JPEG Privacy and Security

JPEG Workshop on Media Blockchain

16 October 2018

Frederik Temmermans

JPEG Privacy and Security Timeline

- Workshops
  - Brussels (October 2015)
  - La Jolla (February 2016)
  - Chengdu (October 2016)
- Use cases and requirements
- Call for proposals issued March 2017
- Proposals received in October 2017
- Initiated Part 4 of JPEG Systems: ”Privacy, Security and IPR features”
- Currently finalizing CD
- https://jpeg.org/jpegsystems/privacy_security.html

JPEG Privacy and Security - Features

- Protection features:
  1. Solutions to support **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.
  2. Solutions to support handling of **hierarchical levels of access** and multiple protection levels for metadata and image protection.
  3. Solutions to support **file carving** systems.

JPEG Privacy and Security - Features

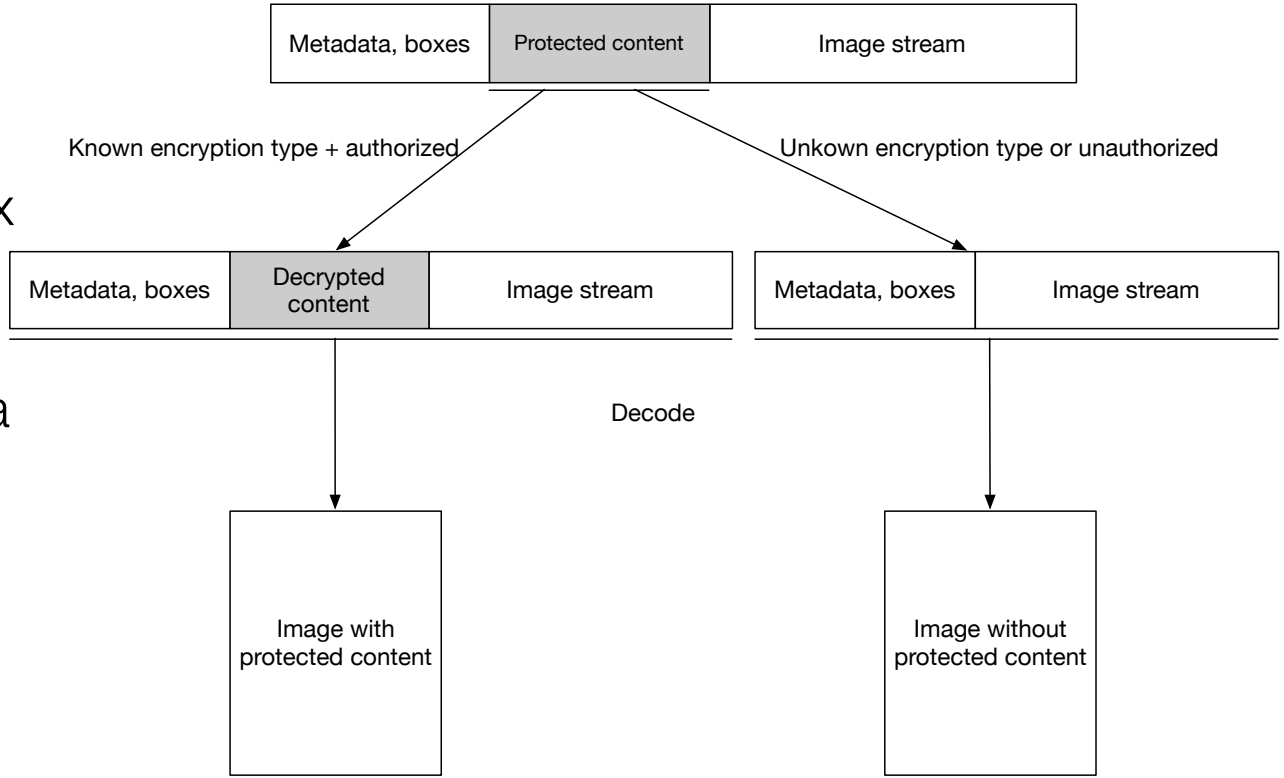
- Authenticity features:
  1. Solutions to support **integrity checking** of image data and/or embedded metadata.
  2. Solutions to support **avoiding stripping off metadata**, especially IPR information.
  3. Solutions to support **versioning** and/or **tracking changes** of an image and/or associated metadata and solutions to support embedding **provenance information**.
  4. Solutions to support embedding of trackable information to allow **identification and assessment of the master image** and identify derived or modified images from the master image.

