Privacy Preservation in Shared Images

Christopher Tran

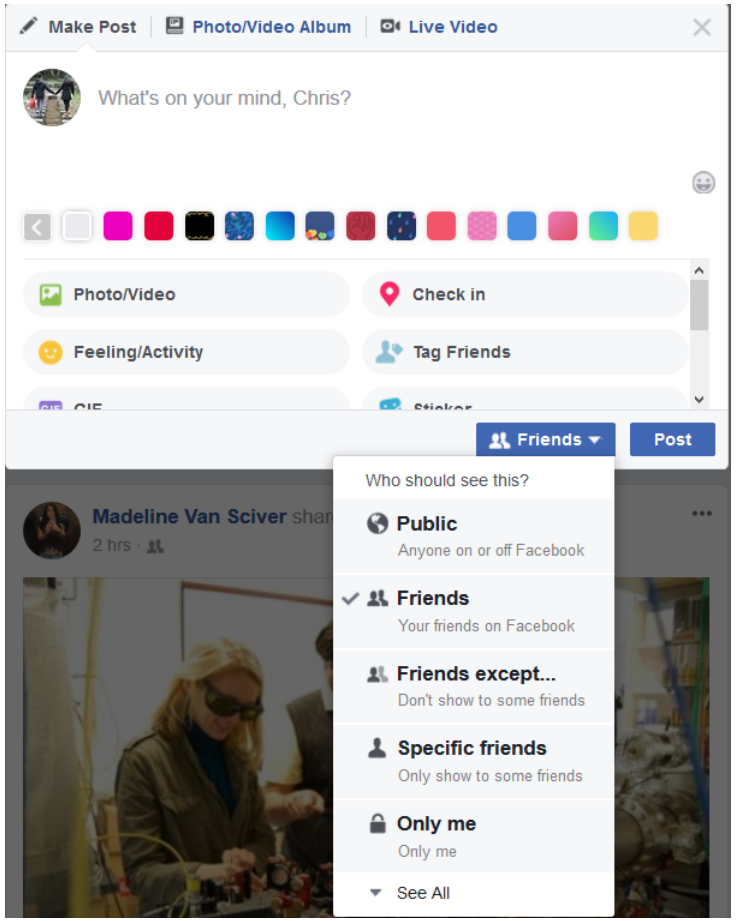
Introduction

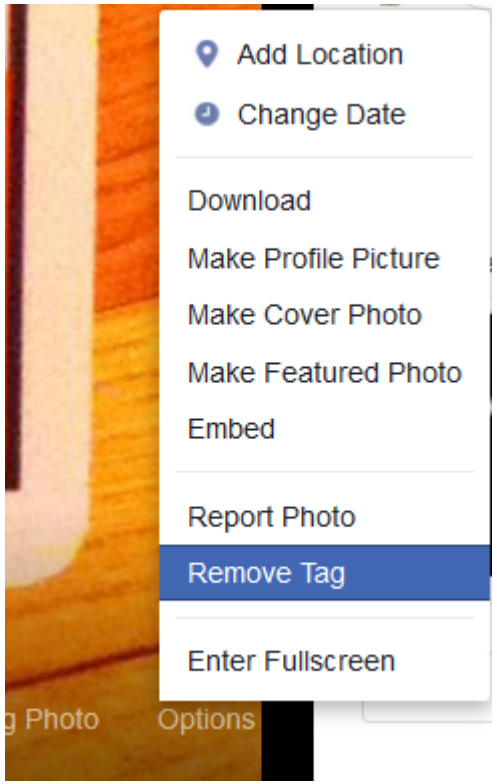
Introduction

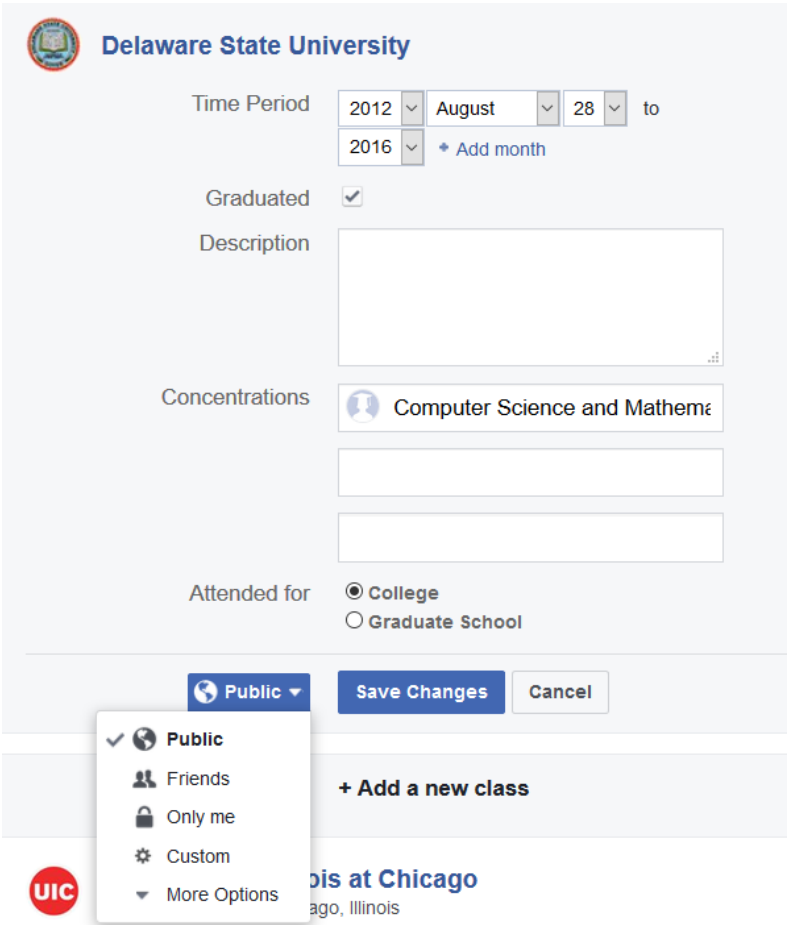
Privacy Settings and Tools

Who can see my stuff?	Who can see your future posts?	**Friends**	Edit
	Limit the audience for posts you've shared with friends of friends or Public?		Limit Past Posts
	Who can see your friends list?	**Public**	Edit
Who can contact me?	Who can send you friend requests?	**Friends of friends**	Edit
