Secure JPEG Scrambling Enabling Privacy in Photo Sharing

Lin Yuan, Pavel Korshunov, Touradj Ebrahimi
Multimedia Signal Processing Group, EPFL
De-ID workshop, Ljubljana, Slovenia
Motivation

- Social network and cloud service
- Easy and fast photo sharing, huge amount
Motivation

• Privacy scandals
  – Governmental surveillance, e.g. PRISM
  – Leakage of celebrities private photos

• Existing privacy protection solutions
  – Rudimental
  – Limited degree of protection

• People lack awareness of privacy issue
Goal and Objectives

• Goal
  – Diminish privacy risks in online photo sharing, while preserving usability.

• Objectives
  – Efficient and secure JPEG scrambling scheme
  – Privacy-preserving photo sharing architecture, preventing privacy breaches against public organizations and individuals
Secure JPEG Scrambling

- Overview
  - Secure and reversible: relying on secret key
  - Backward compatible: JPEG APP11 marker
  - Fast and low overhead: integrate in coding/transcoding
Secure JPEG Scrambling

- Two modes of scrambling and descrambling
  1. JPEG encoding/decoding
Secure JPEG Scrambling

- Two modes of scrambling and descrambling

II. JPEG transcoding
Secure JPEG Scrambling

• The algorithm

Original JPEG photo

Scrambled JPEG photo

Insert parameters in JPEG header

ROI, Level, Key

Signs of DCT coefficients

Pseudo-random number

1 2 3 4 5 6 7 8 9

Metadata

k₁

k₂
Secure JPEG Scrambling

- Variable strength granularity

<table>
<thead>
<tr>
<th>Original</th>
<th>Low</th>
<th>Medium</th>
<th>High</th>
<th>Ultra-high</th>
</tr>
</thead>
</table>

![Images showing original and scrambled images at different levels of granularity](image-url)
Secure JPEG Scrambling

• Experiment: Strength vs. Privacy vs. Overhead

<table>
<thead>
<tr>
<th></th>
<th>Original image</th>
<th>Low-level scrambled</th>
<th>Medium-level scrambled</th>
<th>High-level scrambled</th>
<th>Ultra-high-level scrambled</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO. of detected faces</td>
<td>3944</td>
<td>1638</td>
<td>14</td>
<td>11</td>
<td>10</td>
</tr>
<tr>
<td>AVG. overhead (only face regions scrambled)</td>
<td>1.87%</td>
<td>2.04%</td>
<td>2.15%</td>
<td>3.15%</td>
<td></td>
</tr>
<tr>
<td>AVG. overhead (whole image scrambled)</td>
<td>1.87%</td>
<td>4.89%</td>
<td>5.96%</td>
<td>18.41%</td>
<td></td>
</tr>
</tbody>
</table>

- 1000 images, max. pixel resolution 1024 x 1024, file size 100 KB ~ 330 KB
- OpenCV, Haar Feature-based Cascade face detector
Photo Sharing Architecture

- Assumptions:
  - Client device/application completely trusted
  - Server minimally trusted (for revocation)
  - Social network or cloud service not trusted

- Principles
  - Photo data protection/recovery ONLY on client device
  - ONLY protected data “flying” on cloud
Photo Sharing Architecture

Friend relationship:
- User 1 & 2: ✔
- User 1 & 3: ✔
- User 2 & 3: ✗

Social Networking Services

- **Sender-side operations**
  - Protection and upload
- **Server-side operations**
  - Hosting and Access control
- **Recipient-side operations**
  - Download and Reconstruction
Prototype APP: ProShare

- iOS based
- Facebook interaction
Conclusion

- Efficient and secure privacy protection filter based on JPEG scrambling
- Easy-to-use and privacy-preserving architecture for online photo sharing
- Prototype application
Future Work

• Context-aware privacy protection
• Subjective privacy evaluation
• Inclusion of an easy to use PKI
Thanks for attention.