P3: Toward Privacy-Preserving Photo Sharing

Moo-Ryong Ra, Ramesh Govindan, and Antonio Ortega

Networked Systems Laboratory & Signal and Image Processing Institute

University of Southern California

Cloud-based Photo Sharing Services (PSPs)

PSPs

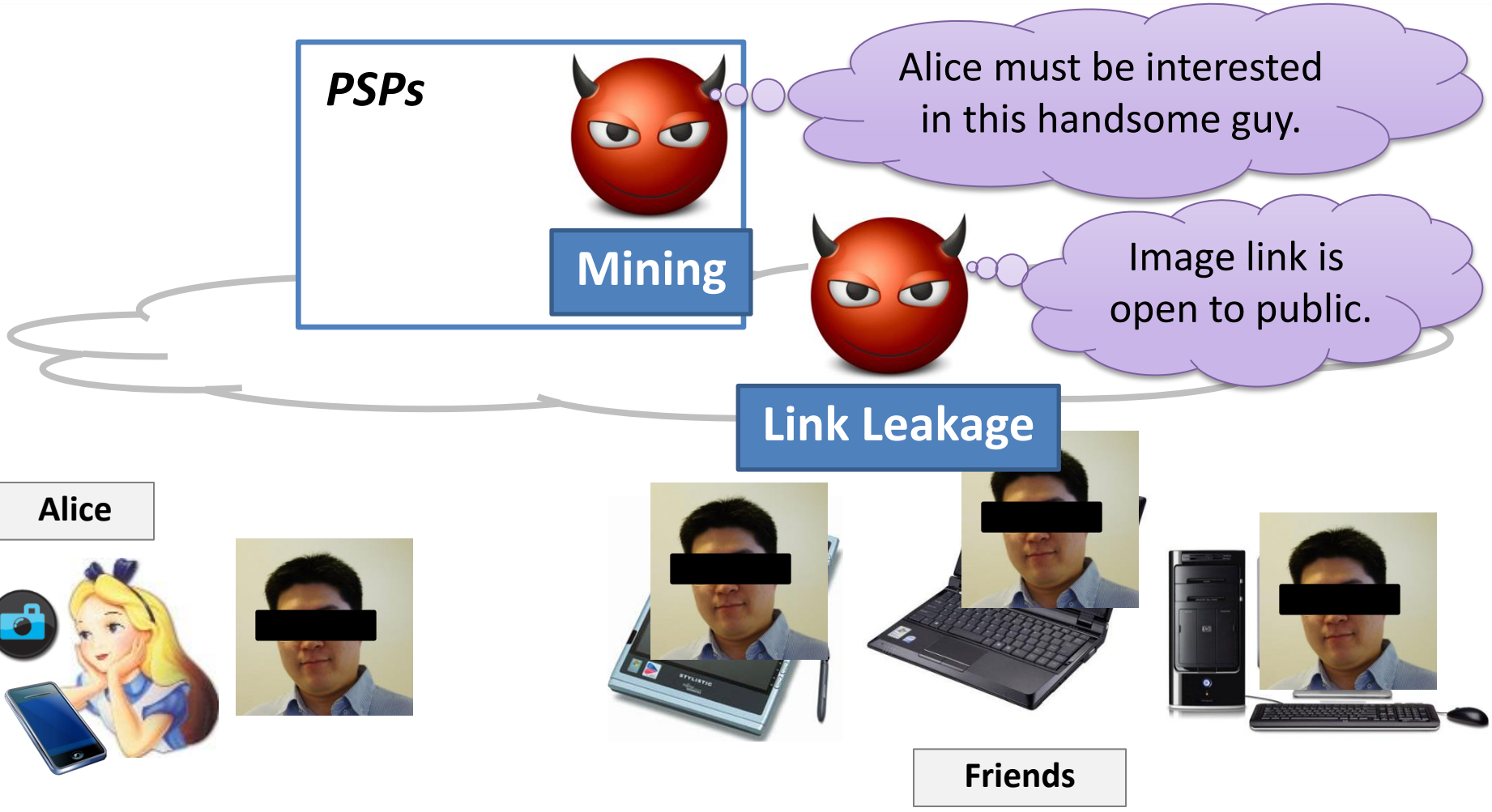
facebook

flickr

Instagram

However, there are serious privacy concerns

The Case of Privacy Infringement by PSPs



Today we have no choice but to trust PSPs

These Privacy Concerns Are Real

Photobucket leaves users exposed

August 09, 2012 | By Julia Grenberg, CNN

CNN.com, August 9, 2012

TECHNOLOGY | June 8, 2011

Facebook Again in Spotlight on Privacy

Photo-Recognition Technology Sparks Privacy Concerns

Wall Street Journal, June 8, 2011

Germans Reopen Investigation on Facebook Privacy

By KEVIN J. O'BRIEN
Published: August 15, 2012

New York Times, August 15, 2012

