Legacy JPEG compliant transmorphing to preserve privacy in social networks

Touradj Ebrahimi

Multimedia Signal Processing Group, EPFL

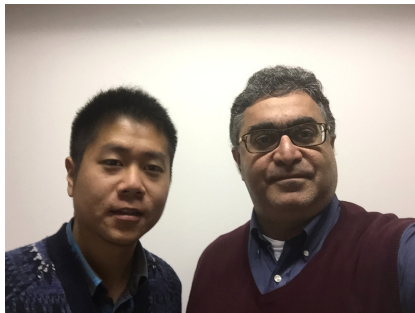ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Goal and Approaches

- Goal
  - Diminish privacy risks in online photo sharing, while preserving a maximal usability

- Approaches
  - Secure JPEG:
    - **JPEG Scrambling**
    - **JPEG Transmorphing**
  - **Photo sharing architecture based on a Public Key Infrastructure (PKI)**

Examples

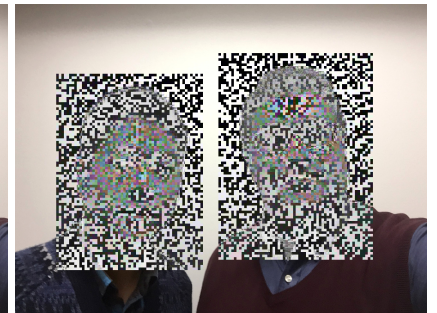- Different visual privacy protection tools
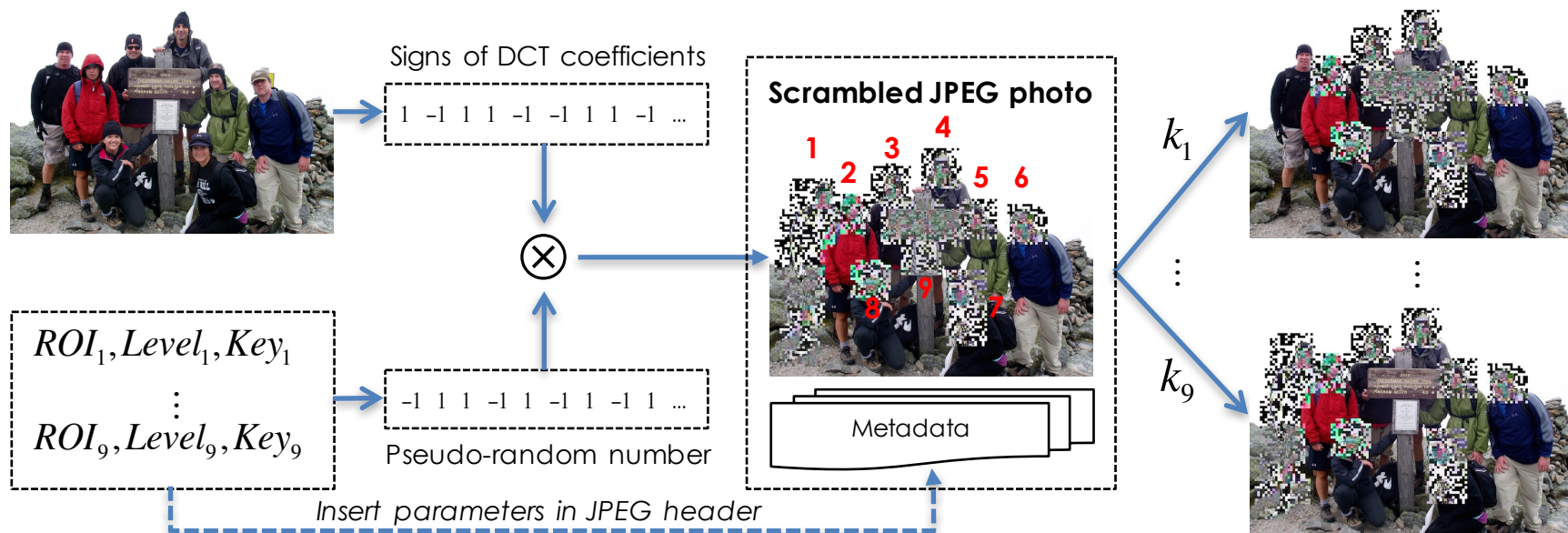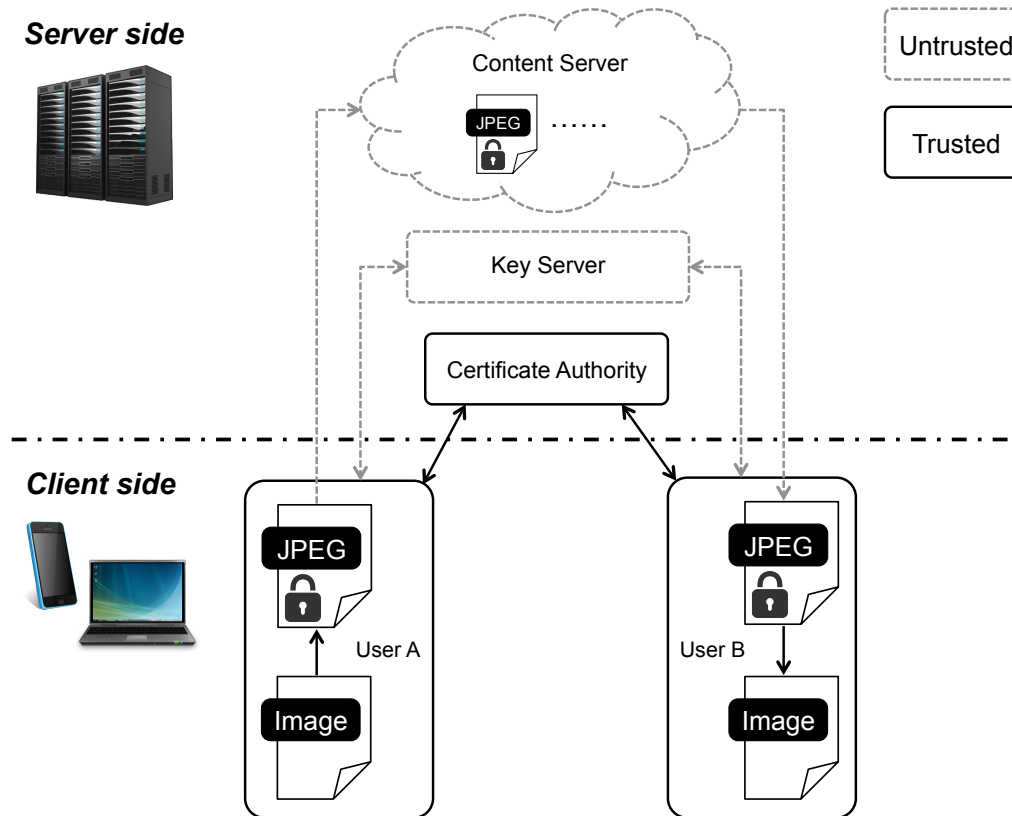
Original	Masking	Pixelation	Inpainting	Scrambling