JPEG Privacy and Security - Aim & Approach

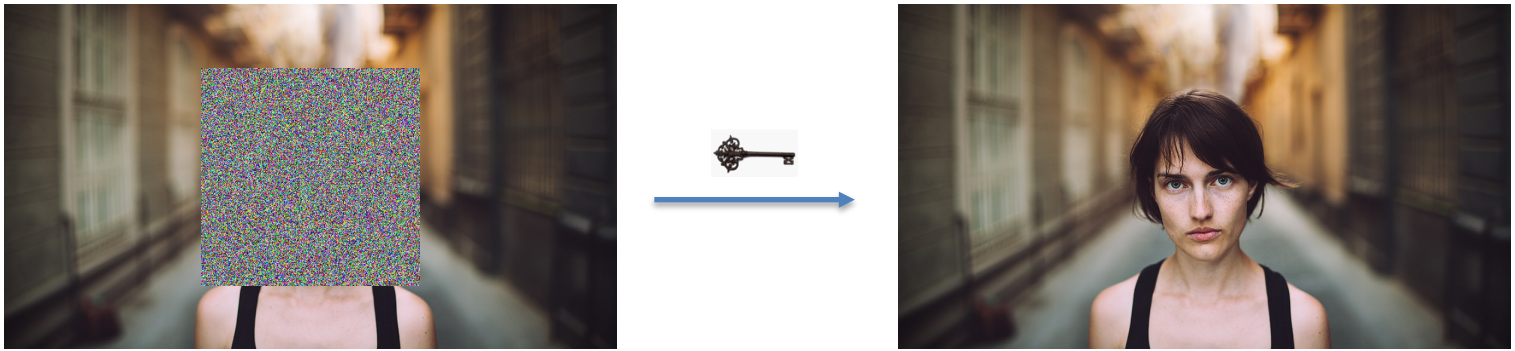
- Definition of tools to **support** protection and authenticity workflows in a **standardized way**
- Focus on **signaling syntax**
- Adoption of **existing technologies** for encryption etc.
- **Box based** approach
- Boxes wrapped in 1 or more APP11 marker segments to support JPEG-1 **backwards compatibility**
- Focus on definition of **generic boxes**
- Combined with **metadata definitions** with possibility to **reference boxes**

Protection

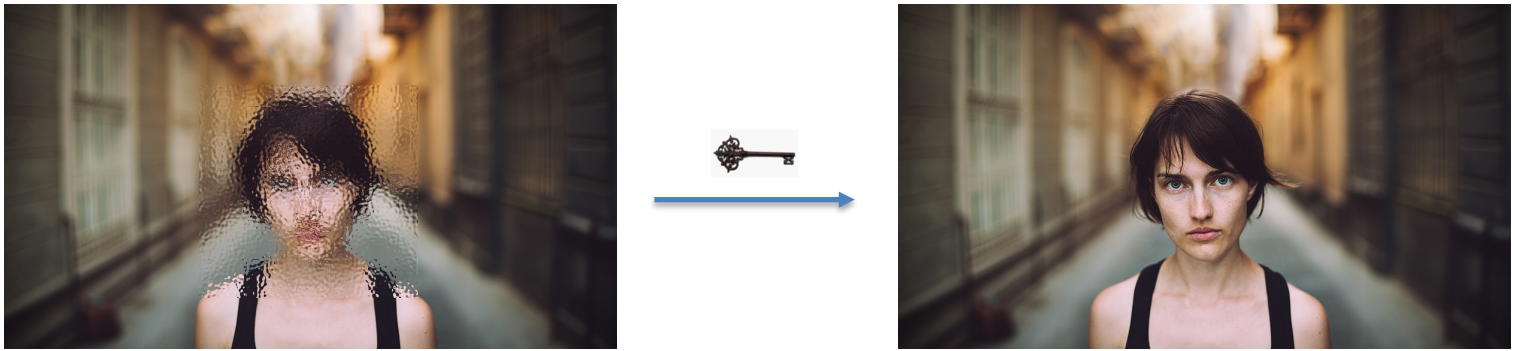
- **Protection box** wraps another encrypted box
- Since boxes are wrapped in APP11 marker segments data is split in chunks of 64kB which helps to support **file carving**