Angry with Instagram? These 'invisible' data brokers sell your privacy every day

By Bob Sullivan

NBC News, December 19, 2012

Cloud-side Processing for Mobile Devices

facebook

flickr

Picasa

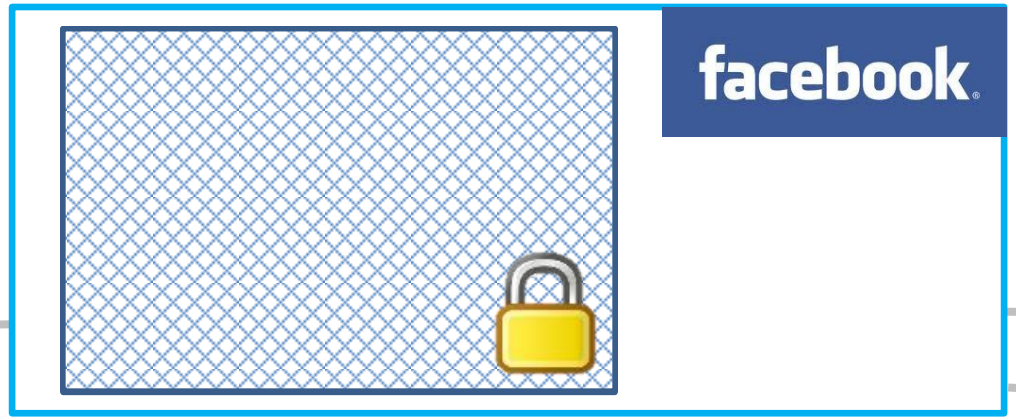
Alice

Friends

Cloud-side processing is often useful for mobile devices in many ways

Question: Can we protect users' privacy while still performing cloud-side image transformation?

Full Encryption?

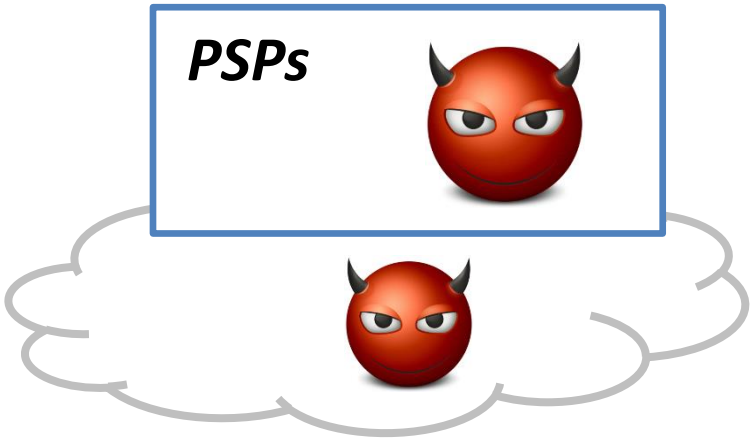


We will lose benefits
provided by cloud-side processing

Goals, Threat Model, and Assumptions

Preserving users' privacy
with cloud-side processing

- **Privacy and Attack Model**
  - Unauthorized access
  - Algorithmic recognition
- **We trust**
  - Mobile devices' HW and SW
- **We don't trust**
  - Eavesdropper on the network
  - "Honest-but-curious" PSPs



