JPEG

# Fake Media – The JPEG Stake

3rd International Workshop on
Multimedia Privacy and Security (MPS 2020)

18th of September 2020

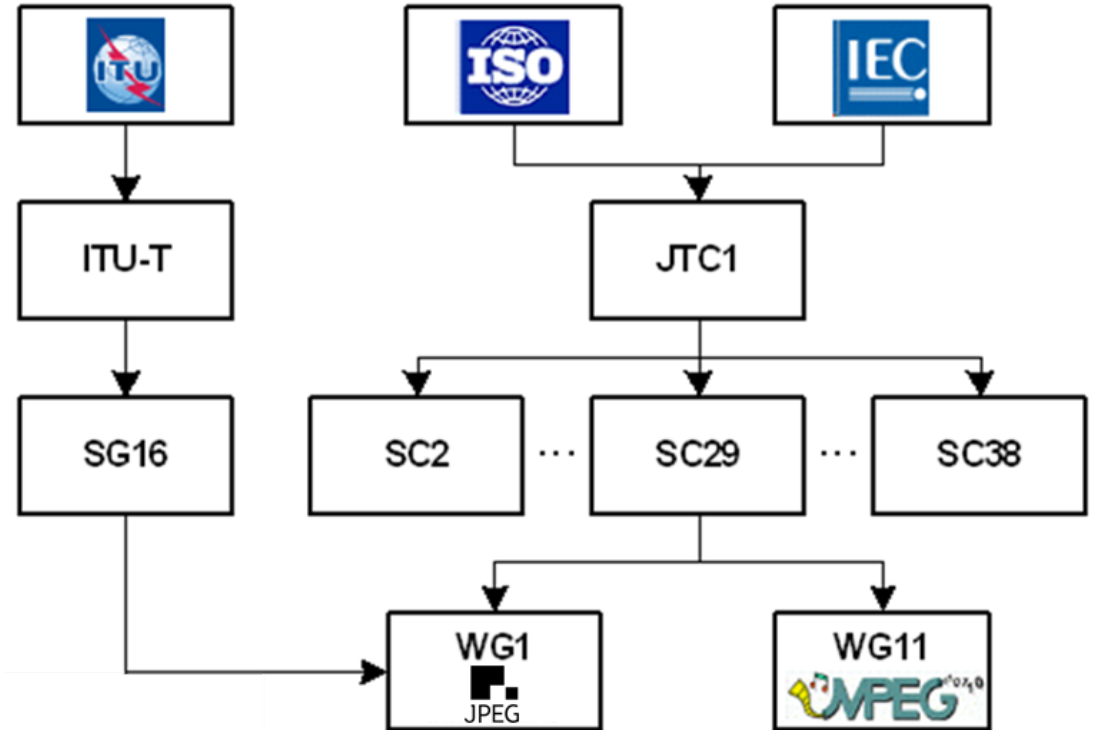
Frederik Temmermans, Deepayan Bhowmik,
Fernando Pereira, Touradj Ebrahimi

# Outline

- About JPEG
- JPEG Privacy and Security Standard
- Media Blockchain initiative
- JPEG Fake Media initiative
- Next steps