Who can look me up?	Who can look you up using the email address you provided?	**Friends**	Edit
	Who can look you up using the phone number you provided?	**Friends**	Edit
	Do you want search engines outside of Facebook to link to your profile?	**No**	Edit

Introduction







Privacy Concerns

Barnes First Monday 2006, Ahern et al. CHI 2007

Privacy Concerns

- “Privacy Paradox”

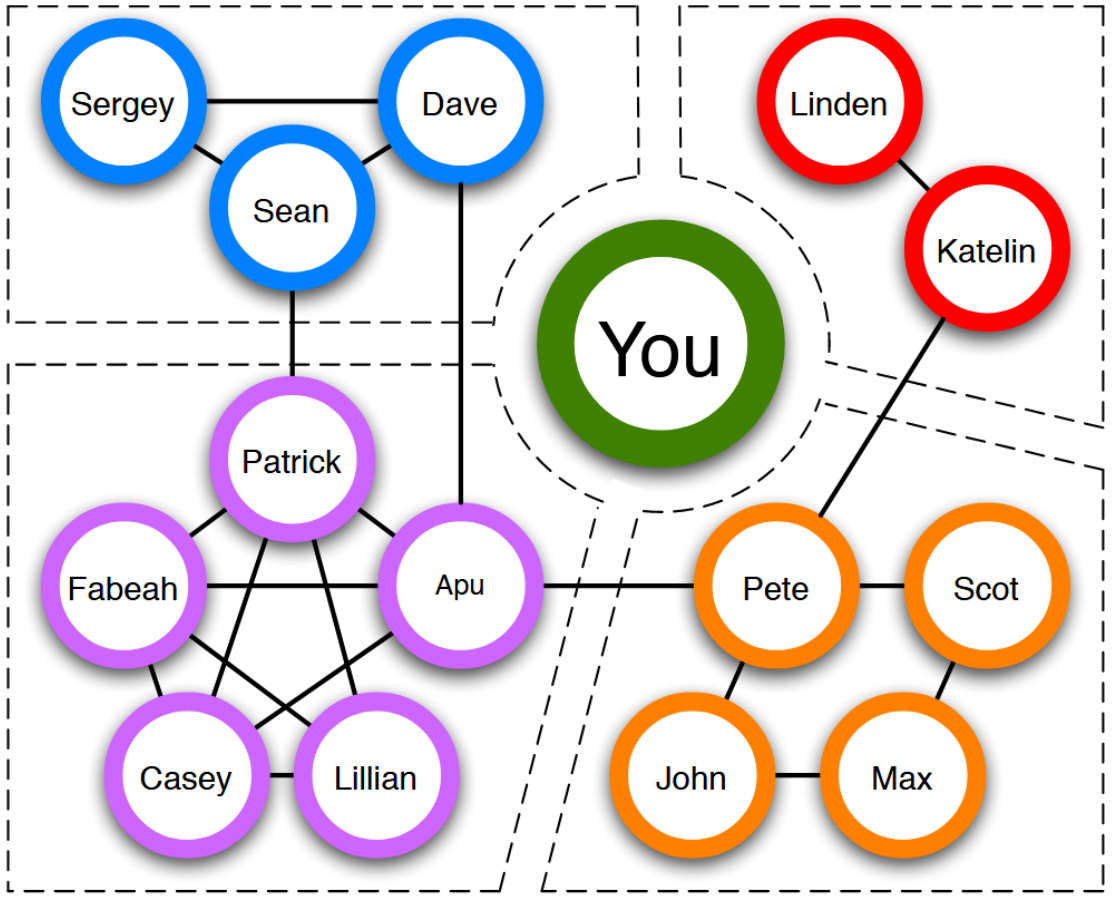
Barnes First Monday 2006, Ahern et al. CHI 2007