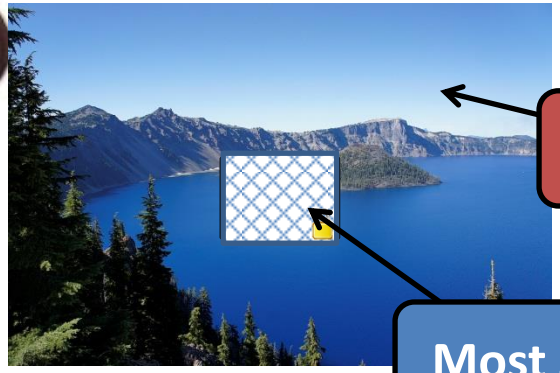
High-level Description of Our Approach

SECRET PART

PUBLIC PART

PSPs

Alice



Least Significant Bits

Most Significant Bits

Bob

P3 Requirements

PSPs

Storage

Standard ***Cloud-side***

Our algorithm and system, collectively called P3, realizes this capability

Privacy ***Processing***

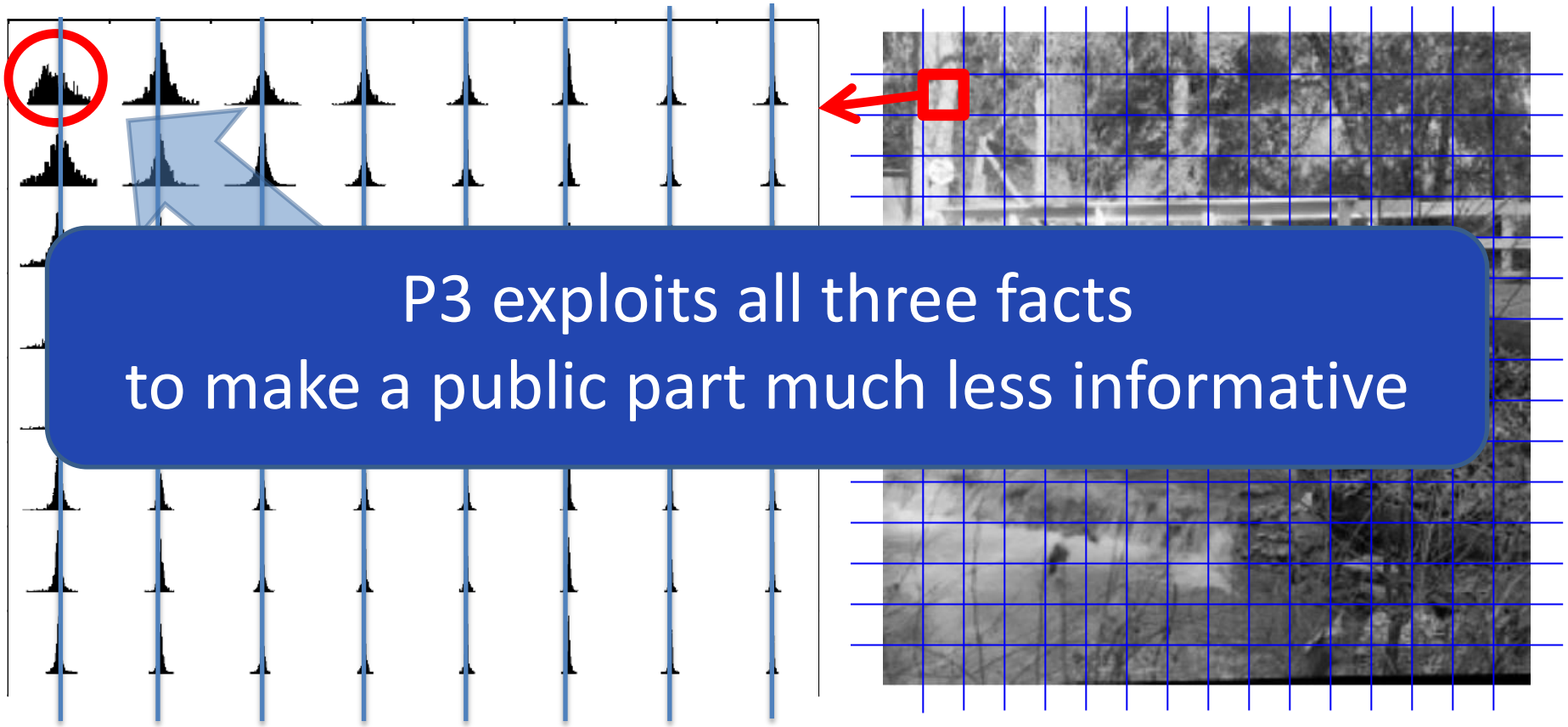
Transparent
Deployment

Alice

Bob

P3 Algorithm: Why It Works

- Exploiting the characteristics of DCT coefficients in JPEG.

