ISO/IEC JTC 1/SC29/WG1 **N74015**
74th Meeting, Geneva, Switzerland, Jan. 16-20, 2017

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: JPEG Privacy and Security Call for Proposals

SOURCE: WG1

PROJECT: ISO/IEC 19566 (JPEG Systems)

STATUS: Draft

REQUESTED ACTION: Provide feedback and response

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

ISO/IEC JTC 1/SC29/WG1 N74015
74th Meeting, Geneva, Switzerland, Jan. 16-20, 2017

JPEG Privacy and Security Call for Proposals

The JPEG Committee has launched a new activity called JPEG Privacy & Security. This activity aims at developing a standard for realizing secure image information sharing which is capable of ensuring privacy, maintaining data integrity, and protecting intellectual property rights(IPR). This activity is not only intended to protect private information carried by images - in the image itself or the associated metadata - but also to provide degrees of trust while sharing image content and metadata based on individual preferences. It is necessary to extend the existing coding standards by adding such preferences. JPEG Privacy & Security will explore ways on how to design and implement the necessary functionality without significantly impacting on coding performance while ensuring scalability, interoperability, and forward and backward compatibility with current JPEG standard frameworks.

Since the JPEG committee intends to interact closely with actors in this domain, the first workshop was organized on October 13, 2015 during the JPEG meeting in Brussels, Belgium, and the second workshop was organized on February 23, 2016 during the JPEG meeting in La Jolla, CA, USA. Following the great success of these workshops, the third workshop was organized on October 18, 2016 during the JPEG meeting in Chengdu, China. These workshops targeted on understanding industry, user, and policy needs in terms of technology and supported functionalities.

This document contains a Call for Proposals (CfP) issued in the context of JPEG Systems standardization. JPEG Systems (ISO/IEC 19566) consists of four individual parts now. Part 4 of the standard will define new tools to support protection of privacy and IPR in image and metadata as well as other security mechanisms.

This call addresses the following components of JPEG Privacy and Security:

- Protection mechanism for intellectual property rights(IPR) information described as metadata;
- Protection tools for image and metadata;
- System-level solutions for privacy and security protection of images encoded by JPEG coding technologies to ensure backward and forward compatibility;
- APIs to access an authorized image efficiently like IIIF (International Image Interoperability Framework), JPSearch extension?

1. JPEG Privacy and Security

1.1. Rationale

The JPEG format is today one of the most popular and widely used multimedia standards. Since cameras switched from analog to digital in the early years 2000 and not much later mobile phones integrated communication and image capturing in one device, nowadays several billion of JPEG encoded images are produced per day. Most of us are using JPEG codecs, on a daily basis – often unknowingly – in devices such as mobile phones, computers, tablets, television screens and of course digital cameras. This vast JPEG ecosystem is expected to continue its exponential growth and to generate additional economical value. In the last two decades, a large number of small, medium-sized and large companies have been relying on JPEG technology for their products, and this trend will likely continue.

More recently, we observed the trend to share images immediately via the Internet by means of social media and cloud-based image repositories (i.e. Facebook, Flickr, YouTube, and Pinterest) as reflected in the figure above. Moreover, electronic newspapers are publishing digital pictures from their photographers or image material provided by news agencies or even their readers.

This proliferation of use of digital images gave also rise to a number of conflicts in terms of non-intended release of privacy information, e.g. metadata associated to a published picture that still contained geographical information that allowed to identify persons that have given anonymous interviews to journalists, or pictures posted on social media only intended for a limited audience that went public. Moreover, images provided by commercial stock image repositories or news agencies have intellectual property rights (IPR) associated with them. Once used the content owners prefer that the IPR conditions continue to be applied, can be consulted and monitored as well.

Currently, these concerns are not well addressed and an inhibiting factor in the further proliferation of digital content distribution. The CEPIC Photographic association, the Plus Coalition, and the IPTC Photo-Metadata groups are all actively engaged on the preservation of the integrity of the metadata, the IPR and the distribution of rights to the private and public sectors.

1.2. Goal and features provided by the standard

JPEG Privacy and Security intends to provide a degree of trust while sharing image content and metadata, and simultaneous also allowing the signalling of the associated policies. It aims to provide technical solutions, for resolving privacy and security issues, which are compliant with legacy technology in the domain, i.e. both image coding technology as well as metadata standards that signal e.g. access policies and IPR conditions.

Supported functionalities will include access to partial or complete image data and metadata, independent protection of image data and metadata, default and additional protection tools, hierarchical levels of access and multiple protection levels for metadata and image protection, privacy policies compliance with the

privacy principles defined under SC 27's privacy framework.

Supported functionalities as new features will also include backward compatibility to JPEG-1 and JPEG 2000 codestreams, compatibilities to existing standards and frameworks (e.g. published by SC27, SC29, and W3C), provenance, agnostic to metadata schemes, identification of the master image, and signalling mechanisms to avoid stripping off metadata.