JPEG Scrambling

- Randomly change the signs of DCT coefficients

Original JPEG photo

Signs of DCT coefficients

1 –1 1 1 –1 –1 1 1 –1 ...

$ROI_1, Level_1, Key_1$

$\vdots$

$ROI_9, Level_9, Key_9$

–1 1 1 –1 1 –1 1 –1 1 ...

Pseudo-random number

$\otimes$

Scrambled JPEG photo

Metadata

Insert parameters in JPEG header

k_1

$\vdots$

k_9

Photo Sharing Architecture

Server side

Content Server

JPEG

Untrusted

Trusted

Key Server

Certificate Authority

Client side

JPEG

User A

Image

JPEG

User B

Image

Photo Sharing Architecture

- Sender-side operations
  - Protection and upload
- Server-side operations
  - Hosting and Access control
- Receiver-side operations
  - Download and Reconstruction

JPEG Transmorphing - Example 1

original
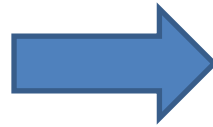
protected in JPEG

JPEG Transmorphing - Example 1
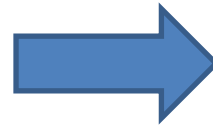
- **Protection**

Protection Pipeline
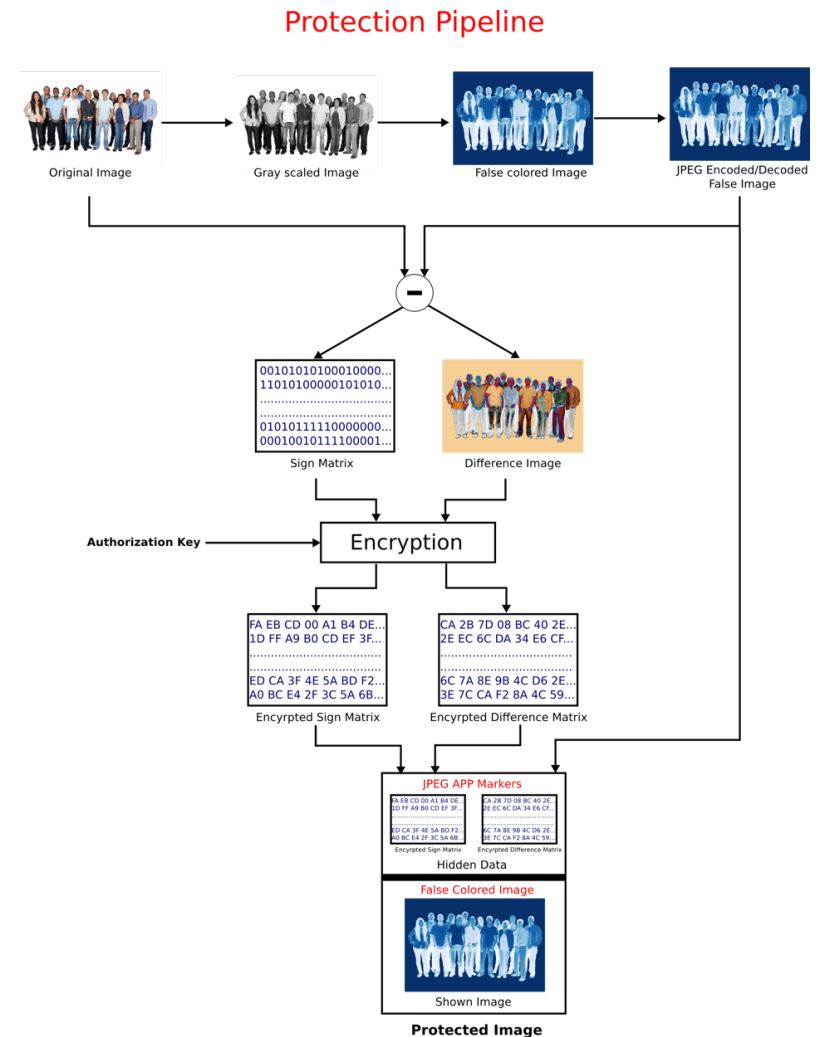
JPEG Transmorphing - Example 1