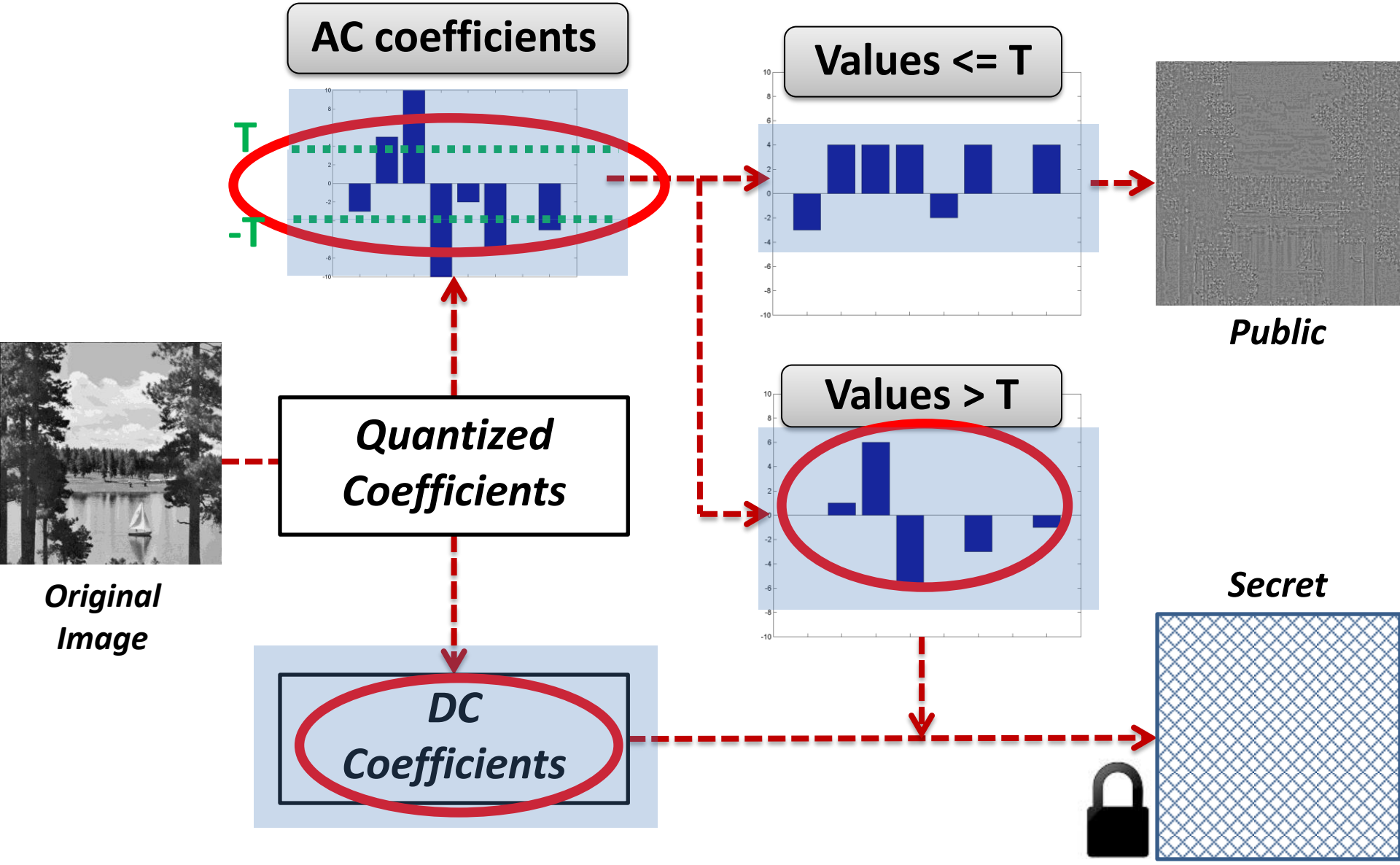


P3 exploits all three facts
to make a public part much less informative

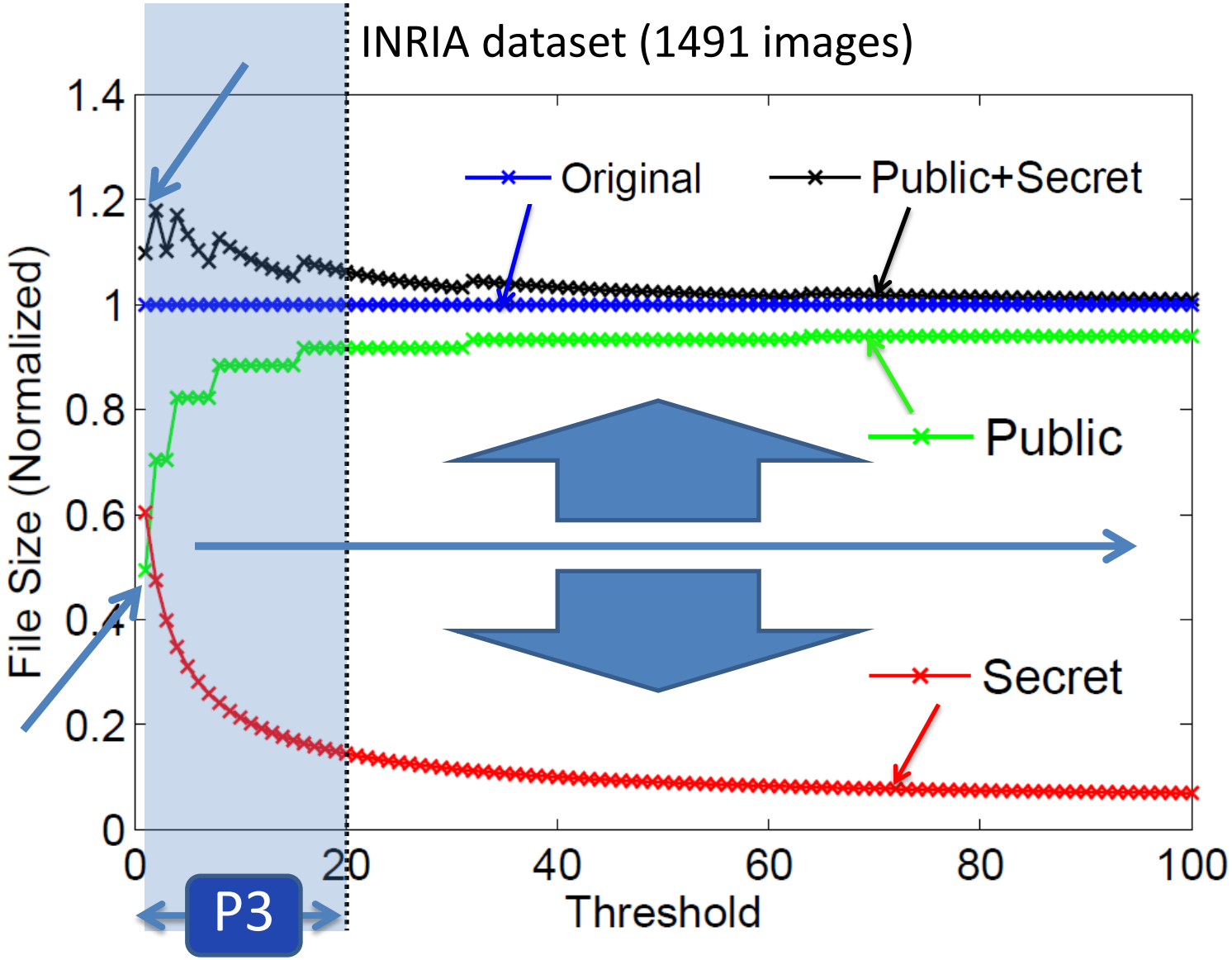
Lam and Goodman, "A Mathematical Analysis of the DCT Coefficient Distributions for Images", ITIP 2000

