DMAG-UPC's answer to JPEG Privacy and Security Call for Proposals

WG1M77026

Jaime Delgado, Silvia Llorente, Daniel Naro

DMAG, UPC BarcelonaTECH

http://dmag.ac.upc.edu

jaime.delgado@ac.upc.edu

October-November 2017

DMAG DISTRIBUTED MULTIMEDIA APPLICATIONS GROUP

Focus of the Proposal

- Focus on Access Control to guarantee image privacy:
  - Express privacy rules (kind of protection we want; over what, to whom, and under which conditions, access is to be granted).
  - Integrate privacy rules in the management of JPEG images; or, at least, to establish an *association* mechanism between *rules* and *images*.
  - Manage mechanisms for both metadata and content protection, including an authorization process over the rules and a systems' architecture.

Main points of the Proposal (1/2)

- Privacy rules expression
  - Use for example of *eXtensible Access Control Markup Language* (XACML) to express privacy rules.

- Inclusion in the image. Two options:
  - Use of `RigthsDescription` element from JPSearch Core Metadata Set.
  - Define a new metadata element in the JPEG file to store privacy rule.

Main points of the Proposal (2/2)

- Mechanisms:
  - Signature:
    - For integrity and authenticity.
    - Sign independent elements and/or on the complete metadata set.
    - For example, if on the complete metadata set, stripping off detectable.
  - Authorization process:
    - To provide access for the image to the appropriate users under given conditions.

Summary of fulfilled requirements

Requirement	Covered (Yes / No / Partially)	Comments
1	Yes	Proposed mechanisms to protect Personally Identifiable Information.
2	Yes	Follow the format proposed in the Call.
3	Yes	Metadata and codestream are encrypted separately.
4	Partially	Application of different rules to different parts of the image.
5	Partially	Application of different rules to different parts of the image.
6	Partially	Not all the proposed tools are used in the solution presented.
7	Partially	The use of additional protection tools could be supported with the external architecture.
8	Yes	Combine protected and unprotected metadata.
9	Not considered	
10	Not considered	
11	Not considered	
12	N/A	
13	N/A	
14	Yes	The proposed solution follows the JPEG formats at system level.
15	Partially	Integrity mechanism should be applied to the image, as well as protection.
16	N/A	
17	N/A	

Conclusions

- Access control: adding privacy policies, (partially) encrypting metadata and/or image codestream. Also digital signatures are considered.
- *Options: use* `RightsDescription` *element of the JPSearch Core Metadata; use XACML.*
- *Example implementation.*
- Partial solution: few of the requirements and use cases defined in the Call.
- Several issues still need further work: details on the encryption procedures and formats, how to integrate privacy rules with other solutions, ...