The associated box-based file format will be harmonized with JPEG Systems ecosystem and will include signalling syntax of associated metadata for access policy, protection tools, editing and changing histories, and information for file carving systems.

1.3. Potential applications

The above features – both those existing in past standards and the new ones – enable applications that have better protection ability of images with associated metadata on cloud networking, image repositories, digital publishing, content distribution, and social photo sharing. Here we briefly describe a few illustrative examples.

- Metadata protection and tracking
  - IPR Protection
  - Provenance
  - Publication and Image annotation
- Image repository with controlled access
  - Medical imaging
- Secure photo sharing in social networking
  - Ephemeral Photo Sharing
  - Social Networking and Photo Sharing
- Surveillance and monitoring
  - Video Surveillance
  - counter terrorism and monitoring
  - Forensic image analysis
  - privacy preserving search

A detailed overview of use cases can be found in Annex A.

2. Scope of this call for proposals

2.1. What is asked in this CfP?

The JPEG Privacy and Security CfP invites contributions to one or more of the following features:

1. Solutions to provide **protection tools** in images to **protect parts of the image** and **associated metadata** independently, and support **backward and forward compatibility** with JPEG coding technologies.
2. Technologies to handle **hierarchical levels of access** and multiple protection levels for metadata and image protection.
3. Mechanisms to embed **provenance information**.
4. Mechanisms to **check integrity** of image data and/or embedded metadata.
5. Mechanisms to **track changes** to an image and/or associated metadata.
6. Mechanisms to store trackable information to allow **identification and assessment of the master image** and identify derived or modified images from the master image.
7. Signalling mechanisms to **avoid stripping off metadata**, especially IPR information.
8. Technologies for **resynchronisation points** to support **file carving** systems.
9. Definition of **specific metadata** to support **privacy rules and/or protection tools**, compliant with JPEG coding technologies.

A detailed overview of requirements that proposed solutions should comply with can be found in Annex B.

2.2. Submission requirements

Proposals answering to this CfP should deliver the following elements:

1. Proposal overview
2. List of features addressed by the proposal (as described in Section 2.1)
3. Detailed technical description
4. Flow charts/diagrams
5. Software demonstrators (optional)
6. Test material (optional)

2.3. Evaluation of proposals

Selection of proposals to be included in the standard will be based on satisfying the requirements and further evaluation by the committee. If multiple proposals cover the same features the committee will decide on an appropriate selection procedure.

2.4. Timeline for Call for Proposals

The following schedule is planned for the development of JPEG Privacy and Security specifications from

the CfP to publication of the standard.

01/17	Release draft CfP
03/17	Release final CfP
06/17	Submission deadline for responses to CfP
07/17	Working draft (WD) and evaluations
10/17	Committee Draft (CD)
01/18	DIS
01/19	IS

2.5. IPR conditions (ISO/IEC Directives)

Proponents are advised that this call is being made in the framework and subject to the common patent policy of ITU-T/ITU-R/ISO/IEC and other established policies of these standardization organizations. The persons named below as contacts can assist potential submitters in identifying the relevant policy information.

2.6. Contribution to Standardization

Proponents are informed that based on the submitted proposals, a standard specification will be created. If they submit a proposal and (part of) the proposed technology is accepted for inclusion in the standard, they will hence have to attend subsequent WG1 meetings and contribute to the creation of the different standard documents. Within this process, evolution and changes are possible as several technologies may be combined to obtain a better performing solution.

2.7. Further information

- **JPEG Privacy and Security Ad hoc Group**

A JPEG Privacy and Security Ad Hoc Group has been established between 74th and 75th JPEG meetings in order to continue activities and progress with the planned work. All interested parties are requested to register to the email reflector of the AHG.

E-mail reflector: jpeg-privacy@listserv.uni-stuttgart.de
In order to subscribe to the mailing list, please follow the link:
https://listserv.uni-stuttgart.de/mailman/listinfo/jpeg-privacy and follow the steps of the e-mail being received.

- **Use cases and requirements**

Annex A “JPEG Privacy and Security Use cases” and Annex B “JPEG Privacy and Security Requirements” contain currently identified use cases and requirements for JPEG Privacy and Security. The JPEG Privacy

and Security AHG has the mandate to further update the use cases and requirements between face to face meetings which will then have to be approved by JPEG experts during its face to face meetings.

- **Contacts**

Touradj Ebrahimi (JPEG Convener)
Email: Touradj.Ebrahimi@epfl.ch

Frederik Temmermans
Email: ftemmerm@etrovub.be

Takaaki Ishikawa
Email: takaxp@ieee.org

Peter Schelkens
Email: Peter.Schelkens@vub.ac.be

Ambarish Natu
Email: ambarish.natu@gmail.com

Annex A – Use cases

Some use cases for JPEG Privacy & Security are introduced in this Annex.