Sparseness | *Sign* | *Magnitude*

P3 Algorithm: How the encryption works

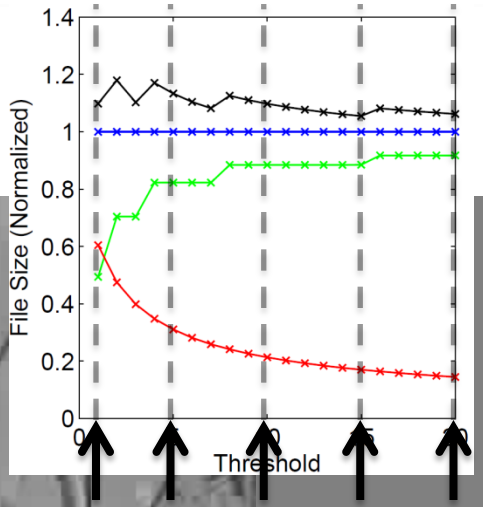


Threshold vs. Storage Trade-off



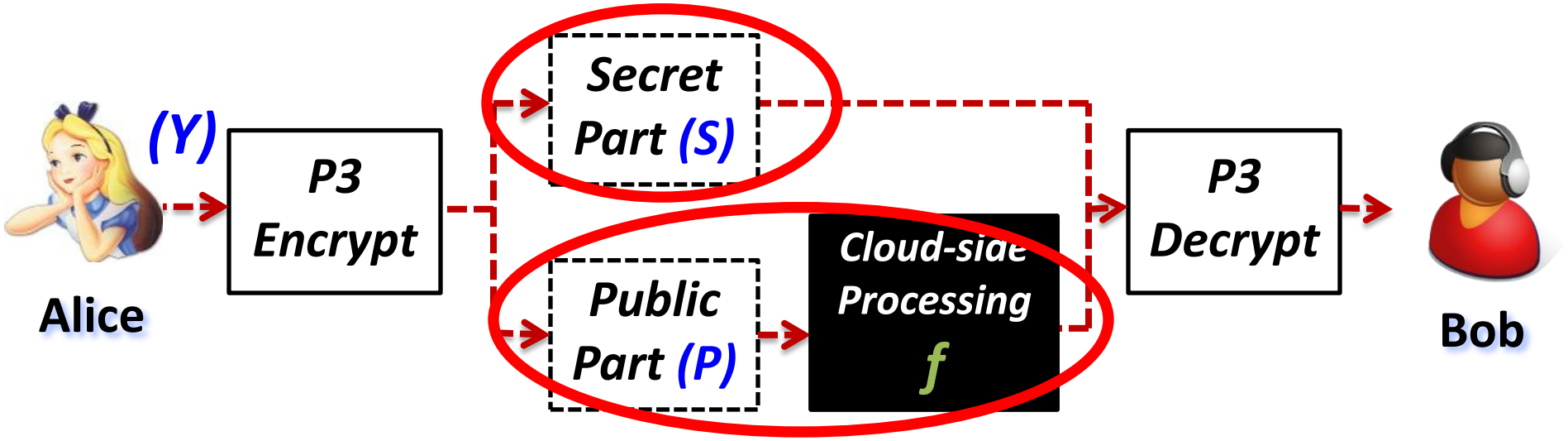
Privacy: What is exposed?