Privacy Concerns

- “Privacy Paradox”
- Automating privacy

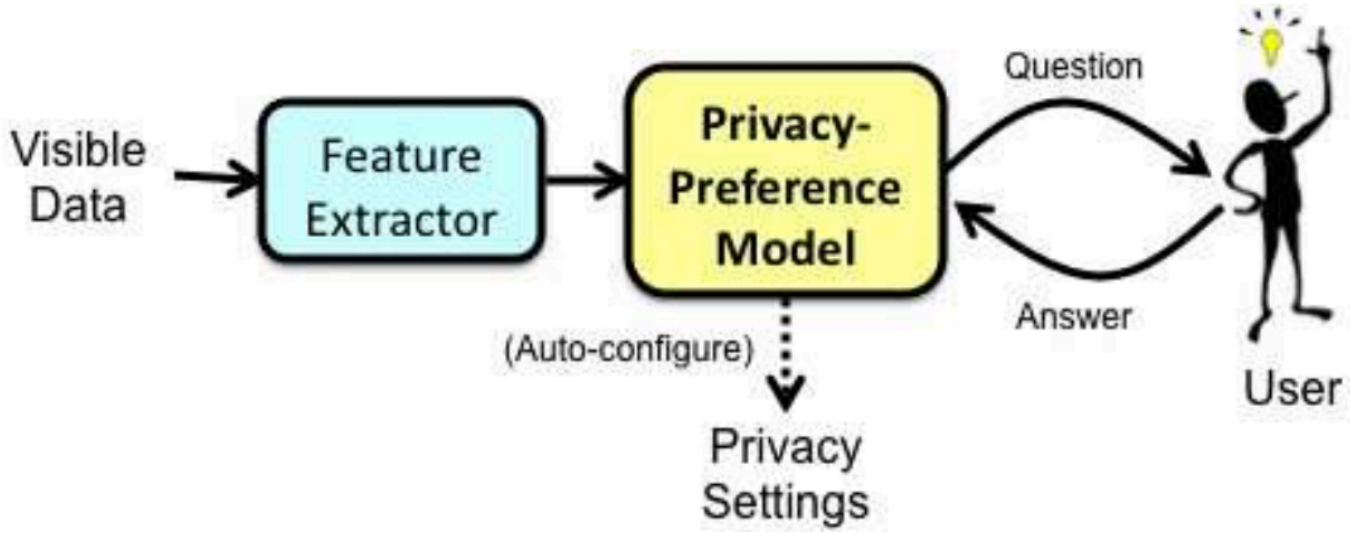
Barnes First Monday 2006, Ahern et al. CHI 2007

Social Circles



Adu-Oppong et al. SOUPS 2008

Privacy Wizard



Fang and LeFevre, WWW 2010

Privacy Concerns

- “Privacy Paradox”
- Automating privacy
- Photos
  - Tags
  - Consequences

Barnes First Monday 2006, Ahern et al. CHI 2007

Privacy in Images

- Using tags for access control
- Image encryption
- Predicting privacy settings

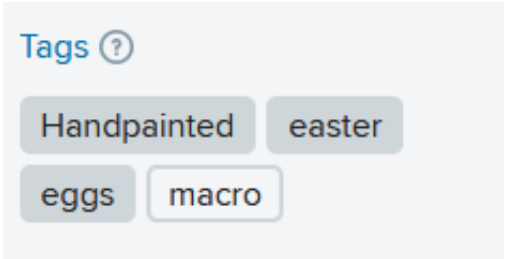
Tags for Access Control

P. F. Klemperer, Y. Liang, M. L. Mazurek, M. Sleeper, B. Ur, L. Bauer, L. F. Cranor, N. Gupta, M. K. Reiter

Conference on Human Factors in Computing Systems (CHI), 2012

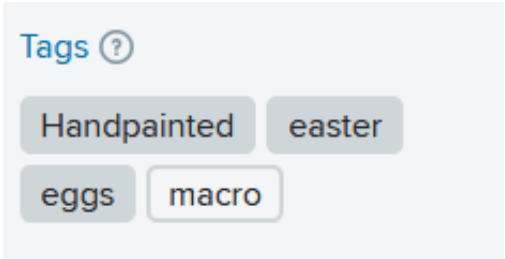
Tags for Photos

- Tags used for organization, search, communication, and description



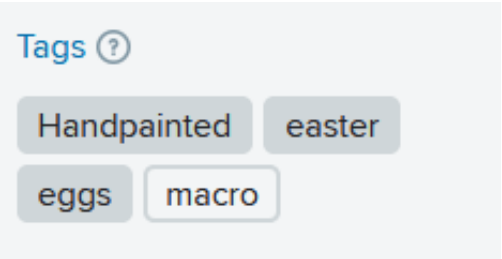
Tags for Photos

- Tags used for organization, search, communication, and description
- Can tags be used for access-control policies?



