Summary of the 1st Workshop of JPEG Privacy and Security

Ambarish S Natu

Australia

Summary

- 7 contributors representing a spectrum of professions
  - NPO, News Organizations, Law Enforcement Agencies, Lawyers and Academia
    - **Michel Steidl** (IPTC), *“I don’t want to get my copyright stripped off”*
    - **Dr. Jeremy Malcolm** (Electronic Frontier Foundation), *“Copyright, Code and Creativity: A Note of Caution About DRM in JPEG”*
    - **Prof. Charlotte Waelde** (Univerity of Exeter), *“Cultural Heritage, Copyright and Code: Europeana Space as a case study”*
    - **Prof. Fred Truyen** (KU Leuven), *“Publishing Archival Photographs: concerns, pittfalls and their technical implications”*
    - **Jaime Delgado** (UPC), *“Privacy rules over JPEG images”*
    - **Lin Yuan** (EPFL), *“Privacy-Preserving Photo Sharing based on Secure JPEG”*
    - **Patrick De Smedt** (National Institute of Criminalistics and Criminology), *“Towards facilitating reliable recovery of JPEG pictures?”*

Michel Steidl (IPTC), “I don’t want to get my copyright stripped off”

- International Press Telecommunications Council – Global Standards Body for News Media
- A not-for-profit organisation with more than 50 members agencies
- Three Major Aspects of the IPTC Photo Metadata Standard
  - Describes what can be seen in an image
  - Write down administrative data
  - Defines data relevant for rights
- Supply Chain Metadata Changes
- Secure metadata against modifications without permission
  - Multi-Level Metadata Editing Permissions

Dr. Jeremy Malcolm (Electronic Frontier Foundation), "Copyright, Code and Creativity: A Note of Caution About DRM in JPEG"

- JPEG Privacy & Security may be interpreted as some form of DRM?
- Anti-circumvention laws threaten liability for those reporting vulnerabilities in DRM implementations
- Alternatives to DRM
  - Encrypting Metadata and not Encrypting Whole Image
  - Online Platforms preserve Image Metadata

Prof. Charlotte Waelde (Univerity of Exeter), “Cultural Heritage, Copyright and Code: Europeana Space as a case study”

- Identification of rights holders
- Extent of permissions to re-use
- Authenticity and integrity (moral rights)
- Data on how cultural heritage is used and re-used (and monetised) in the cultural economy
- Facilitate (collective) licensing
- Privacy: private information carried by images; privacy of person using images?

Prof. Fred Truyen (KU Leuven), “Publishing Archival Photographs: concerns, pittfalls and their technical implications”

- Challenges in European Photography
- Over 450,000 early photographs selection, digitization, enrichment, ingestion to Europeana
  - Analog to Digital
  - Privacy and Ethics
  - IPR
- Privacy Issues
  - Not everything in an archival collection can be published
  - The meaning changes over time, also the sensitivities
  - Privacy of people depicted

Patrick De Smedt (National Institute of Criminalistics and Criminology), “Towards facilitating reliable recovery of JPEG pictures?”

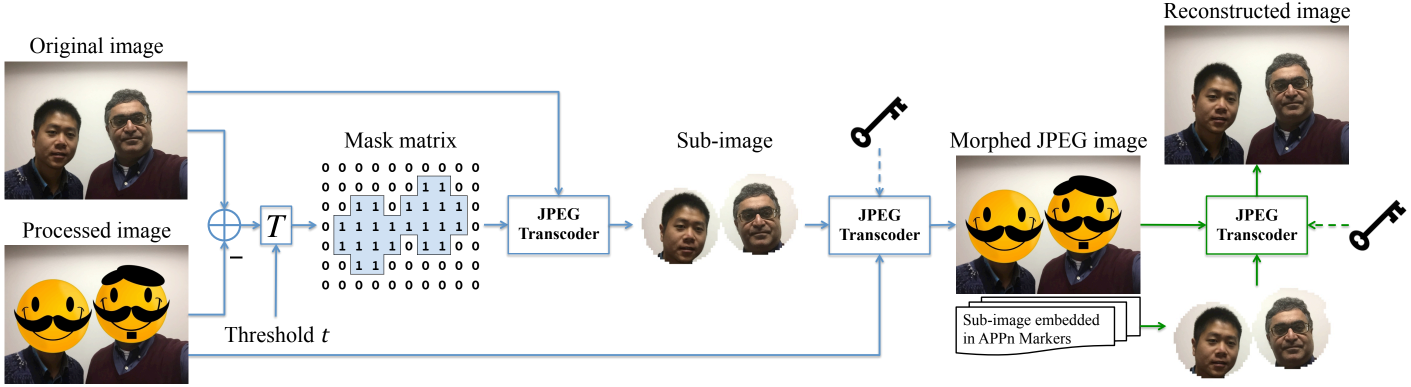
- Forensic Data Recovery
  - Consider file system fragmentation: a file can be split at any point, into one or multiple fragments
    - IDing JPEG remnants: within data dump
    - IDing JPEG remnants: as being parts of the same or a similar file
    - regrouping and matching JPEG remnants to reconstruct files
    - robustness against loss of meta-data and/or any part of the data (certain fragments)

Jaime Delgado (UPC), “Privacy rules over JPEG images”

- MIPAMS architecture for a solution
  - Definition of privacy rules to control access to JPEG images
    - eXtensible Access Control Markup Language (XACML)
  - JPSearch metadata as placeholder for policies

Lin Yuan (EPFL), "Privacy-Preserving Photo Sharing based on Secure JPEG"

- Secure JPEG
  - JPEG Scrambling
  - JPEG ***Transmorphing -*** APP marker in JPEG header ***holds Metadata information***



$$\begin{matrix} 0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&1&1&0&0\\ 0&0&1&1&0&1&1&1&1&0\\ 0&1&1&1&1&1&1&1&1&0\\ 0&1&1&1&1&0&1&1&0&0\\ 0&0&1&1&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0 \end{matrix}$$

- Photo Sharing Architecture

SUMMARY OF REQUIREMENTS

- Secure metadata against modifications without permission
    - Suggested Layers of Protection – by limiting editing of metadata.
- Address Intellectual Property Rights (IPR)
    - Identify Master and Copies
- Sensitivities with Archival Rights
    - Change with Time – Maintain Image Integrity through Secure Mechanism
- Define Privacy Rules/Policies
    - The Who, How/When/Where and What