protected in JPEG

recovered original

JPEG Transmorphing - Example 1

- **Recovery**

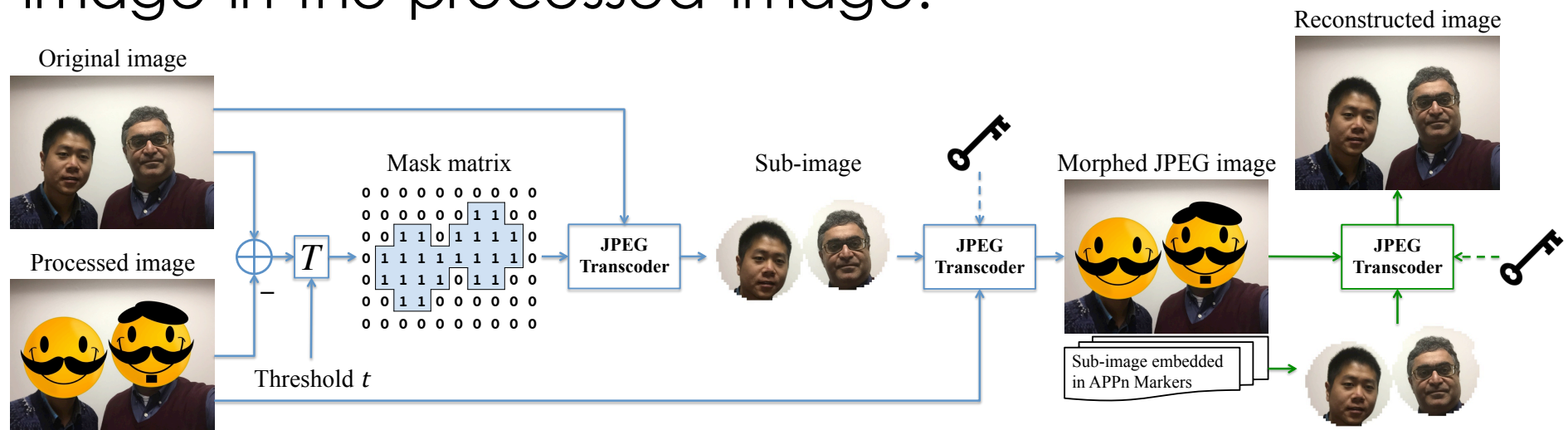