A.1 Images repository with controlled access

The main features of this use case are:
- Conditional access: The access control to specific images is defined with rules (privacy policies) or ACL (Access Control List).
- Policies are defined either by the service provider or by the image owner.

Concerning rules (policies), they could be based on conditions over information on:
- User: individual, group, location, role, …
- Context: date and time, number of accesses, action (view, download, …), …
- Image: quality, geo-location, author, date, semantic information (using RDF, for example), …
- Action: read, update, delete, …

A specific example of rules could be: "only my workmates can see the Christmas Dinner photo album during this month" [1]. In this case, the conditions are:
- User: my workmates
- Context: this month
- Image: Christmas Dinner
- Action: read.
- Timing: unlimited

This use case could be extended:
- with specific kinds of images (e.g. medical images),
- allowing that different parts of the image might have different privacy policies,
- limiting access to specific metadata elements, or
- providing different levels of image quality based on roles or licenses bought.
- time restricted (image can become unusable after certain period of time)

Furthermore, images do not necessarily need to be physically in a specific repository and be accessed there, but it is also possible that they are distributed by other means (for example through a specific URI).

Therefore, the solution to implement this general use case should:
- Set-up privacy policies at specific level of detail.
- Include the policies (or a link to them) within the image file.
- Provide for the evaluation of privacy policies to authorize or not the access to partial or complete metadata and codestream.
- Keep information on the encryption/decryption tools used.

The use case assumes an images repository that would implement the relevant standards and mechanisms to preserve privacy by controlling access according to the specified rules (the specification of these rules should also follow a standard). However, another even more general scenario could be considered where images are distributed between users or are stored in different servers (i.e. Europeana.eu). In this case, the access to the images might not be controlled by the repositories themselves. Therefore, images should be

protected until the proper mechanism allowing access to authorized users is made available (for example by external applications). This last case variation is detailed in the following sub-clause.

Details of the "external applications" case

In this variation of the use case we assume 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 images, creation of the privacy policies, etc.).

To provide a realistic use case on this, Multimedia Information Protection And Management System(MIPAMS) [2] architecture, a web services based distributed system, has been used. Among other functionality, it provides the storage and authorization of privacy policies defined with XACML [3]. Moreover, it supports key storage and retrieval after positive authorization.

Figure 1 shows MIPAMS modules, the operations they provide and their relationship.

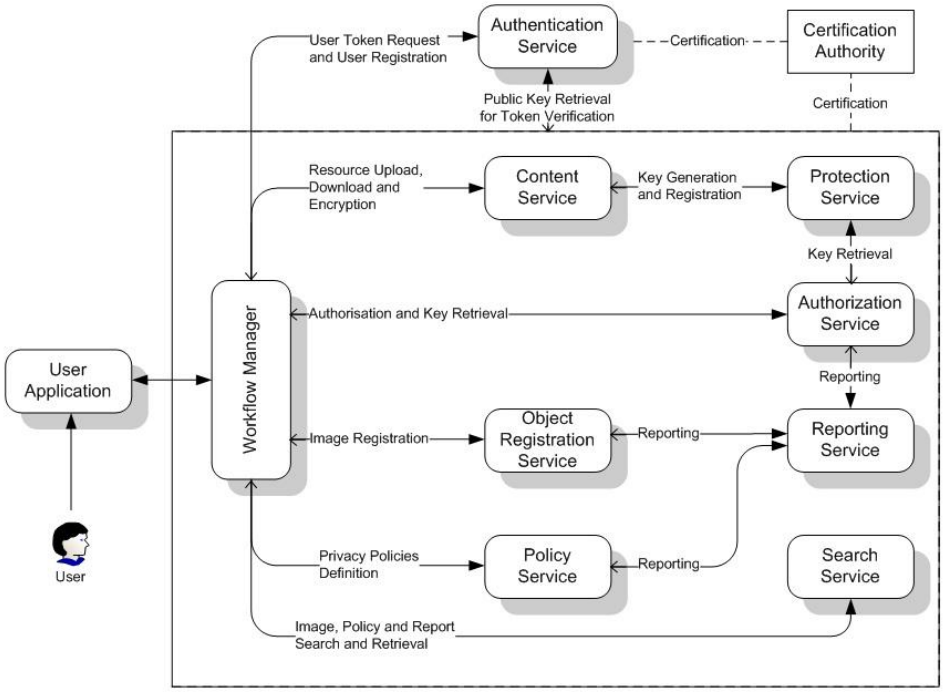


Figure 1. MIPAMS architecture

The modules relevant for the provision of privacy services are the Policy Service (PoS) and the Authorization Service (AS). The PoS offers the functionality needed to create privacy policies using XACML. AS module authorizes user access to a protected image based on the policies associated to it. In case of positive authorization, it gives access to the keys protecting the image.