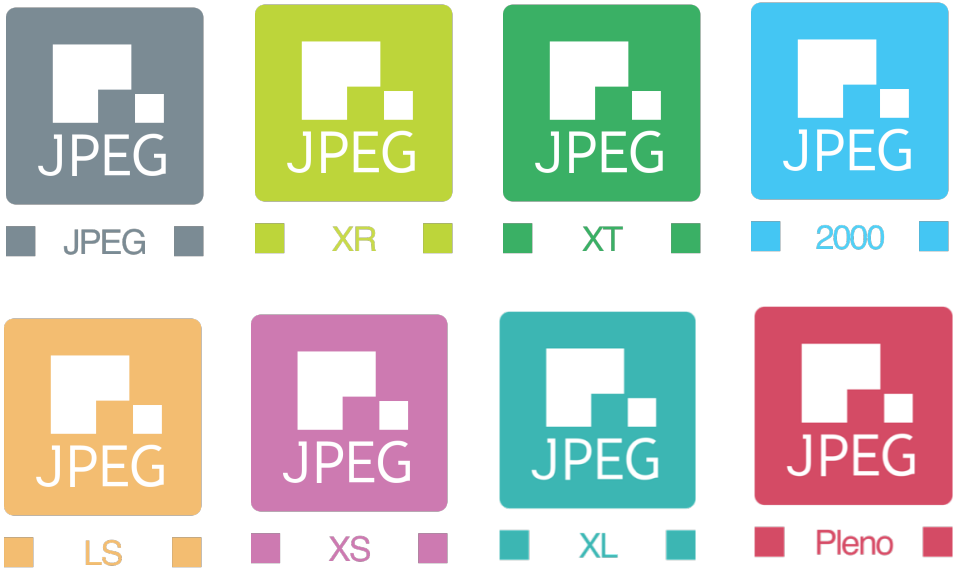
# About JPEG

# What is JPEG?

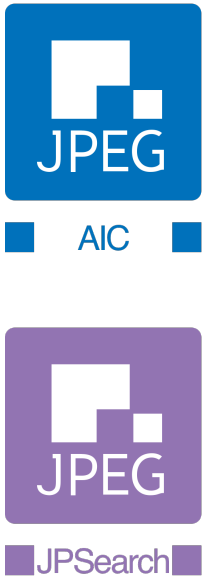



- Joint Photographic Experts Group
  - ISO/IEC
  - ITU-T
- Informally known as JPEG
  - WG1 in official communications

# JPEG Family of Standards







# Main objective of JPEG

- Contribute to enabling imaging/media ecosystems

# Biggest challenge in JPEG

- Anticipate trends and future needs in imaging/media



*"The best way to predict the future is to create it."*

# Working together

# JPEG Privacy and Security Standard

# JPEG Privacy and Security

- Part 4 of **JPEG Systems** (ISO/IEC 19566-4)
- Extends JPEG images with **protection and authenticity features**
  - Supported by the suite of JPEG standards including JPEG 1, JPEG 2000, JPEG XS, …
- International Standard published in 2020

# 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

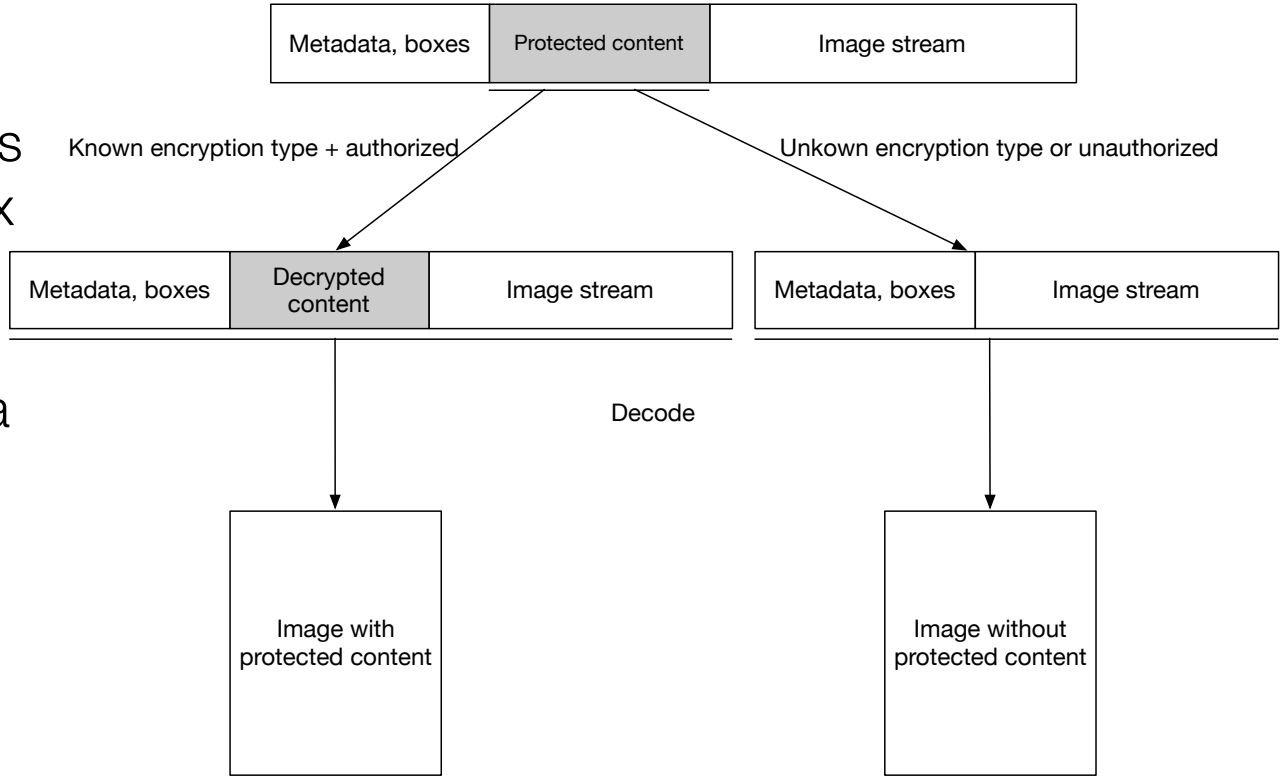
- Authenticity features:
  1. Solutions to support **integrity checking** of image data and/or embedded metadata to allow **identification and assessment of the master image** and identify derived or modified images from the master image.
  2. Solutions to support **avoiding stripping off metadata**, 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**.