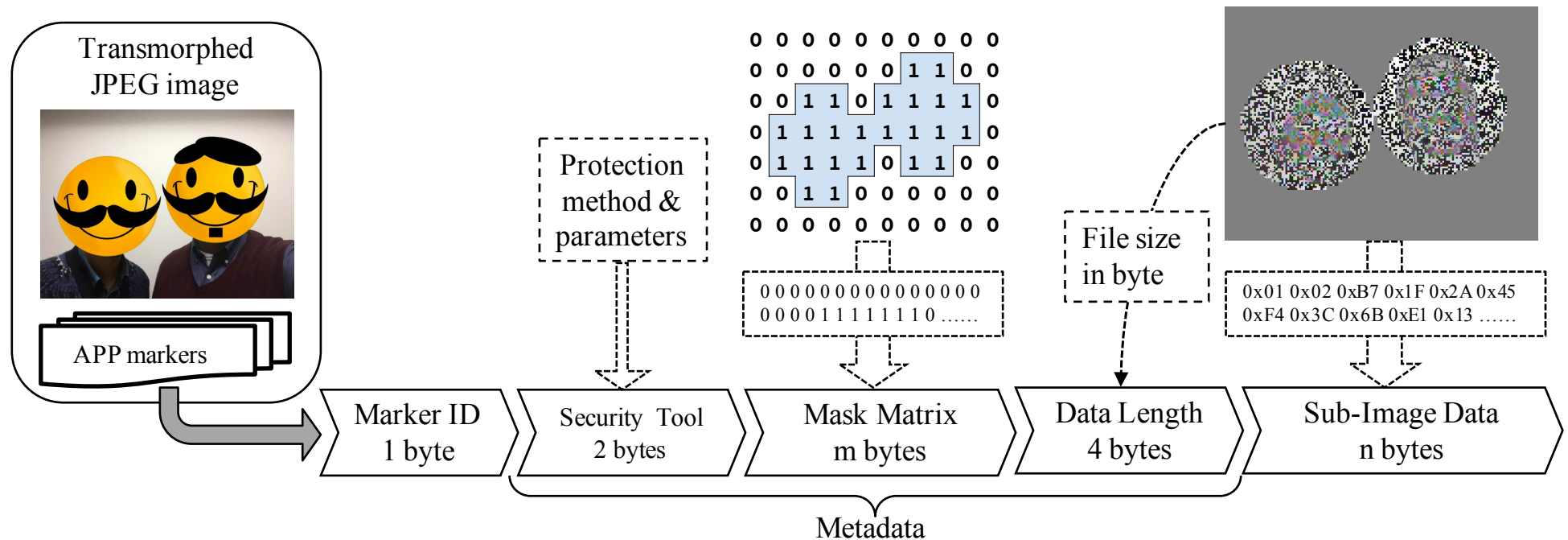Recovering Pipeline
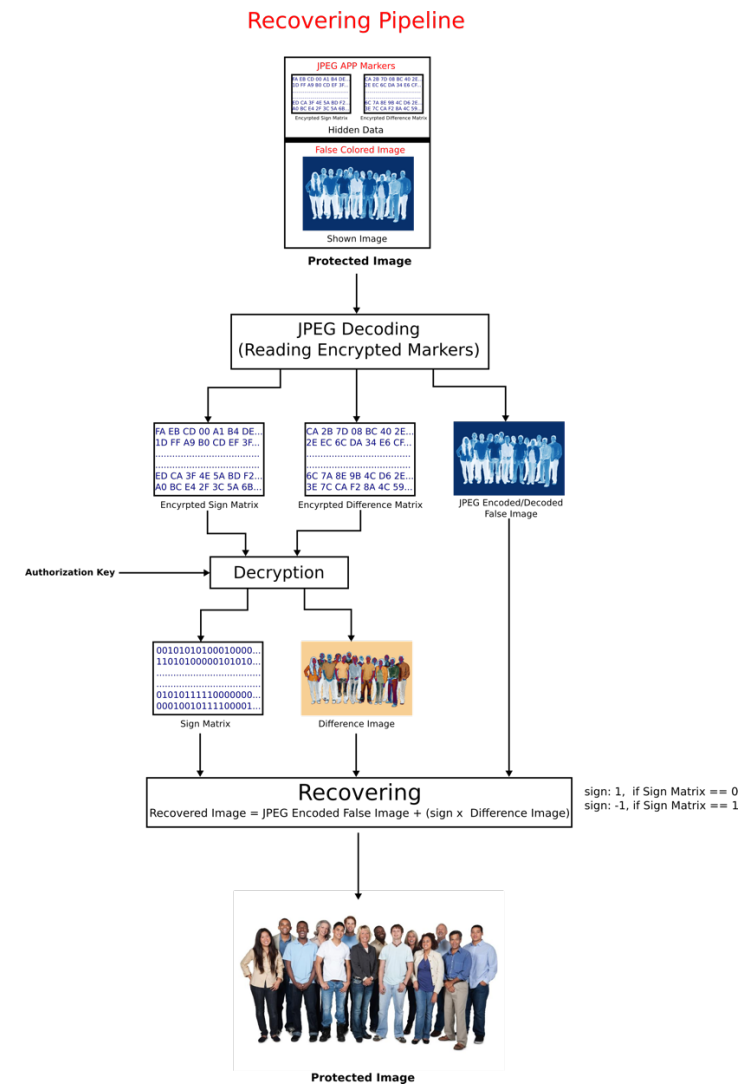
JPEG Transmorphing – Example 2