Secret Part (T=20)



Public Part (T=1)

P3 Decryption Challenge

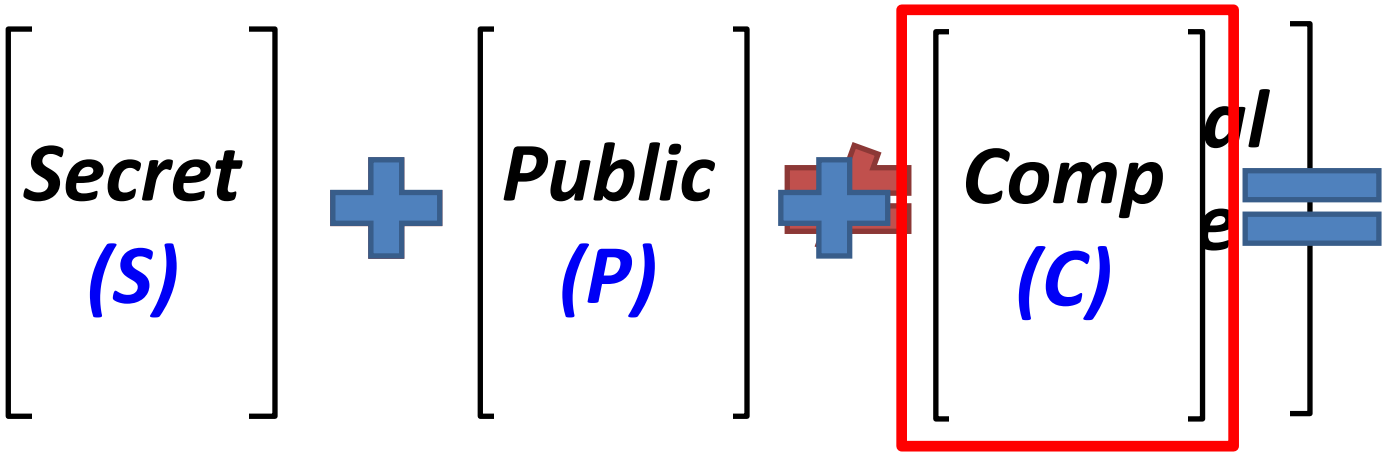


Challenge: Given ***S*** and ***f(P)***, *can we get* ***f(Y)***?

We need to perform careful analysis since P3 encryption hides sign information.

