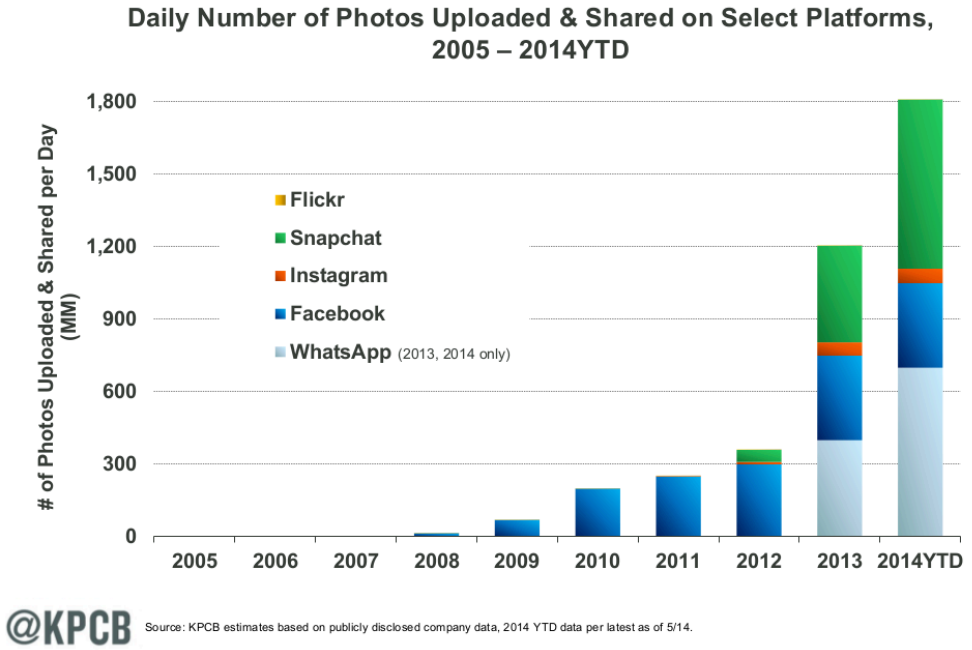
Secure JPEG Scrambling Enabling Privacy in Photo Sharing

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

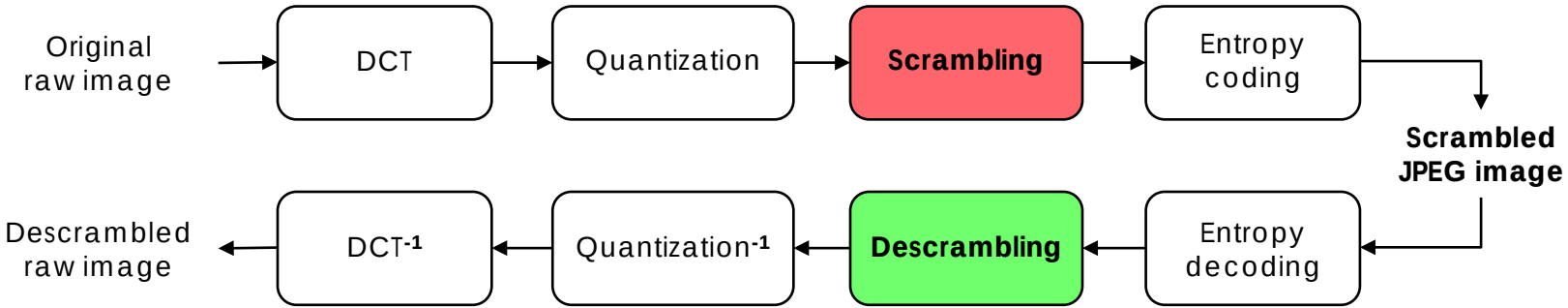
- Goal
  - Diminish privacy risks in online photo sharing, while preserving usability.
- Objectives
  - Efficient and secure JPEG scrambling scheme
  - Privacy-preserving photo sharing architecture, preventing privacy breaches against public organizations and individuals

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

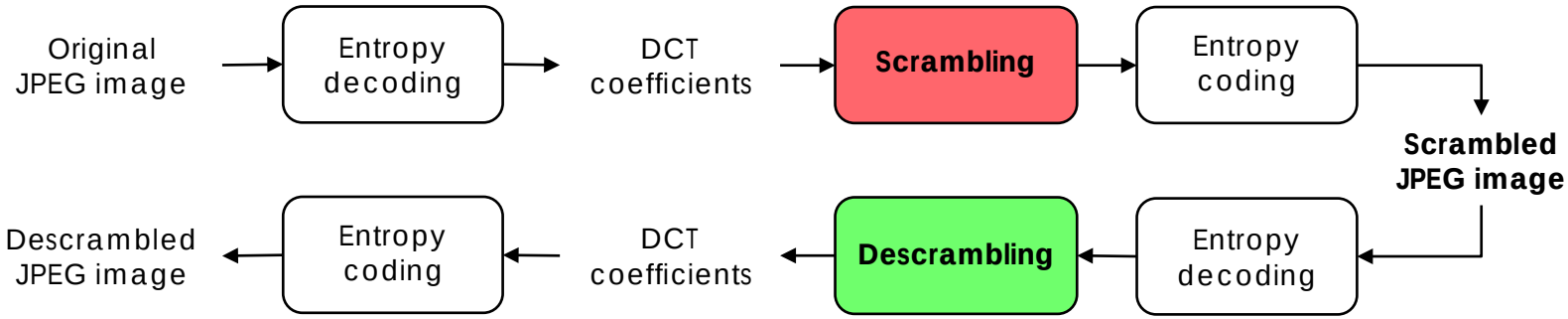
- Two modes of scrambling and descrmbling
  - **I. JPEG encoding/decoding**