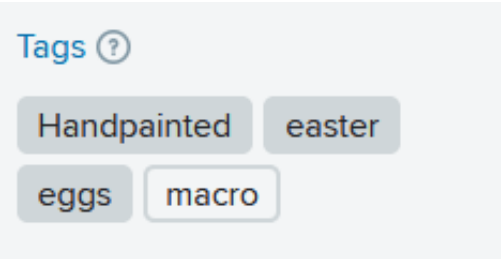
Tags for Photos

- Tags used for organization, search, communication, and description
- Can tags be used for access-control policies?
- Does tagging with access control in mind improve the performance of tag-based access control?



Tags for Photos

- Tags used for organization, search, communication, and description
- Can tags be used for access-control policies?
- Does tagging with access control in mind improve the performance of tag-based access control?
- How do users engage with the concept of access-control?



User Study

- 18 Participants
  - Tag or add captions “often” or “always”

User Study

- 18 Participants
  - Tag or add captions “often” or “always”
- Three tasks
  - T1: Organizational Tagging
  - T2: Tagging for access control
  - T3: Refinement of Tags

Organizational Tags

- Participants were asked to tag their uploaded photos

Organizational Tags

- Participants were asked to tag their uploaded photos
- Friend-photo preferences
  - Strong allow
  - Weak allow
  - Neural
  - Weak deny
  - Strong deny

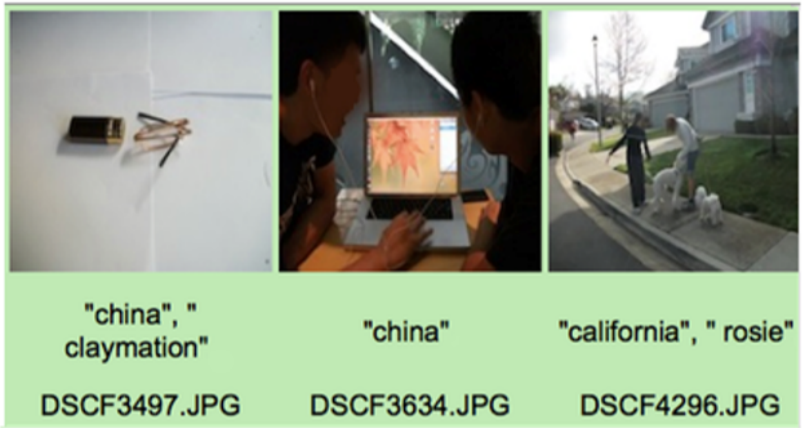
Rule Generation

- Preferences were mapped to binary labels
  - Allow
  - Deny
- Rules were generated using decision tree for each friend
- Generated rules were shown to each participant

Tagging for access control

Rules
1. If not tagged with allen then ALLOW ACCESS
2. If not tagged with rosie then ALLOW ACCESS
3. If tagged with rosie AND allen then DENY ACCESS
4. Otherwise ALLOW ACCESS

Stan Can See...

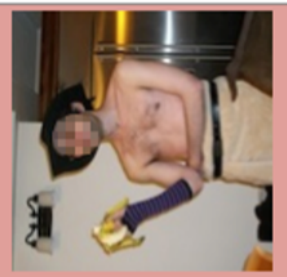


"china", " claymation" DSCF3497.JPG

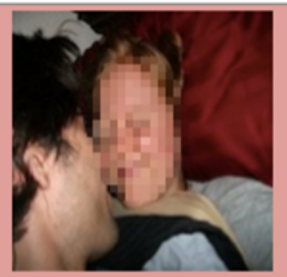
"china" DSCF3634.JPG

"california", " rosie" DSCF4296.JPG

Stan Can't See...