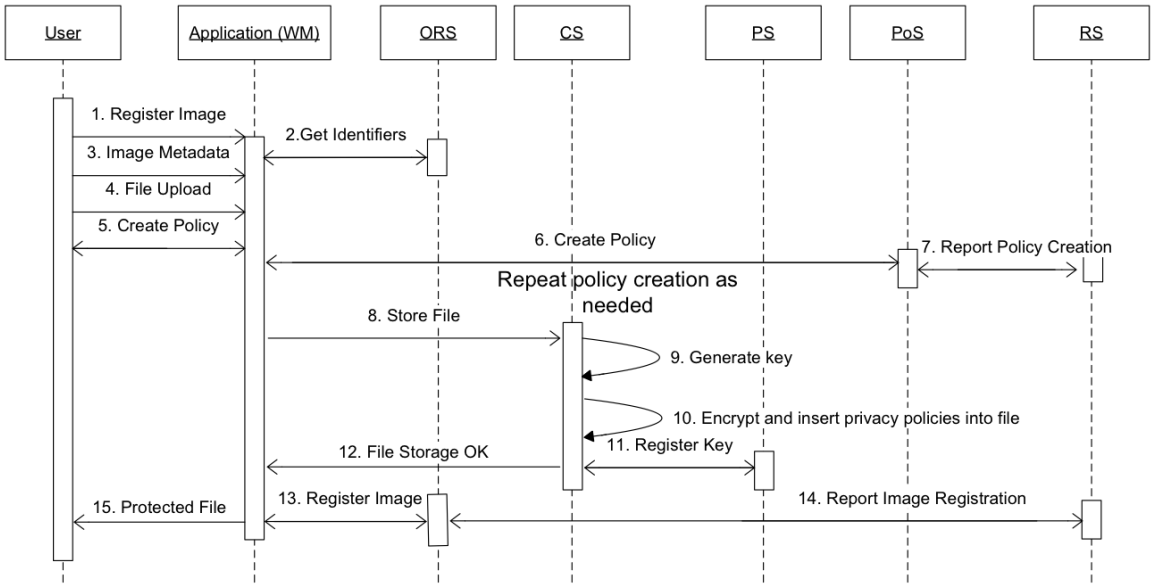


Figure 2. Image protection

Figure 2 shows the sequence diagram for protecting an image with MIPAMS. The steps can be summarized as follows:

1. User wants to protect the privacy of an image, so it asks for registration to the Application, which also involves the Workflow Manager (WM).
2. The Application contacts the Object Registration Service (ORS) to get a unique identifier for the image.
3. User fills the image metadata.
4. User uploads the image.
5. The user creates the privacy policy(ies) over the image.
6. The Application sends the policy(ies) to the PoS.
7. The PoS informs of the policy creation to the Reporting Service (RS).
8. Application sends the image to the Content Service (CS).
9. CS generates an encryption key to protect the image.
10. CS encrypts and inserts privacy information into the image file. It may apply to both metadata and image. The encryption part is optional, as the user can decide not to encrypt the image.
11. The key is registered in the Protection Service (PS).
12. CS informs Application of the correct image generation.
13. The Application registers the image into the ORS.
14. The registration of the image is reported to the RS.
15. The privacy protected file is sent back to the user.

In turn, figure 3 shows the sequence diagram for accessing the protected image through MIPAMS.
The steps can be summarized as follows:

1. User wants to render a privacy protected image using the Application.
2. The Application contacts the Authorization Service (AS). If the authorization is positive, the encryption keys are sent to the user.
3. AS reports to RS about the authorization done.

4. The Application decrypts the image (if encrypted) and renders it.
5. The user can view the image.

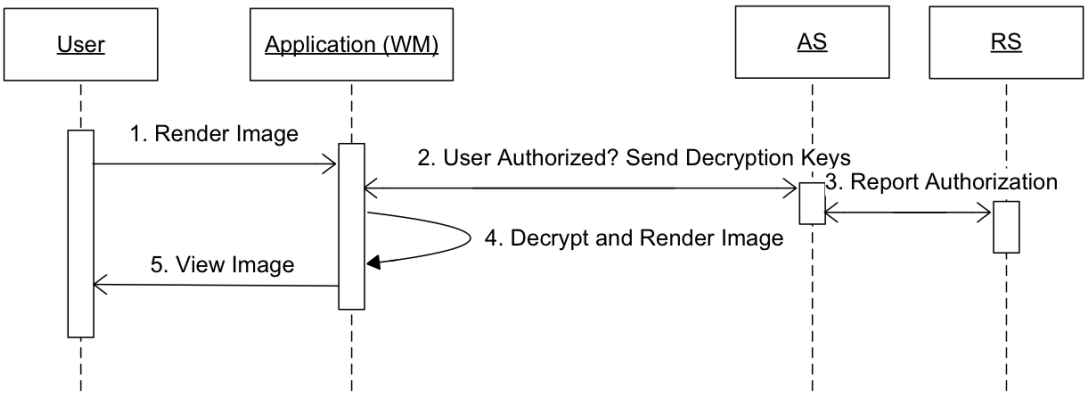


Figure 3. Authorization of access to a protected image

A.2 Metadata protection

Scenario:

1. A user set a password in a digital camera before taking photos.
2. The camera protects metadata of the photo by the password at the moment of shooting.
3. The user will distribute and share the photo based on the user's access privileges (access/read/copy).
4. Users who know the password are allowed to read the metadata.
5. People who do not know the password can only see the image data (view only).

Figure 4 shows the overview of an example for Exif and other metadata protection supporting compatibility with JPEG-1 standard. Existing JPEG-1 compliant decoder skips over the protected metadata and image data located in APP_{11} application marker.

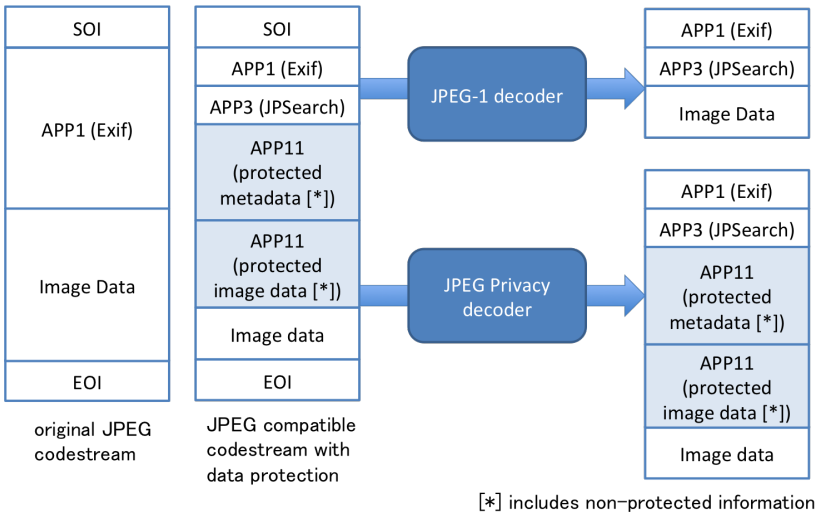


Figure 4. An example of Exif data protection

A.3 Publication and Image annotation

Scenario:

1. A photo includes many objects, of which may not be appropriate to be shown at the moment of publication.
2. A publisher wants to protect some regions of interest in the photo (e.g. hiding some faces as black painted area). The regions can be protected by partial encryption and/or scrambling per ROI.
3. The user will distribute the photo with true information encrypted by a password.
4. People will see the photo being protected with a black painted region.
5. At a later date, the publisher will distribute a key to limited users.
6. Users and people who got the key will be able to see the entire image by decryption of the region.

Figure 5 shows the overview of an example for layered images. An extended image layer will cover over the lower image layers when a user has an appropriate access right. Upper layers will hide some regions on lower layers that possibly represent private information to identify an individual based on specific features, such as faces and landmark. Each layer can be protected with different protection tools. The underlying techniques to protect the content include digital signatures, watermarking, encryption, scrambling, and key generation and management.
Especially, encryption mechanism includes partial protection of the latter, or encryption with different strengths. Some layers may describe annotations for images, which can be synchronized with the metadata stored in the image.

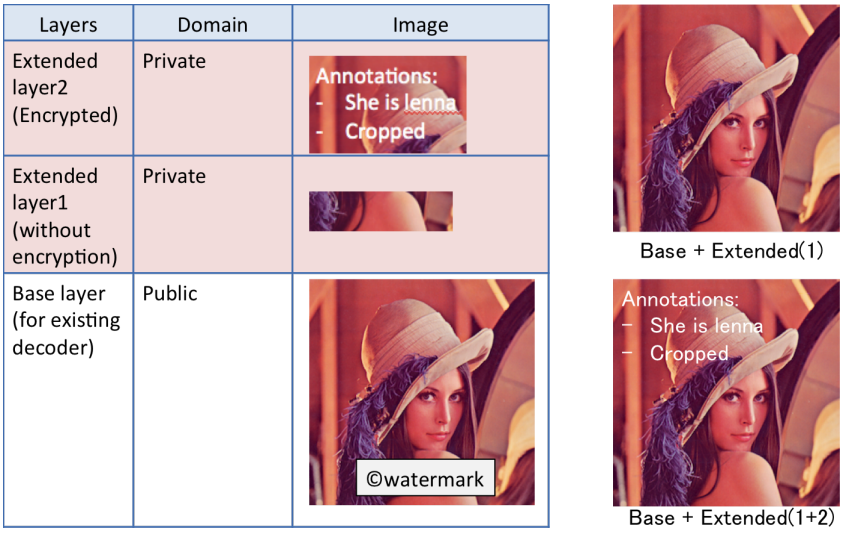


Figure 5. An example of layered image representation

A.4 Ephemeral Photo Sharing

Popularization of smart mobile devices makes communications between people extremely easy and instant. People communicate with each other with not only conventional texts like short messages or online chatting, but sharing images and video, a more enjoyable and interactive way. However, sharing photos