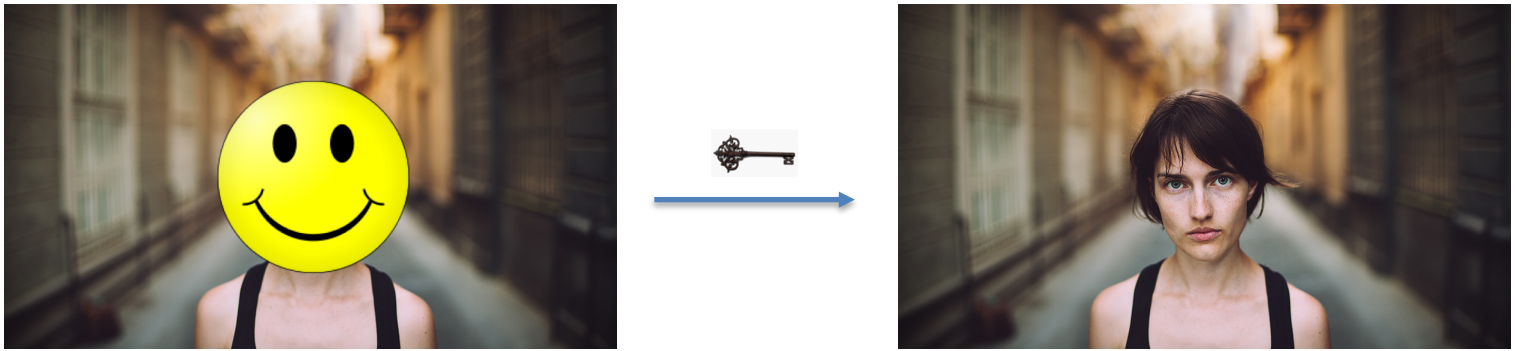
Partial protection support



Partial protection support

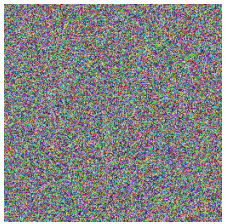


Partial protection support



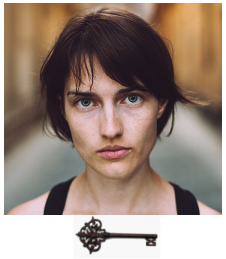
Partial protection

Header, metadata	Encrypted data (Original content)	Image stream (Protected image)



