schelkens (eds.), *JPEG Privacy and Security 3rd Workshop Proceedings, (wg1n73012)* (ISO/IEC JTC 1/SC 29/WG 1, Chengdu, 2016). https://jpeg.org/items/20161104_privacy_security_3_proceedings.html
12. ISO/IEC JTC 1/SC 29/WG 1: Privacy and Security Final Call for Proposals (2017). ISO/IEC JTC 1/SC 29/WG 1
13. T Richter, A Artusi, T Ebrahimi, JPEG XT: a new family of JPEG backward compatible standards. IEEE Multimed. **23**(3), 80–88 (2016)
14. L Yuan, T Ebrahimi, in *Proceedings of the IEEE International Conference on Image Processing (ICIP); Quebec City, Canada*. Image transmorphing with JPEG (IEEE, New York, 2015), pp. 3956–3960. doi:10.1109/ICIP.2015.7351547
15. L Yuan, T Ebrahimi, Image privacy protection with secure JPEG transmorphing. IET Signal Process. **23**, 80–88 (2017). http://digital-library.theiet.org/content/journals/10.1049/iet-spr.2016.0756
16. F Dufaux, T Ebrahimi, in *Proc. of SPIE: Conference on Applications of Digital Image Processing XXIX, San Diego, CA*. Toward a secure JPEG, vol. 6312 (SPIE, Bellingham, 2015)
17. ProShare for iOS. https://itunes.apple.com/us/app/proshare/id1047578277?mt=8. Accessed 25 Sept 2017
18. J Delgado, S Llorente, in *Proceedings of the IEEE International Conference on Multimedia & Expo Workshops (ICME), Seattle, CA*. Improving privacy in JPEG images (IEEE, New York, 2016)
19. OASIS, eXtensible Access Control Markup Language (XACML) Version 3.0 (2013). http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.pdf. Accessed 25 Sept 2017