# JPEG Privacy and Security - Aim & Approach

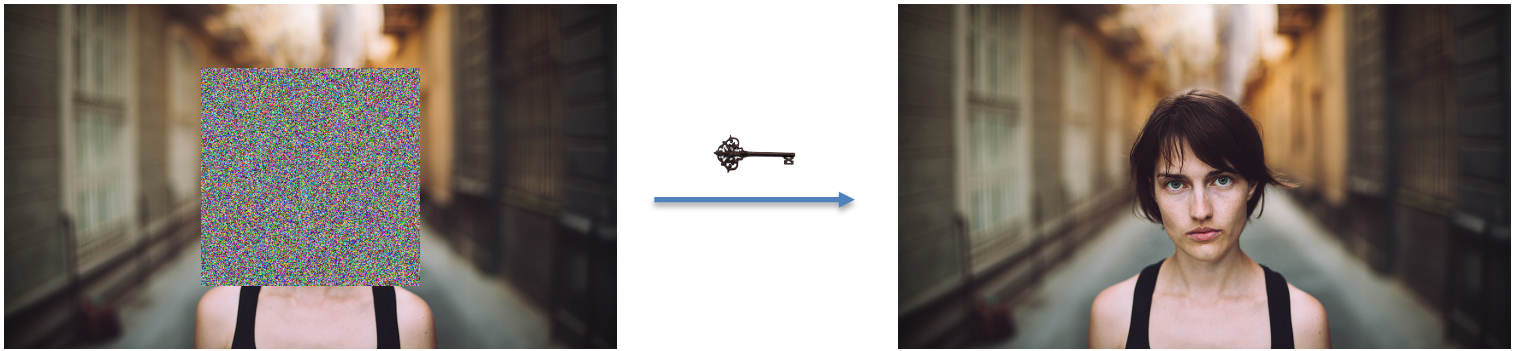
- Definition of tools to **support protection** and authenticity workflows in a **standardized way**
- Focus on **signaling syntax**
- Adoption of **existing technologies** for encryption etc.
- Focus on definition of **generic boxes**
- Boxes wrapped in 1 or more APP11 marker segments to support JPEG-1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

# Protection

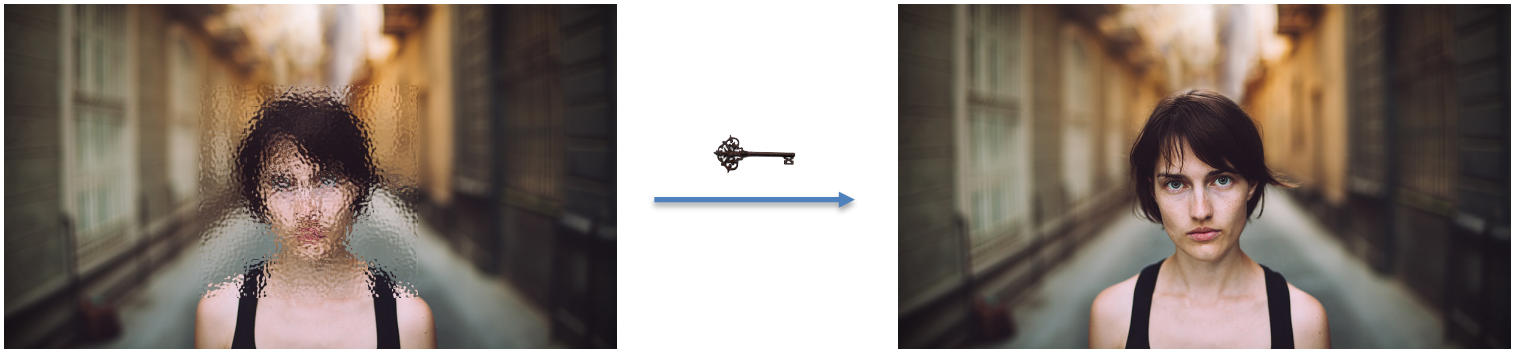
- **Protection box** wraps another encrypted box
- Since boxes are wrapped in APP11 marker segments data is split in chunks of 64kB which helps to support **file carving**