Partial protection

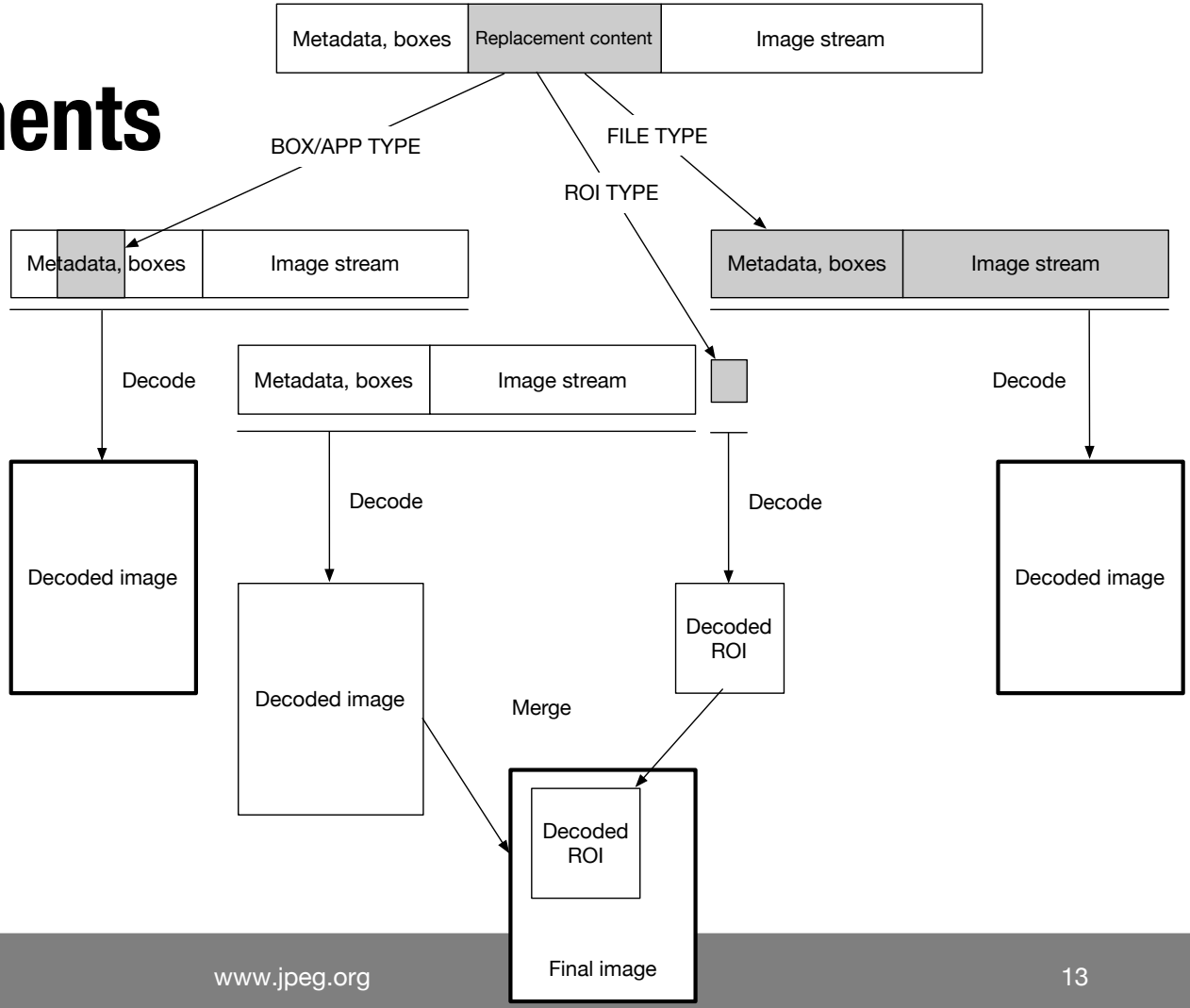
Header, metadata	Encrypted data (Original content)	Image stream (Protected image)



Partial protection

Header, metadata	Image stream (Original image)