raises much more privacy concern than that of traditional texts as a photo can contain or reveal rich privacy related 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 pre-set interval, came to people's attention. In ephemeral photo, users can pre-set an interval, during which other friends can access the original or clear version of the 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 (https://www.snapchat.com/), Yovo (https://yovo.me/), Privately (http://www.privately.eu/) and Dstrux (https://dstrux.com/). 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 interesting and very useful if JPEG can incorporate the ability of dynamic access control to image data so that any device and application can easily apply it as a solution for ephemeral photo sharing.

A.5 Social Networking and Photo Sharing

Online social networking environment is highly sophisticated due to the great number of users and complex social graphs. Information "flies" extremely fast in online social networks and it therefore creates a problematic privacy issue. Wide spread of smart mobile devices with high-resolution cameras and user-friendly social networks applications makes photo sharing an easy and therefore popular activity. Photo, which is "worth a thousand words", contains a great amount of user's privacy information. In the environment of online social networks, shared photos can be accessed and commented easily and quickly by many people with most photos being tagged with identification information.

Almost all existing social networking services provide the functionality of photo sharing, but most of them lack a sound scheme for protecting users' privacy especially photo privacy. Especially after reports of citizen's surveillance by governmental agencies and the scandalous leakage of celebrities' private photos online, people have become concerned about their online privacy and are looking for ways to protect it. A desired privacy-preserving photo sharing in social networks may have the following properties:

1) A user can protect the content of the photo (both visual information and metadata) securely before sharing the photo to social networks.
2) The applied protection should be reversible, so that the photo can be recovered and then be viewed by authorized users.
3) The user who attempts to share a photo can decide the "friends" on social networks who can access the shared photos.
4) The user can revoke one's access rights at any time.
5) A photo owner should be able to control the re-sharing of his or her photo, e.g., decide those who can re-share the photo on their social network page.
6) An efficient access control and key distribution system enabling the secure and effective distribution of protected images.

A.6 Medical imaging

Scenario:

1. A doctor receives a patient with an unknown disease develop during a recent trip in a remote land.
2. The doctor makes some pictures of the disease and sends the photos, encrypted and with specific personal and private confidential information to few laboratories and hospitals specialized in foreign diseases.
3. After few hours, the doctor receives the analysis back on his personal email with details about the possible disease and the best suggested cure.
4. All information and data exchanged between the doctor and the external laboratory are done in full confidentiality, privacy and security and the doctor has the option to erase permanently all information, if pertinent, whenever he needs to do it.

Figure 6 shows the overview of an example for layered images. An extended image layer will cover over the lower image layers when a user (in this case, a doctor) has an appropriate access right. Upper layers will totally scramble the entire regions on lower layers that possibly represent private information to identify an individual based on specific features, such as faces and body, etc. Each layer can be protected with different protection tools. The underlying techniques to protect the content include digital signatures, watermarking, encryption, scrambling.
Especially, encryption mechanism includes partial protection of the latter, or encryption with different strengths. Some layers may describe annotations for images, which can be synchronized with the metadata stored in the image. Image authenticity should be guaranteed in order to provide the originality and genuine origin of the picture. No quality loss is required.

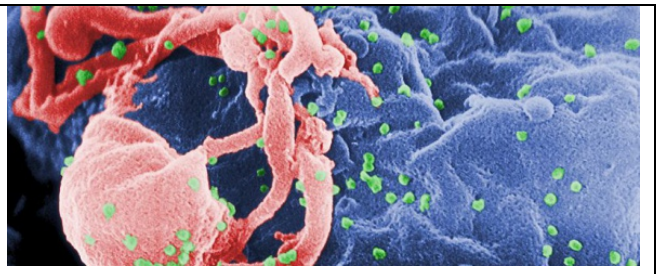
No encryption	Original picture of the infected cells (HIV-budding-Color' by CDC/ C. Goldsmith, P. Feorino, E. L. Palmer, W. R. McManus is in the public domain)	
Extended layer 2 (encrypted)	Private (picture sent from doctor office to the laboratory for further analysis). Decryption done at laboratory office.	

Figure 6. An example of layered image representation

A.7 Forensic image analysis

Scenario:

1. A couple is killed in their private home in London, UK
2. The police investigation come to the crime scene and make photos before the scene can be altered.