Addressing P3 Decryption Challenge

Challenge: Given ***S*** and ***f(P)*, *can we get f(Y)?***

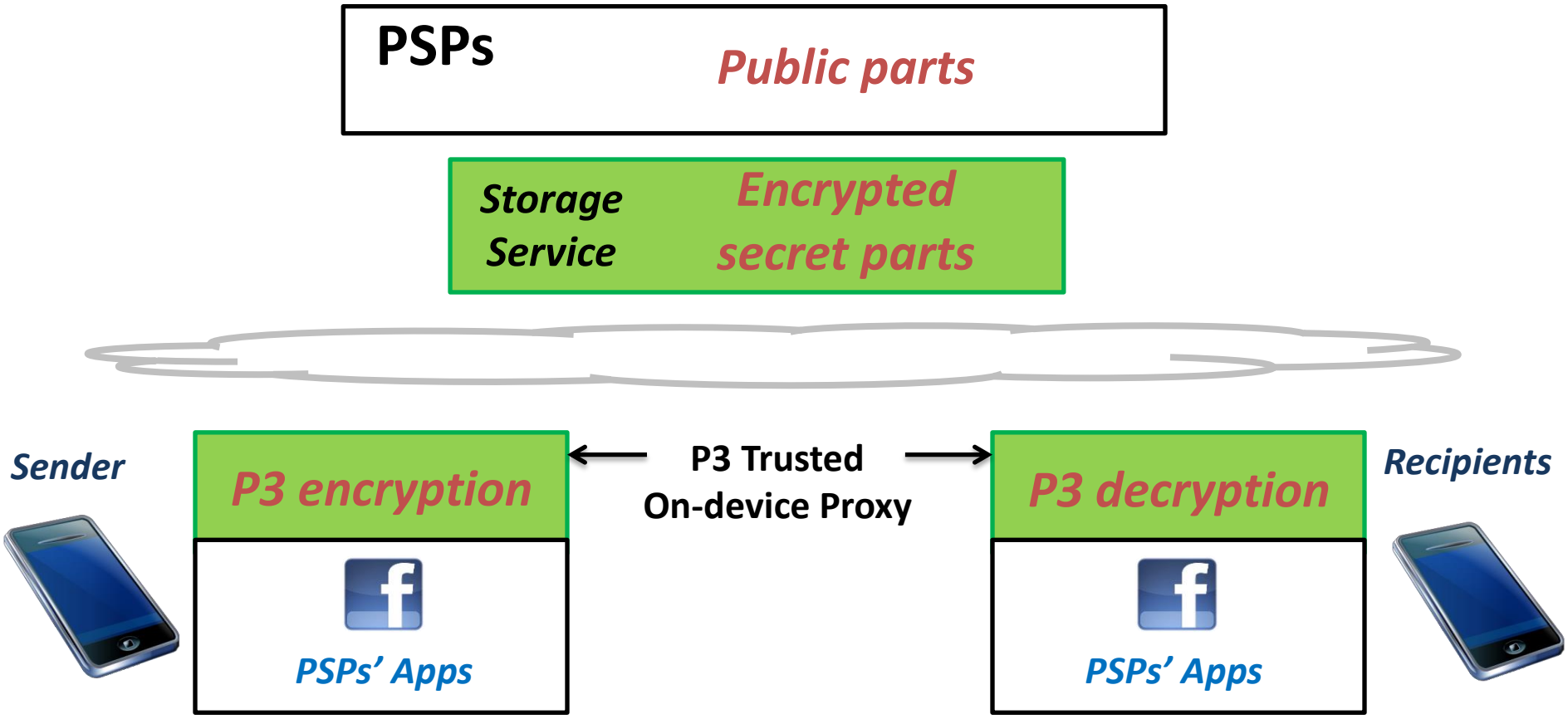


Analysis Result: C can be derived from S

P3 can handle ANY linear processing

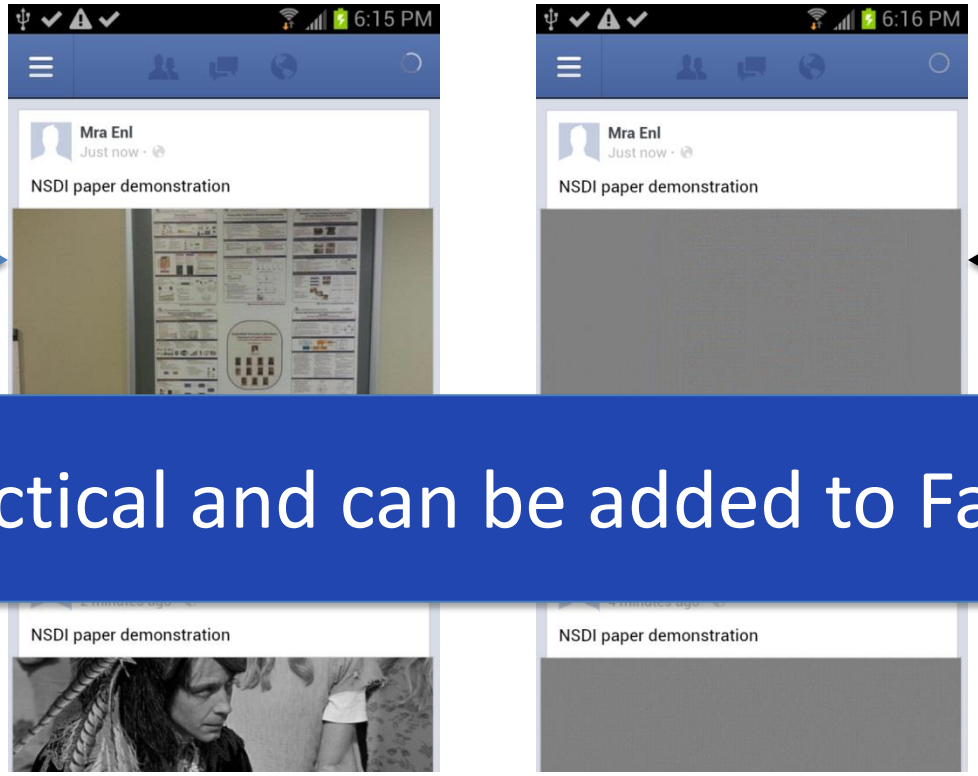
- Scaling
- Cropping
- Sharpening
- Blending
- Smoothing

P3 System Architecture



P3 can be implemented with existing PSPs without causing infrastructure changes

Prototype on Android Phone



P3 is practical and can be added to Facebook

Category	Average	Stdev
P3 Encryption	152.7 ms	20.87
P3 Decryption	191.85 ms	24.83