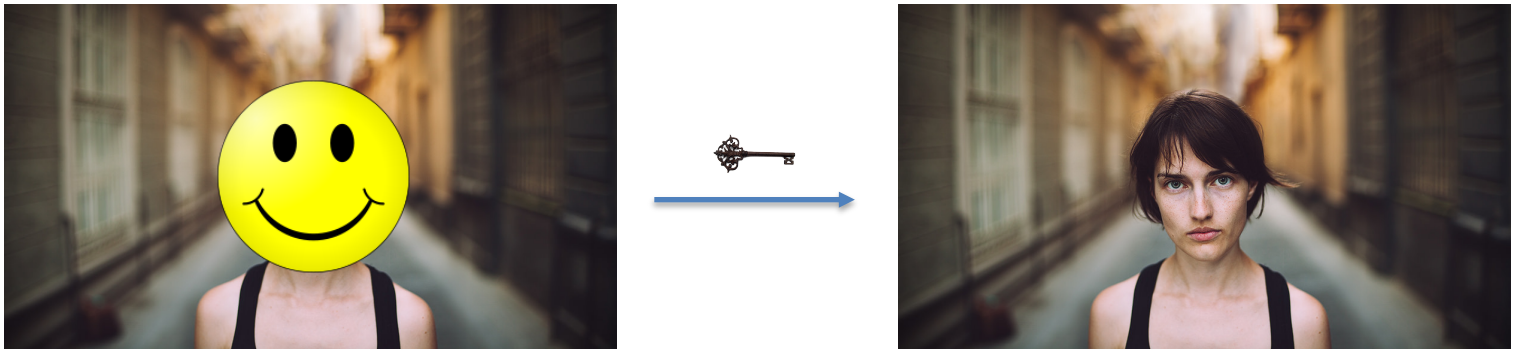
# Partial protection support



# Partial protection support

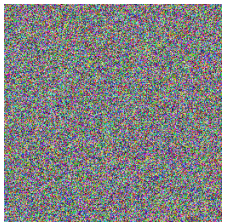


# Partial protection support



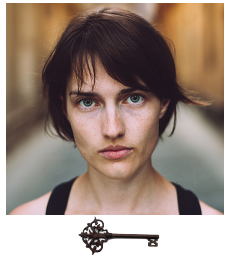
# Partial protection

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



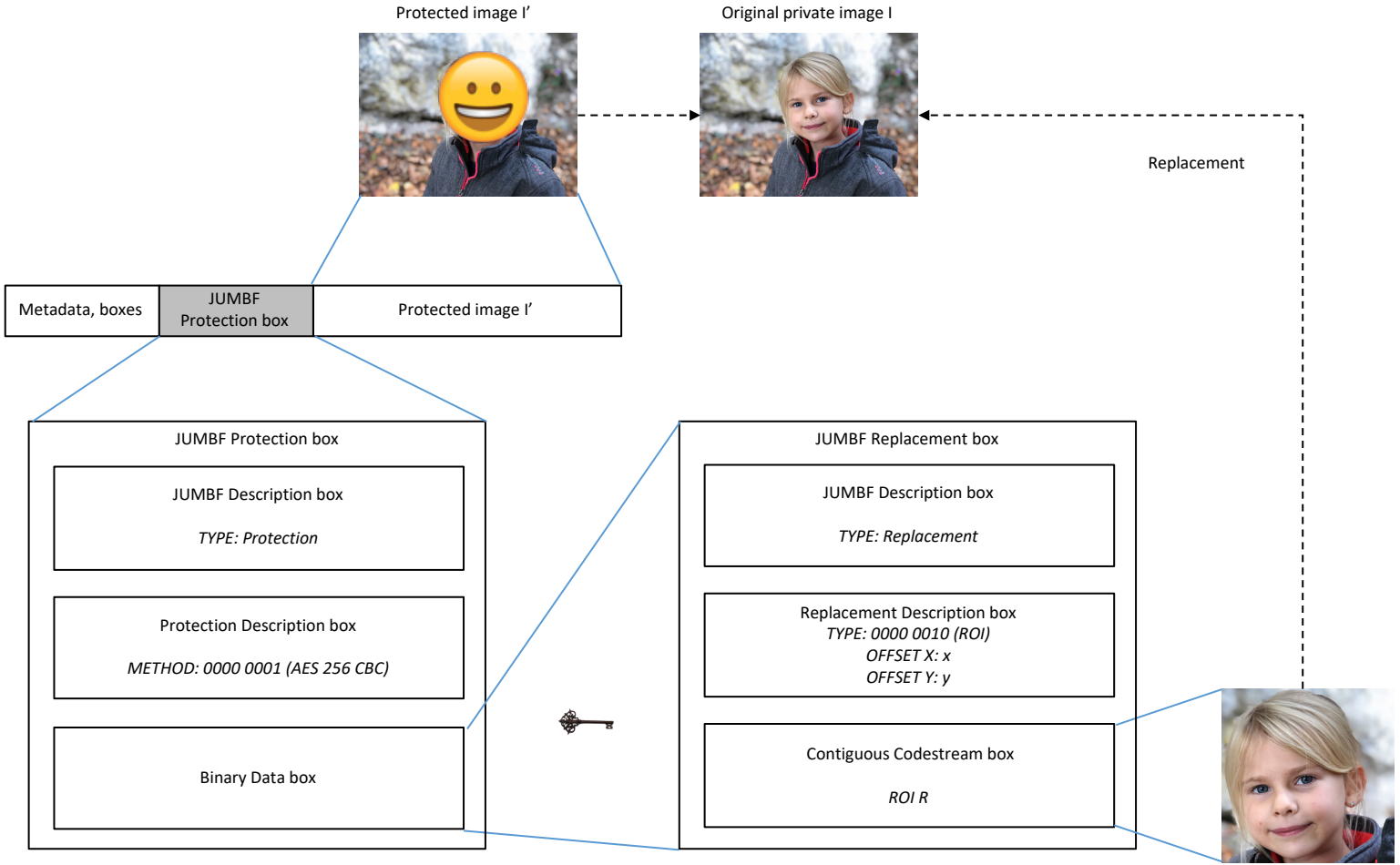
# Partial protection

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

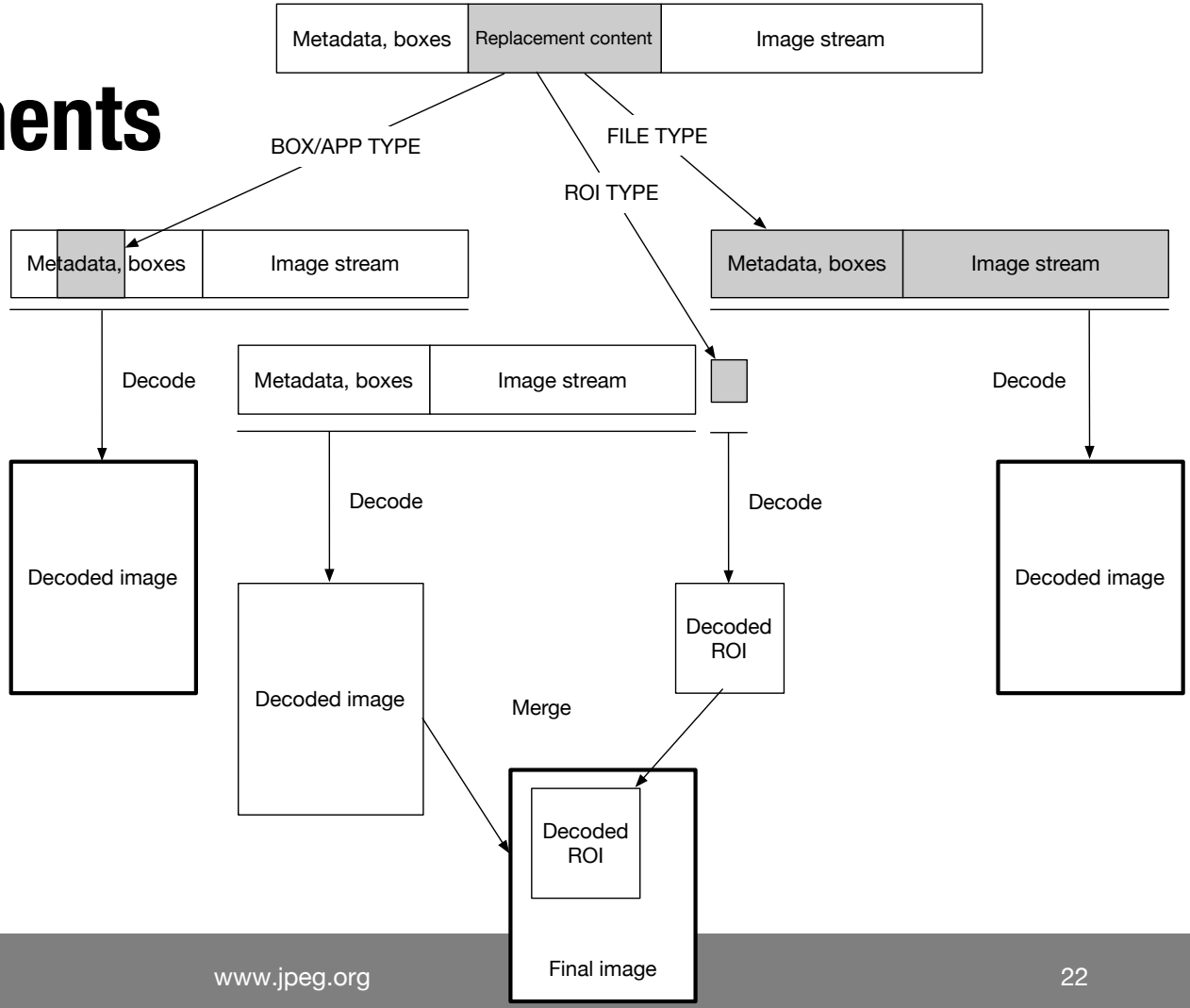


# Partial protection

| Header, metadata | Image stream<br>(Original image) |
| --- | --- |


Protected image I'
Original private image I
Replacement
Metadata, boxes
JUMBF Protection box
Protected image I'
JUMBF Protection box
JUMBF Description box
TYPE: Protection
Protection Description box
METHOD: 0000 0001 (AES 256 CBC)
Binary Data box
JUMBF Replacement box
JUMBF Description box
TYPE: Replacement
Replacement Description box
TYPE: 0000 0010 (ROI)
OFFSET X: x
OFFSET Y: y
Contiguous Codestream box
ROI R