3. Photos are used in the trials and because they were taken under specific conditions that guarantee the authenticity of the crime scene without being manipulated, they are used as tangible evidence in the murder case

The importance of this use case is to be able to count on few, but very important facts about the usage of digital images. In fact, in order to be used in a legal case, for a forensic case, they must guarantee the following criteria:

1. To preserve the source image, without any change
2. To preserve the full metadata and date/location
3. To guarantee the authenticity of the image (means no manipulation is possible)
4. To be used in legal cases as a full legal proof

A.8 Counter terrorism and monitoring

Images that prove to be authentic and preserve all date such as the provenance, origin, date, location, content creators and so on can be well used in monitoring terrorism. Especially if those images are associated with intelligent technologies that automatically detect specific features in a scene, to improve and speed up detection in terrorism and crimes, this could create an effective time saving and efficient methodology to work well in catching possible terrorist without much waste of time. Machine learning and file integrity should match properly.

A.9 Privacy preserving search

In this use case, an image and its metadata (image descriptors) are protected using JPEG Privacy & Security protection tools before they are shared across different image sharing services such as Facebook, Google Photos and Flickers. The protected image can be then queried using the encrypted metadata without removing the protection (e.g. only the user should be able to decrypt the image and the metadata).
Main requirements for privacy preserving search are:

1. Any search performed by a third party (e.g. image sharing services) should be privacy preserving
2. Evaluation of the privacy preserving property should be transparent
3. Search performance shouldn't be compromised greatly

Privacy preserving metadata generation

From the perspective of the metadata generation, the image sharing services are encouraged to help, as long as the whole process is privacy preserving. In other words, metadata generation should take place only in the user's computer and no unencrypted private data should be transmitted to the image sharing services without the user's consent. Suitable candidates and tools for evaluating whether a service is privacy preserving should be investigated.

Privacy preserving encryption tools for metadata

The encryption of the metadata should support the privacy-preserving query. The database should be able to

1. Determine the user's scope of the search

2. Be able to return an encrypted query without the need to decrypt it.

Scenario

Alice and her friends are in Hawaii, taking some time off to relax. While there, she takes many photos of herself and her friends. Upon coming back, she tags and uploads the photos to online (social network sites, photo sharing sites, emails, etc.). Alice tags people with their respective faces, the location information (GPS and landmarks), to organized them. Once the tagging is done, the image and the tags are either fully or partially encrypted before uploading to the server. Two specific use scenarios are demonstrated:

a. Consider a hacker, who doesn't have access to Alice's images, breaks into the server and extracts the encrypted images and the tags
    - Images are encrypted: Alice and her friends are not recognizable in the image, ensuring the privacy.
    - Tags are encrypted: identity information (from the faces), location information are encrypted, ensuring privacy.
b. Consider one of Alice's friends Bob, who received rightful access to some of her photos. Bob can access those photos using his online account. On a later date, Bob searches for images with Alice with Hawaii.
    - Bob sends an encrypted query to the server
    - Server determines the scope of Bob's search
    - From the scope, server returns images with matching encrypted query
    - Bob decrypts the image from his local machine

A.10 Provenance

Scenario 1:

1. An image is captured using a mobile phone by a tourist during vacation.
2. Some metadata is added manually, such as some personal tags.
3. The image is processed in Photoshop to make some enhancements.
4. The image is shared on Facebook, during this step quality and size are reduced.
5. Some metadata is added on Facebook to identify recognized faces in the image.
6. After some time, a user downloads the image from Facebook. He can check the provenance information to check when and by whom the image was modified.
7. Provenance information is expressed as W3C PROV [4].

Scenario 2:

1. An image is signed in its original stage.
2. After sharing and distributing the image, at any point, the integrity of the image can be checked. I.e. one can identify whether any changes have been made since it was signed, even is provenance information is not explicitly tracked.

A.11 Video surveillance

Scenario:

1. A suspect person enters into an airport and approach the security control zone
2. The surveillance system detects the potential intruder and capture the video (face recognition)
3. The data are automatically sent to the police control system at the airport with an alert flag
4. The suspect traveler is catch and put in custody for security reasons

The video footages are used in the trial as they are delivered without any manipulation and they are provided through a secure mechanism that assure authenticity, privacy and origin of the capture scene.

References

[1] Delgado, J., Rodríguez, E., Llorente, S., *User's privacy in applications provided through social networks*, WSM '10 Proceedings of second ACM SIGMM workshop on Social media. ACM New York, ISBN: 978-1-4503-0173-2, 2010.

[2] Llorente, S., Rodríguez, E., Delgado, J., Torres-Padrosa, V., *Standards-based Architectures for Content Management*, IEEE Multimedia, Volume 20 Issue 4, IEEE Computer Society, Oct-Dec 2013.