"california", " rosie", " allen" DSCF4287.JPG



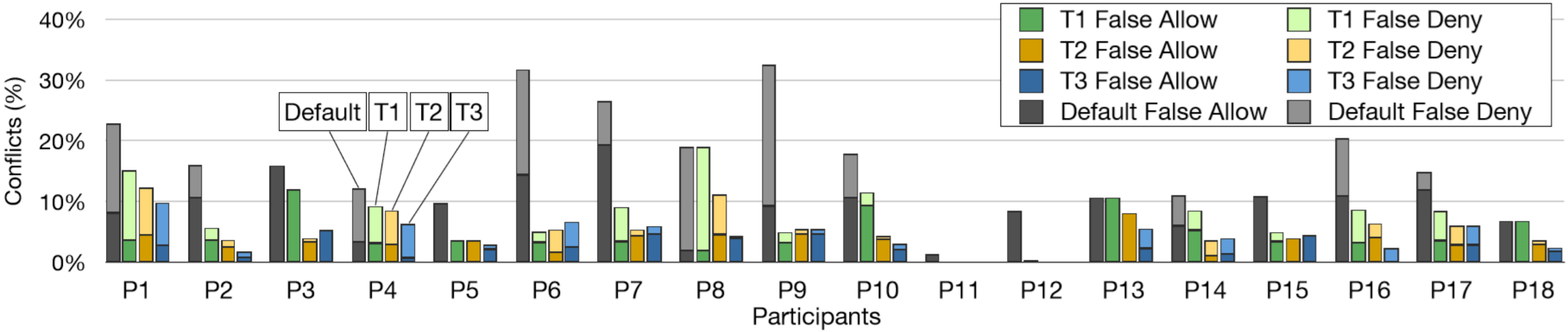
"california", " rosie", " allen" DSCF4293.JPG

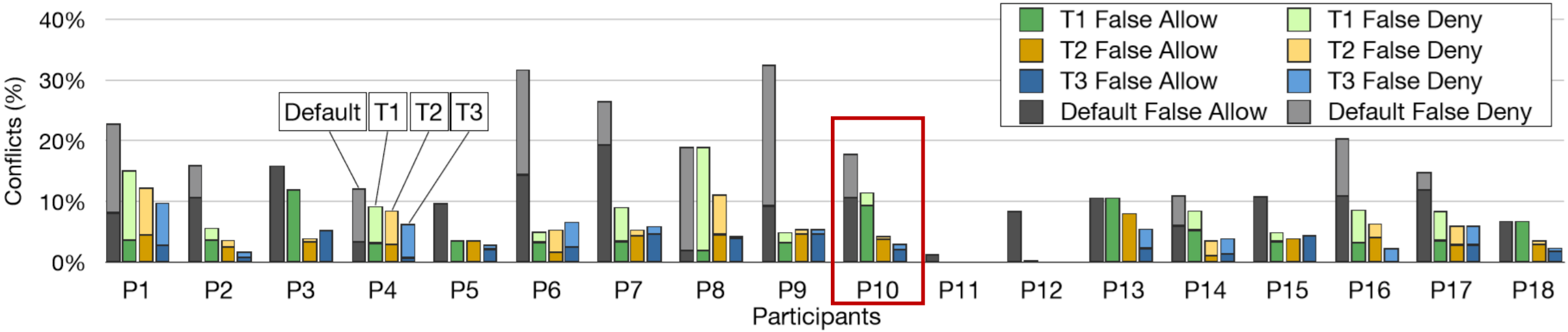
Tagging for Access Control

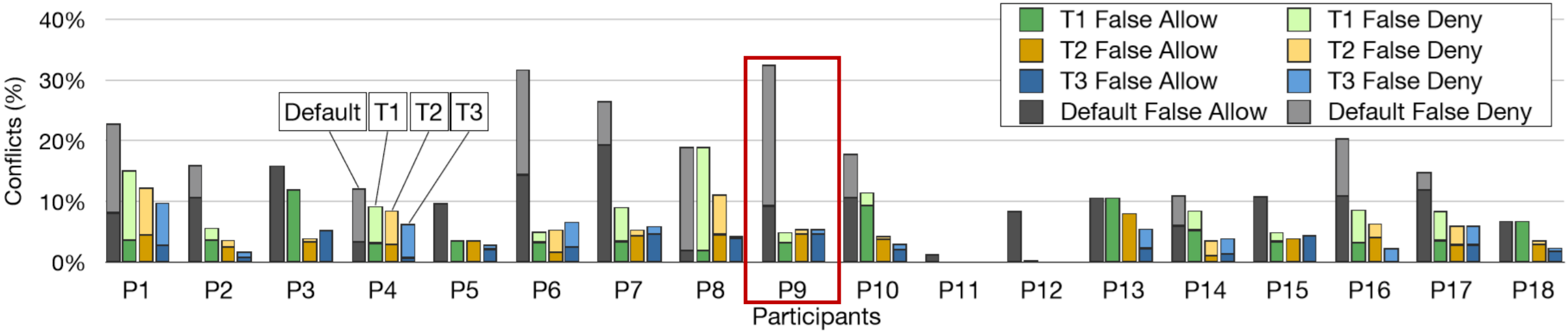
- In T2, participants were invited to add to and/or delete tags made in T1
- Goal of creating tag-based access-control rules
- New rules created from T2 and reviewed with participant
- In T3, participants were invited to modify tags in T2