Replacements



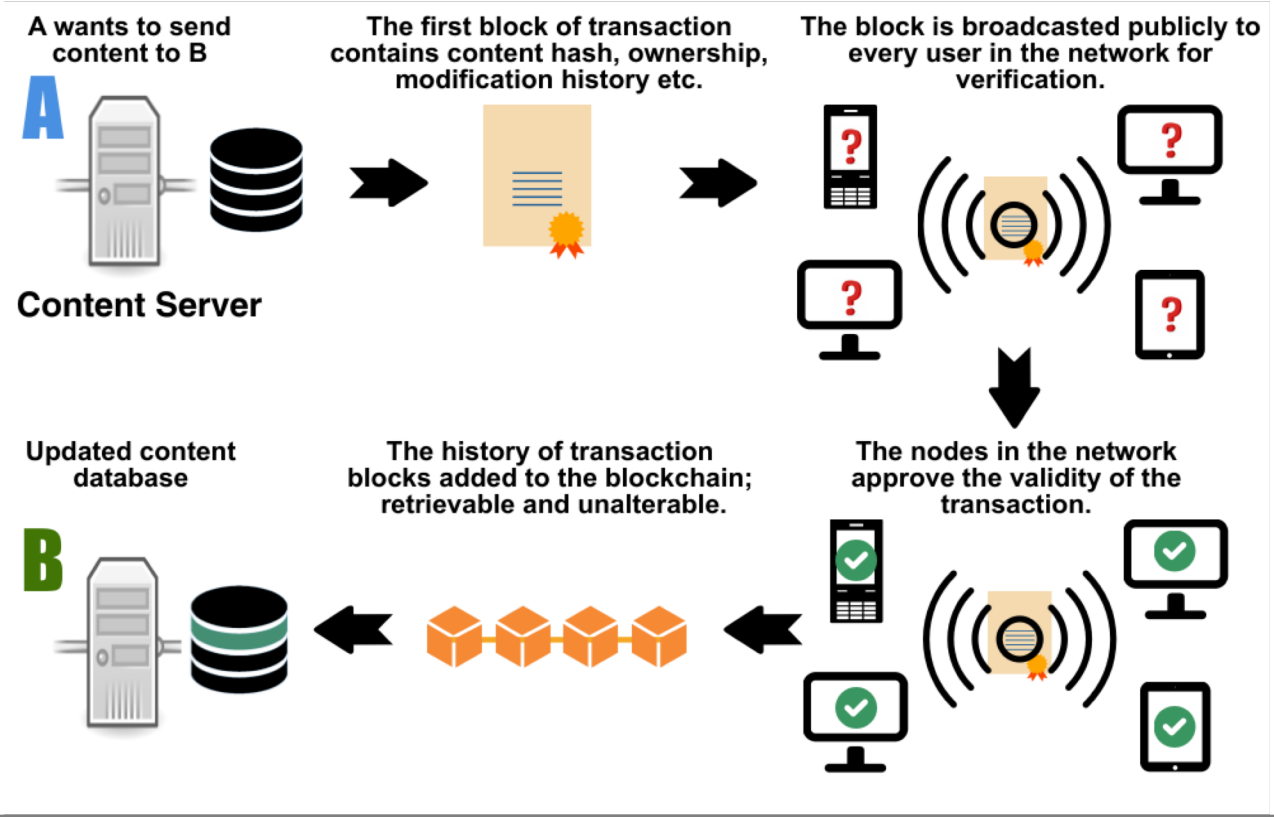
Metadata

- Metadata features
  - Access control
  - IPR
  - Provenance
- Adoption of **JPEG Universal Metadata Box Format** (JUMBF)
  - Wraps **metadata** and/or **associated content**
  - Mechanism for **referencing** boxes within metadata

Image integrity

- Support **embedding of signatures** of image content or metadata
- Allows to **identify** if **changes** were made in combination with:
  - Watermarking
  - Third party registration authority
  - Blockchain / distributed ledger
- New AhG on **Blockchain** initiated in January 2018

Blockchain technical overview



Blockchain benefits

- Blockchains provide a solution for a **distributed ledger** that is proven to be **immutable** and **community driven**
- Avoids need of trusted third parties
- **Adopted in many domains**, including cryptocurrencies, IP and creative work registration, registration of diamonds & artworks, contracts, multimedia, …
- Opportunity for new business models

Blockchain downsides

- Mining requires **huge amounts of computation power** (and energy)
  - Current estimate is 73TWh/year, almost equal to energy consumption of Austria (72TWh/year)[1]
- At this moment, **no proven alternative for proof of works** exists that do not rely on a third party
  - However, active research on this topic, e.g. “proof of stake”

[1] https://digiconomist.net/bitcoin-energy-consumption

Blockchain in a multimedia context

- Blockchains can be used to **register entire images or IPR information**
- Provides a **solution for authenticity use cases** without need for a third party register or watermarking
- Can provide a novel solution for **rewarding photographers**
- **Camera manufactures** could make a closed blockchain of all pictures taken with a particular camera

Challenges

- **Incentive** for mining?
- **Environmental impact** of computational power / energy needs
- **Alternatives** to proof of work?
- **Privacy concerns** and right to be forgotten

Standardization efforts

- ISO TC 307 Blockchain and distributed ledger technologies
- CEN-CENELEC Focus Group on blockchain and distributed ledger technologies
- ITU-T Focus Group on Application of Distributed Ledger Technology (FG DLT)

Standardization steps

Inform and engage

Collect additional use cases

Assess use cases

Define requirements

A decision on issuing a call for proposal