[3] Delgado, J., Llorente, S. and Rodriguez, E., *Digital rights and privacy policies management as a service*, IEEE Consumer Communications and Networking Conference (CCNC) 2012, IEEE Computer Society, January 2012.

[4] W3C Working Group, PROV-Overview - An Overview of the PROV Family of Documents (http://www.w3.org/TR/prov-overview/), April 2013.

Annex B – Requirements

B.1 Compliance with the privacy principles defined under SC 27's privacy framework

JPEG Privacy and Security shall comply with privacy principles defined under ISO/IEC JTC 1/SC 27 privacy framework [1] in defining all elements under this activity.

B.2 Support JPEG-1 and JPEG 2000 backward compliant codestreams

JPEG-1 and JPEG 2000 legacy decoders shall be able to (partially) decode codestreams that carry JPEG Privacy & Security functionality, i.e. non-protected codestream parts should be processable without causing legacy codecs to crash. Codecs equipped with JPEG Privacy & Security functionality shall be able to process the JPEG Privacy & Security related syntax as well. Hence, JPEG codestreams carrying JPEG Privacy & Security extension shall be decodable by legacy JPEG decoders even if metadata and codestream are protected.

B.3 Support encrypting metadata and image data independently

The protection mechanisms shall support independent protection of metadata and image data. This will facilitate the deployment of independent privacy policies on these distinct data components.

B.4 Support hierarchical levels of access and multiple protection levels for metadata and image protection

Since different metadata description fields and spatial or quality components of the image data might require different privacy and security policies, hierarchical metadata and codestream protection syntax shall be supported.

B.5 Privacy policies need to be evaluated and allow access to partial or complete metadata and image data

Access control should not only be to the complete image, but also for specific parts of the image and metadata. This full or partial access has to be evaluated (i.e. authorized) in order to decide if access is provided or not for a specific user, based on the existing policies.

B.6 Support common protection tools

JPEG Privacy & Security shall support a set of common protection tools (cf. JPEG 2000's JPSEC framework): encryption, authentication, hash, certification, watermarking, digital signature and fingerprinting. Signaling of these tools will be defined by the standard.

B.7 Enable mechanism to support for additional protection tools

Besides the common protection tools, JPEG Privacy & Security shall specify a registration mechanism. These additional protection tools shall be registered by means of a Registration Authority (RA) as was installed for JPEG 2000's JPSEC.

B.8 Support storing of non-protected information in the APP_{11} marker

JPEG Privacy & Security extension shall also facilitate the signaling of non-protected metadata or codestream data.

B.9 Support box-based file format

JPEG Privacy & Security shall comply with the file format requirements as specified by JPEG Systems. Hence, this imposes the adoption of a box-based file format as specified in ISO/IEC 19566-1.

B.10 Support for metadata formats

JPEG Privacy & Security shall be agnostic to metadata schemes, for instance, Exif metadata, IPTC Photo metadata, XMP (ISO 16684-1) [2] and other types of metadata formats.

B.11 Support provenance functionality

JPEG Privacy & Security shall support provenance functionality to allow tracking modifications made to an image as well as guaranteeing the integrity of an image. With this respect W3C PROV will be adopted to describe provenance information while the JPEG Privacy & Security standard shall specify how to embed the information into an image and how to check the integrity.

B.12 Compatibilities to other standards (e.g. published by SC27, SC29, and W3C) and frameworks

Given the global structure of the personal data environment, international collaboration is likely to play an important role in ensuring that efficient and consistent approaches to privacy and personal information protection are required. With developments of international frameworks for the protection of citizens' personal data attempts to provide international consistency in this area requires working hand in hand with such bodies.

B.13 Support identification of the master image

JPEG Privacy and Security shall be able to store tractable information to allow identification and assessment of the master image. Global unique identifier shall also be supported to identify derived or modified images from the master image.

B.14 Signaling at system level and additional normative functionalities

JPEG Privacy and Security shall provide privacy protection functionalities and signaling mechanisms at system level. Additional normative functionalities shall remain harmonized with JPEG Systems ecosystem.

B.15 Support to security features for metadata and content

JPEG Privacy and Security shall support signaling mechanisms to avoid stripping off metadata, especially IPR information.

B.16 Resynchronisation points to support file carving systems

JPEG Privacy and Security shall support inserting synchronization markers into an encrypted codestream for facilitating reliable recovery of images.

B.17 Support for transport mechanisms

Support transport mechanisms such as JPIP that communicate image data and metadata incrementally.

References

[1] ISO/IEC JTC1/SC 27, *ISO/IEC 29100 – Information Technology – Security techniques – Privacy framework*, December 2011.

[2] ISO/TC 130, ISO 16684-1 *–Graphic technology – Extensible metadata platform (XMP) specification – Part 1: Data model, serialization and core properties, Feb. 2012.*