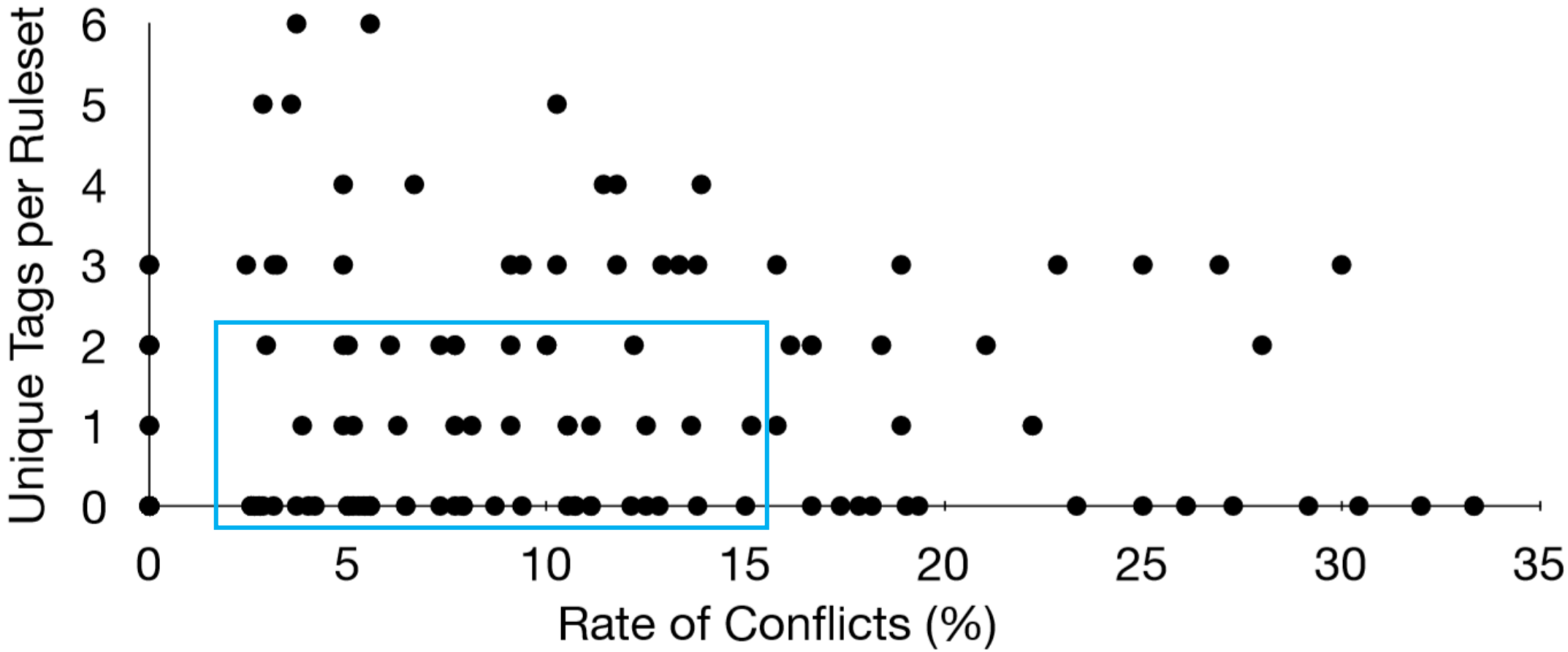
Results

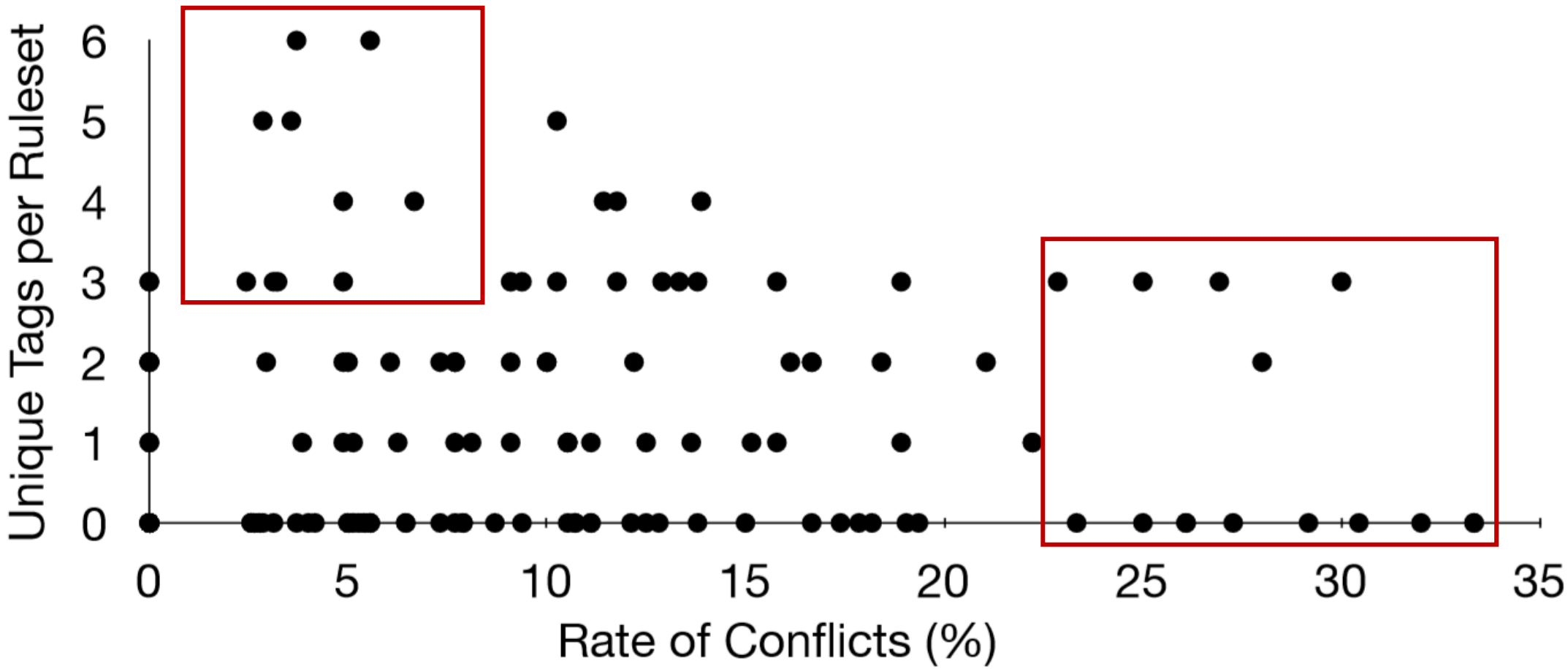
- Conflict rate
- Rule complexity
- Reactions


40%
30%
20%
10%
0%
Conflicts (%)
Default
T1
T2
T3
T1 False Allow
T1 False Deny
T2 False Allow
T2 False Deny
T3 False Allow
T3 False Deny
Default False Allow
Default False Deny
P1
P2
P3
P4
P5
P6
P7
P8
P9
P10
P11
P12
P13
P14
P15
P16
P17
P18
Participants


40%
30%
20%
10%
0%
Conflicts (%)
Default
T1
T2
T3
T1 False Allow
T2 False Allow
T3 False Allow
Default False Allow
T1 False Deny
T2 False Deny
T3 False Deny
Default False Deny
P1
P2
P3
P4
P5
P6
P7
P8
P9
P10
P11
P12
P13
P14
P15
P16
P17
P18
Participants


40%
30%
20%
10%
0%
Conflicts (%)
Default
T1
T2
T3
T1 False Allow
T2 False Allow
T3 False Allow
Default False Allow
T1 False Deny
T2 False Deny
T3 False Deny
Default False Deny
P1
P2
P3
P4
P5
P6
P7
P8
P9
P10
P11
P12
P13
P14
P15
P16
P17
P18
Participants


Unique Tags per Ruleset
0
1
2
3
4
5
6
0
5
10
15
20
25
30
35
Rate of Conflicts (%)


Unique Tags per Ruleset
0
1
2
3
4
5
6
0
5
10
15
20
25
30
35
Rate of Conflicts (%)

Reactions to Sample Rules

- Many participants liked the rules
  - P05 – the rules “conceptualized what [she] was thinking”
  - P17 – rules created matched “the intuitive rule that [he] made”

Reactions to Sample Rules

- Many participants liked the rules
  - P05 – the rules “conceptualized what [she] was thinking”
  - P17 – rules created matched “the intuitive rule that [he] made”
- Not always successful
  - P09 – Denying photos tagged “gf” to a roommate was too general
  - P14 – rules “seem[ed] roughly accurate” but was upset a teacher could see one embarrassing picture

Reactions to Tag-Based Access Control

- Do tag-based access control rules make sense?
  - 13 said the concept made complete or some sense
  - 2 said were neutral
  - 1 said the concept did not make sense
  - 2 said depends on circumstance

Critique

- Pros
  - Organizational tags work reasonably well
  - User reactions and behaviors for tagging for access control