- Converting an image to processed version while preserving sufficient information about the original image in the processed image.

JPEG Transmorphing – Example 2
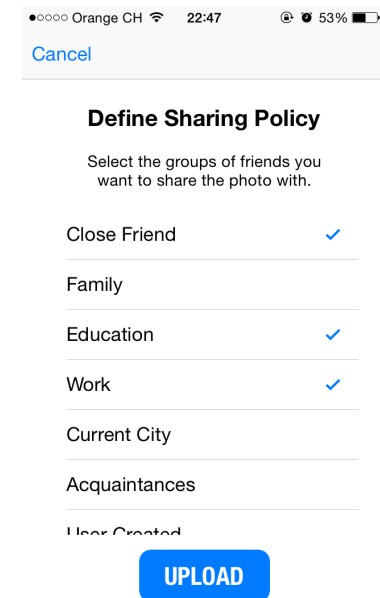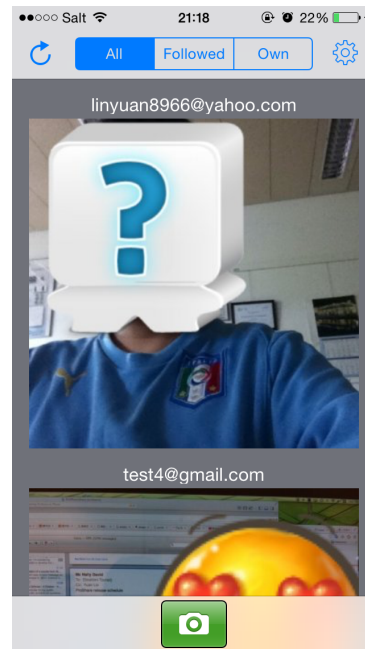
- APP marker in JPEG header

Transmorphed JPEG image

APP markers

Protection method & parameters

0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 1 1 1 1 1 1 0 ......

Protected Sub-image

File size in byte

0x01 0x02 0xB7 0x1F 0x2A 0x45
0xF4 0x3C 0x6B 0xE1 0x13 ......

| Marker ID 1 byte | Security Tool 2 bytes | Mask Matrix m bytes | Data Length 4 bytes | Sub-Image Data n bytes |

Metadata

Prototype and Demo

- Prototype application: *ProShare*
  - iOS
  - Android

ProShare

Thanks!
Question?

Acknowledgements: Lin Yuan (EPFL), Serdar Ciftci (METU), Ahmed Oguz Aykuz (METU)