Secure JPEG Scrambling

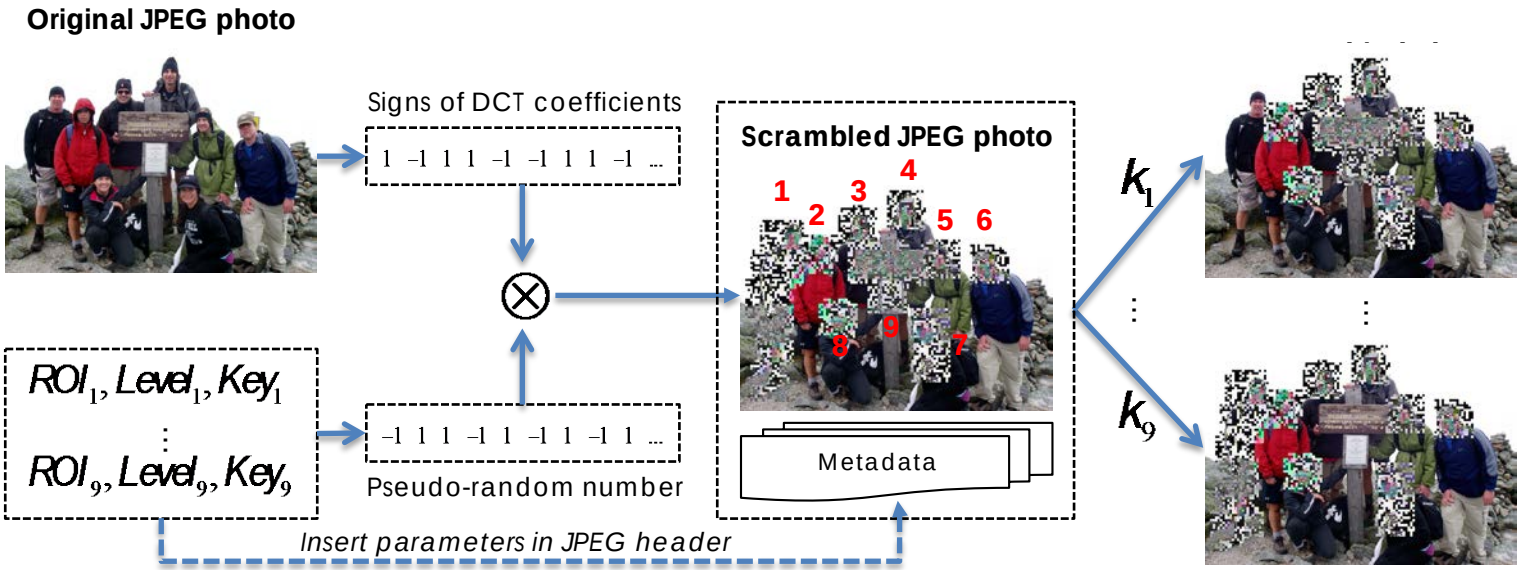
- Two modes of scrambling and descrmbling