Evaluating Privacy

- **Objective metric**
  - *PSNR*
- **Computer vision algorithms**
  - *SIFT feature detection*
  - *Edge detection: Canny*
  - *Face detection: Haar*
  - *Face recognition: EigenFace*

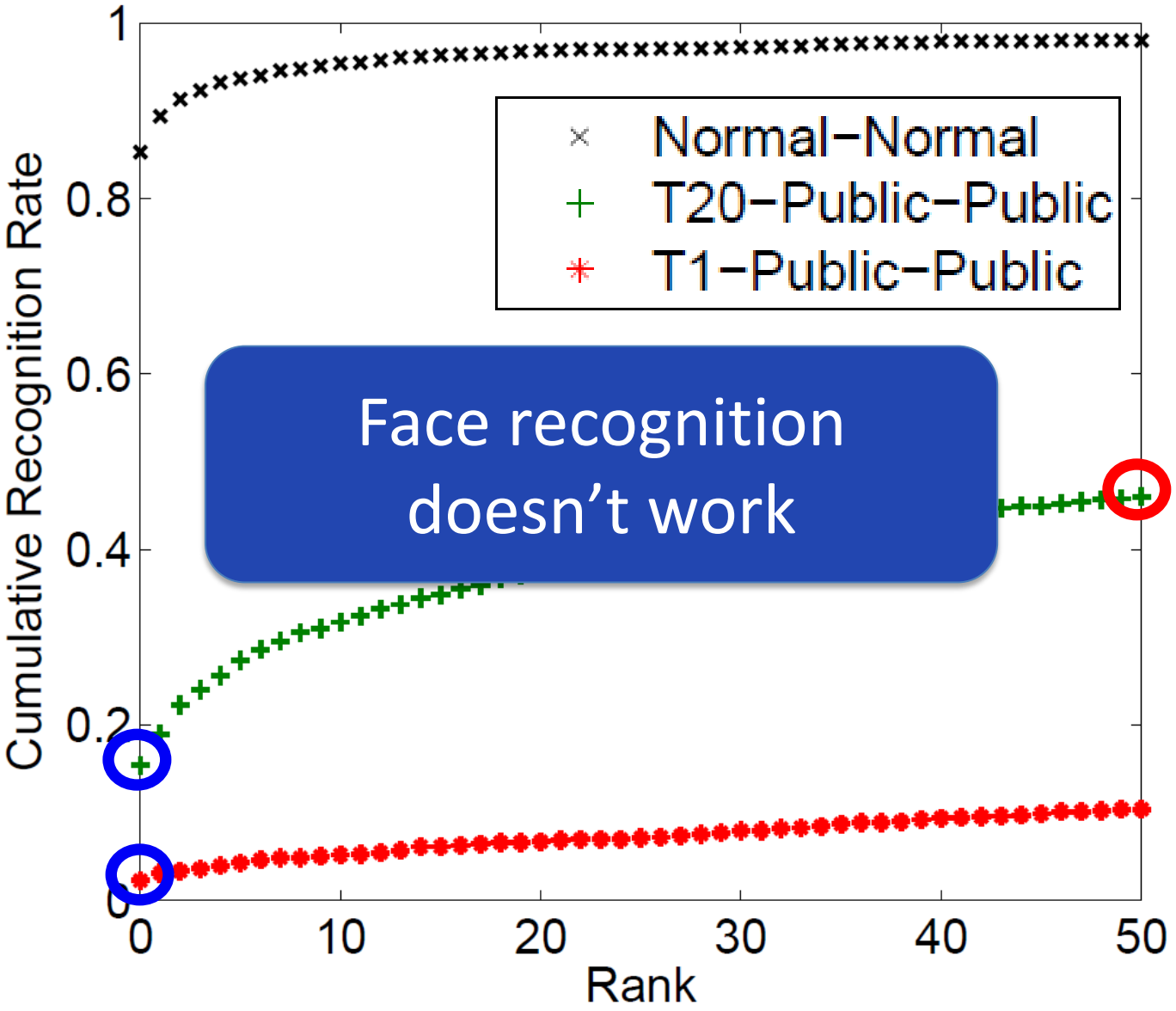
P3 preserves privacy against algorithmic attacks

Results: Face Recognition

- EigenFace [Turk et al. 1991] with the Color FERET database
- CSU's face recognition evaluation system

- **4 probing (testing) sets**
- **2 distance metrics (Euclidean, MahCosine)**
- **Different P3 thresholds from 1 to 100**
- **Public parts as a training set**

P3 Successfully Breaks Face Recognition



Summary and Contributions

Our algorithm and system, collectively called P3, provides privacy-preserving photo sharing

- Propose a novel photo encryption/decryption algorithm.
- Transparent system design that can work with existing PSPs.
- A complete prototype and extensive privacy evaluation using computer vision-based recognition algorithms.