# Replacements



# Metadata applications

- Metadata features
  - Access rules
  - IPR information
  - 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:
  - Private key
  - Watermarking
  - Third party registration authority
  - Blockchain / distributed ledger
- AhG on **Media Blockchain** initiated in January 2018

# Media Blockchain initiative

# Blockchain in a multimedia context

- Provides a **solution for authenticity use cases** without need for a third party register or watermarking
- Proven to be **immutable** and **community driven**
- Can provide a novel solution for **rewarding photographers**
- **Camera manufactures** could make a closed blockchain of all pictures taken with a particular camera
- **Registering image** in a blockchain as a **signature or feature vector**
- **Embedding a reference** to a blockchain inside an image

# Challenges

- **Privacy concerns** and right to be forgotten
- **Incentive** for mining?
- **Environmental impact** due to computational power / energy needs
  - Current estimate for Bitcoin is 73TWh/year, almost equal to energy consumption of Austria (72TWh/year)[1]
- **Alternatives for proof of works** still under investigation
  - **Consensus models for blockchain media transactions** (Stephen Swift, 1st JPEG Workshop on Media Blockchain Proceedings, ISO/IEC JTC1/SC29/WG1, wg1n81033, Vancouver, CAN, October 16th, 2018)

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

# 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)

# A simple but fundamental question…

- What is the impact of blockchain and distributed ledger technologies on JPEG standards

# Scope

- Which requirements can be **fulfilled by existing JPEG standards**?
- Which requirements are dealt with by **other standardization committees**?
- Which requirements need **new JPEG standards** or **extensions to existing JPEG standards**?

# 1st JPEG Workshop on Media Blockchain

## 16 October 2018, Vancouver, Canada

15:00-15:05 **ISO JPEG committee overview** (Touradj Ebrahimi)

15:05-15:30 **Overview of JPEG Privacy & Security and relation to Blockchain** (Frederik Temmermans)

15:30-16:00 **The multimedia blockchain: challenges and perspectives** (Eric Paquet)

16:15-16:45 **Managing Digital Information on Blockchains and Distributed Ledgers as Evidence** (Victoria Lemieux)

16:45-17:15 **Consensus models for blockchain media transactions** (Stephen Swift)

17:15-18:30 **Panel Discussion** (Moderator: Fernando Pereira)

# 2nd JPEG Workshop on Media Blockchain

## 22 January 2019, Lisbon, Portugal

16:00-16:20 **JPEG in a Nutshell** (Touradj Ebrahimi)

16:20-16:40 **JPEG Privacy and Security Activities** (Frederik Temmermans)

16:40-17:20 **Blockchain, Distributed Trust and Privacy** (Zekeriya Erkin)

17:20-17:50 **An overview of ISO/TC 307 - Blockchain and distributed ledger technologies** (Carlos Serrão)

17:50-18:30 **Panel Discussion** (Moderator: Fernando Pereira)

# 3rd JPEG Workshop on Media Blockchain

## 20 March 2019, Geneva, Switzerland

14:00-14:05 **Overview of JPEG Activities** (Touradj Ebrahimi)

14:05-14:20 **Privacy-preserving photo sharing based on blockchain** (Pablo Pfister)

14:20-14:35 **JPEG Privacy and Security Activities** (Frederik Temmermans)

14:35-15:00 **Adopting Blockchain in Image Security** (Deepayan Bhowmik)

15:00-15:30 **Use of blockchain for data privacy and protection**, (Bryan Ford)

16:00-16:30 **An Introduction of ITU-T DLT Standardization** (Wei Kai)

16:30-16:45 **Image forgery detection - A use case for blockchain and distributed ledger technologies** (Anthony Sahakian)

16:45-17:00 **FabToken: Tokenization on HyperLedger Fabric** (Kaoutar Elkhiyaoui)

17:00-18:00 **Panel Discussion** (Moderator: Fernando Pereira)

# 4th JPEG Workshop on Media Blockchain

## 16 July 2019, Brussels, Belgium

14:00-14:05 **Overview of JPEG Activities** (Fernando Pereira, IST-IT)

14:15-14:30 **JPEG Privacy and Security Activities** (Frederik Temmermans, imec-VUB)

14:30-15:00 **Blockchain & Privacy: Two cases from the government field** (Kristof Verslype, Smals)

15:00-15:30 **Trusted Archives of Digital Public Documents** (John Collomosse, University of Surrey, CVSSP)

16:00-16:30 **Blockchain for content licensing** (Robert Learney, Digital Catapult)

16:30-17:00 **Blockchain Application Domains & Use Cases for Media & Entertainment** (Jérôme Pons, Music won't stop)

17:00-18:00 **Panel Discussion & Closing** (Moderator: Fernando Pereira)

# Use cases

- **Trust, Privacy and Security in Media Consumption Chain**
  - Detection of unauthorized content usage
  - Integrity verification for forensic evidence
  - Insurance fraud detection
- **Transparent and Trusted Media Distribution Eco System**
  - Content ownership and monetization
  - Identifying copyright infringements
  - Facilitating DRM management, privacy policies, and IPR conditions
  - Means for copyright transfer and licensing to various stakeholders.