II. JPEG transcoding



Secure JPEG Scrambling

- The algorithm



Secure JPEG Scrambling

- Variable strength granularity

Original Low Medium High Ultra-high

Secure JPEG Scrambling

- Experiment: Strength vs. Privacy vs. Overhead

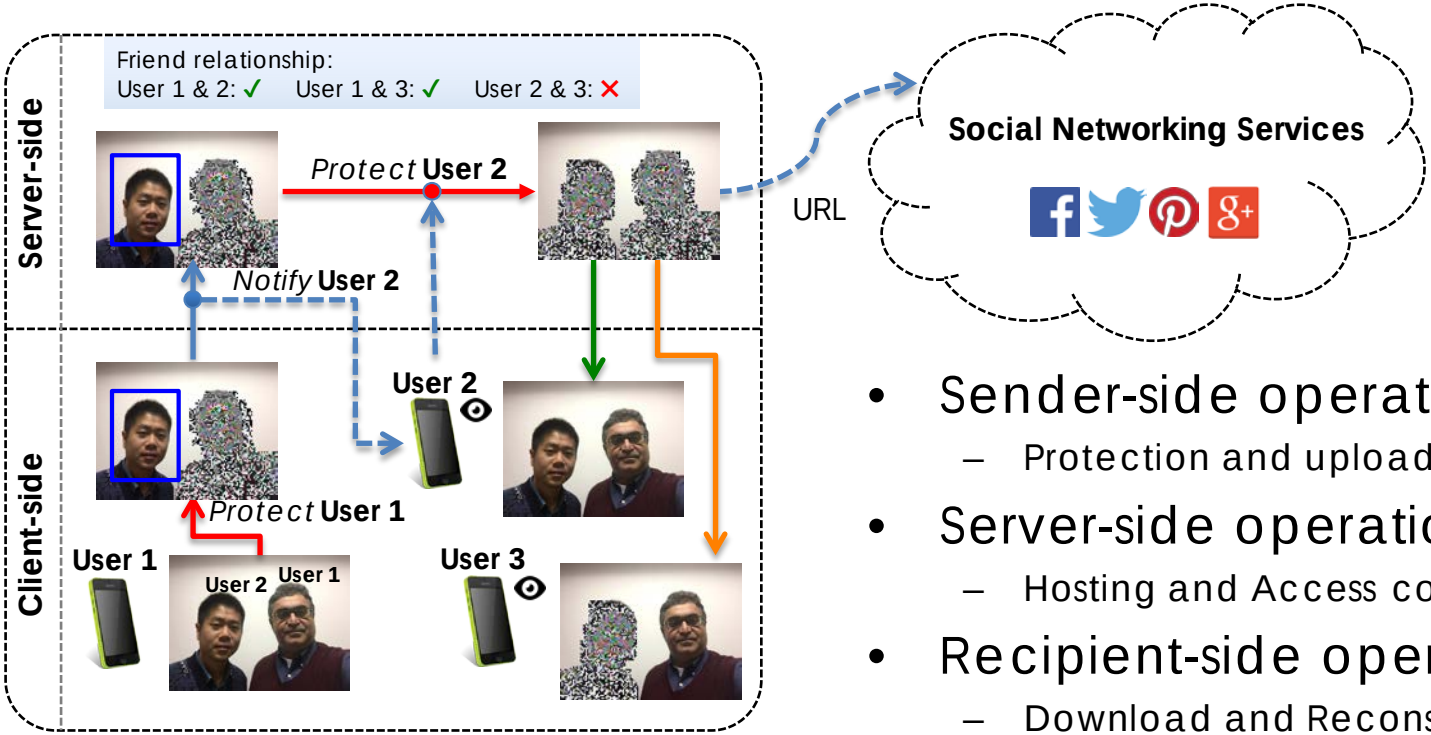
	Original image	Low-level scrambled	Medium-level scrambled	High-level scrambled	Ultra-high-level scrambled
NO. of detected faces	3944	1638	14	11	10
AVG. overhead (only face regions scrambled)		1.87%	2.04%	2.15%	3.15%
AVG. overhead (whole image scrambled)		1.87%	4.89%	5.96%	18.41%

- 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

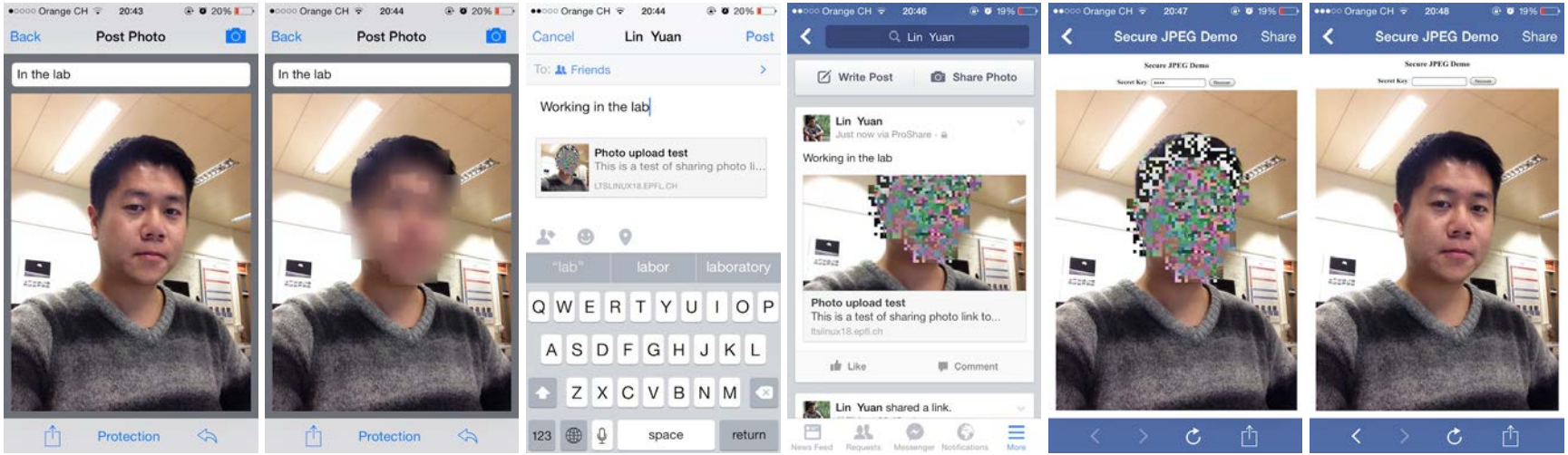
Photo Sharing Architecture



- 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.