# Requirements

- Digital rights management
- Copyright protection
- Integrity
- Authenticity
- Traceability
- Privacy legislation compliance
- Asset distribution and monetisation
- Contract management (smart contract)
- Consensus model
- Content versioning
- Micropayments

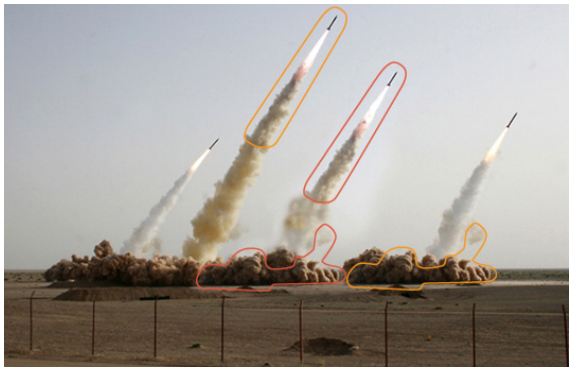
# JPEG Fake Media initiative

# Aim and Objectives

- Stakeholders' involvement to better **understand applications and scenarios** relevant to **fake media use cases**.
- **Identification of key requirements** for a standard in fake media.
- Ensuring **interoperability** between a wide range of applications dealing with fake media.
- A set of **standard metadata** to signal authenticity information along with relevant information.
- Standard mechanisms for **security and protection of integrity** both metadata and fake media content are desired.

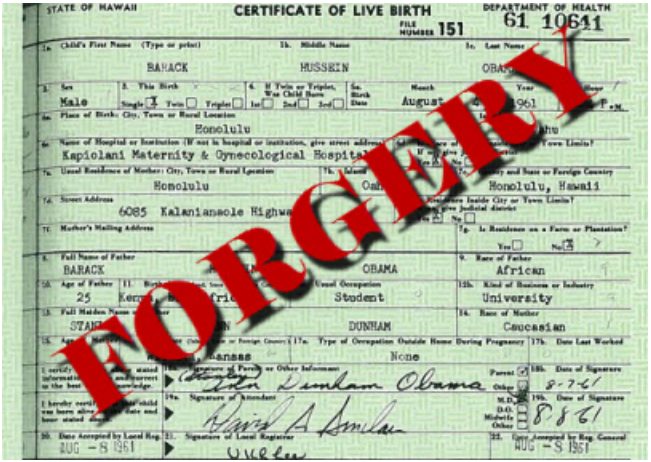
# Some Use Cases

- **Misinformation and fake news**
  - Deepfakes
  - Manipulated media
  - Authentic media used out of context
  - Manipulated framing



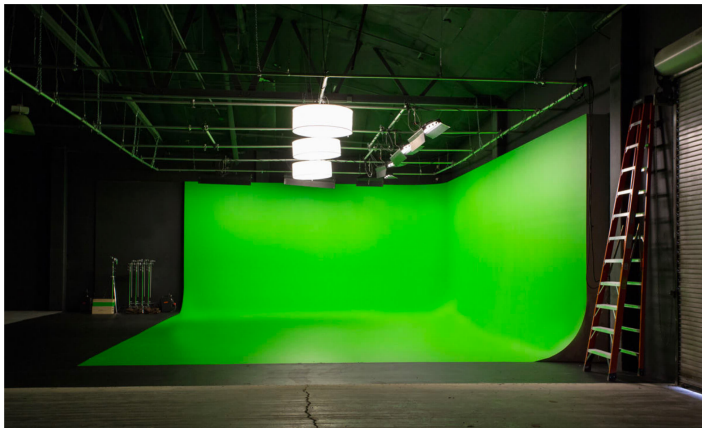

# Some Use Cases

- **Forgery / Media forensics**
  - Document forgery (e.g. IDs and passports)
  - Insurance fraud (e.g. pictures of accidents)
  - KYC (Know Your Customer) (e.g. fake identity)
  - Impostoring (e.g. impersonating a celebrity)




# Some Use Cases

- **Media manipulation**, e.g. enhancement, post-processing, restoration/colorization
  - Image editing software
  - Movie preservation
  - Film enhancement
  - Old movies restoration
- **Media creation**, e.g. green screen, processing and composition, deepfake for special effect
  - Movies special effects
  - Short content bursts
  - UGC (User Generated Content) e.g. TikTok, Triller, Adobe Spark
- **Media tracing**, e.g. provenance, content versioning, context
  - Picture and movies production



# Some Key Requirements

## Modification Description

- The standard shall provide means to describe how the content was created and/or modified.
- Authenticity labels: camera raw, enhanced, restored, colorized, edited, composed, deep fake, ...

## Secure signaling of authenticity information

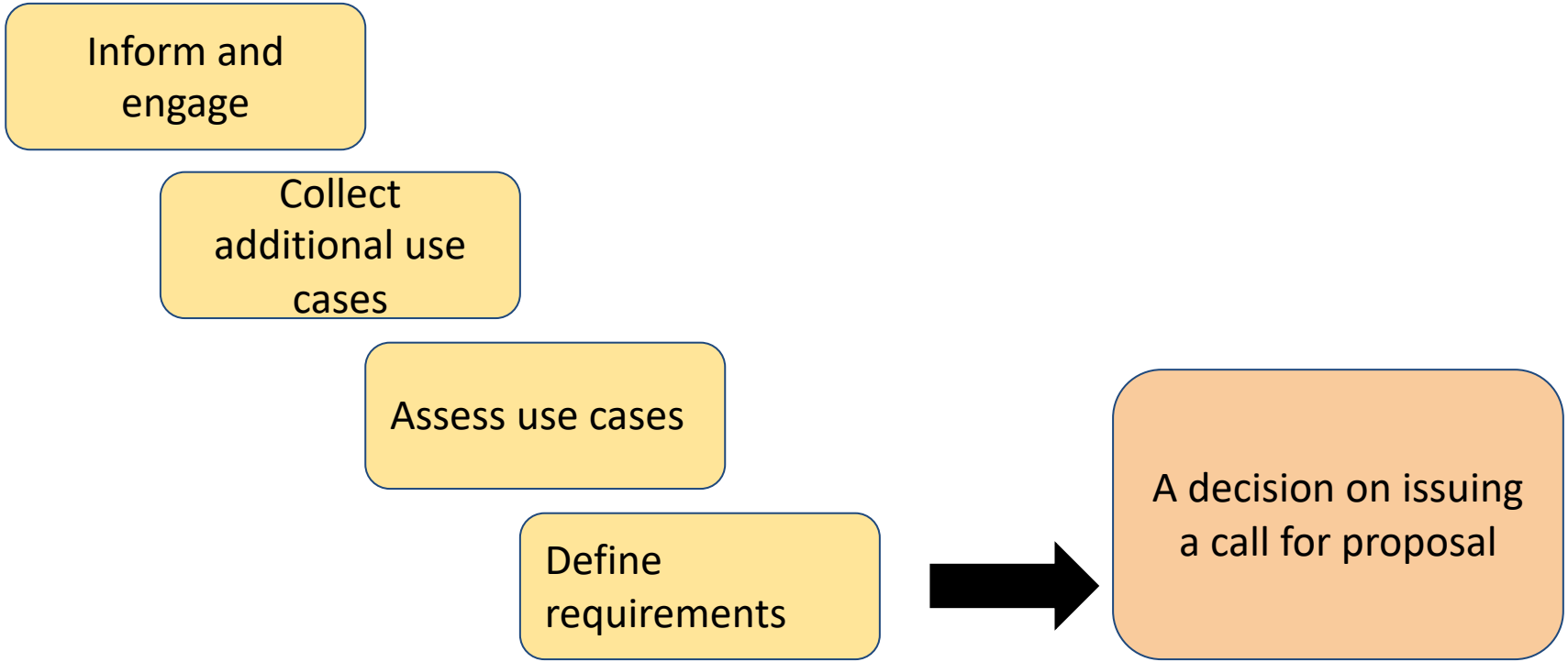
- The standard shall provide means to protect metadata information related to specifics of the modification.

# Next steps





# Standardization Roadmap



# Next Steps

- Collect fake media **use cases and requirements**.
- Survey on relevant **industry and government initiatives**.
- **Engage with stakeholders** and attract them to contribute.
- Organization of **workshops**

# How can you contribute?

- **Spread the word** and encourage participation.
- **Identify use cases** with text descriptions.
- **Identify requirements** with text descriptions.

# Thank you!

- **Key contacts**
  - Frederik Temmermans, ftemmerm@etrovub.be (AhG Chair)
  - Deepayan Bhowmik, d.bhowmik@ieee.org (AhG Co-Chair)
  - Fernando Pereira, fp@lx.it.pt (Requirements SG Chair)
  - Touradj Ebrahimi, Touradj.Ebrahimi@epfl.ch (Convenor)
- **Email reflector**: jpeg-fake-media@jpeglists.org
  - Subscribe via http://listregistration.jpeg.org