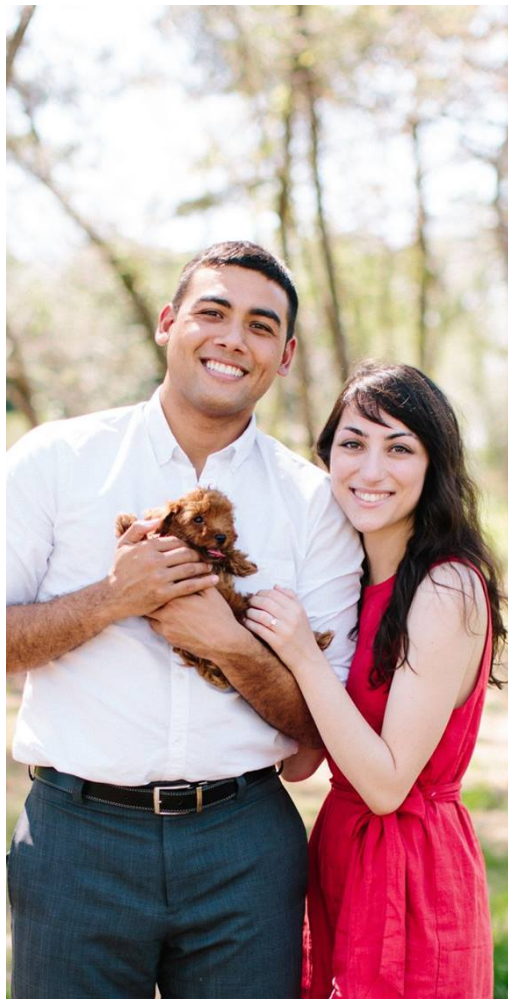
Critique

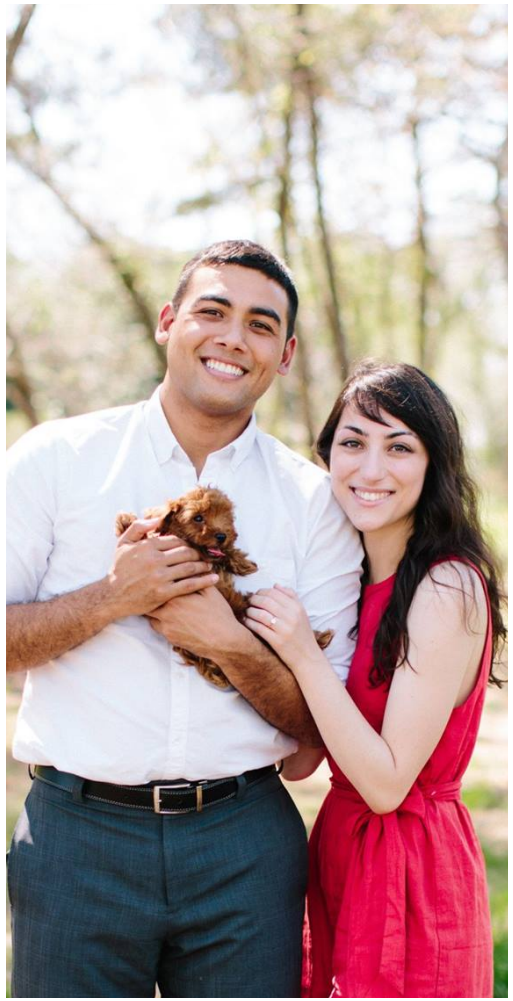
- Pros
  - Organizational tags work reasonably well
  - User reactions and behaviors for tagging for access control
- Cons
  - User burden
  - Generalization
  - Scalability

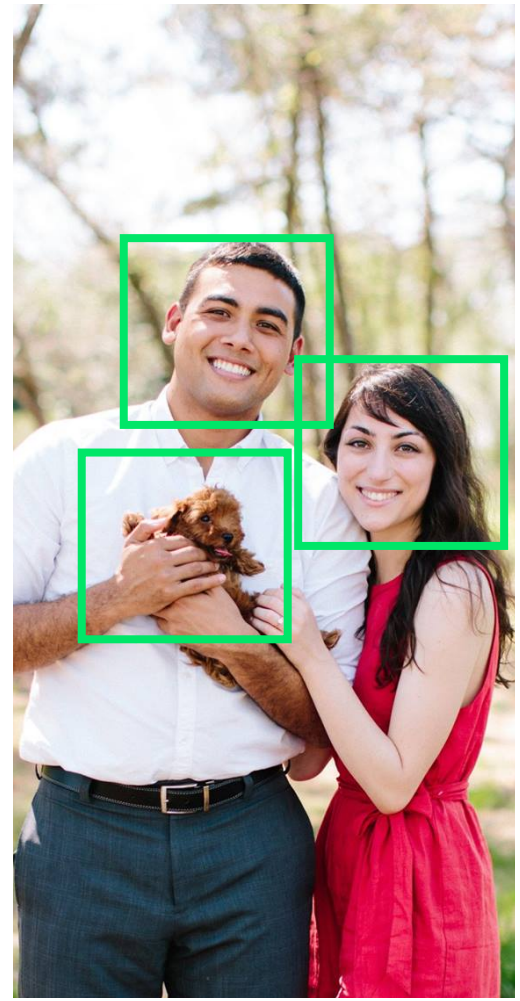
Privacy Preserving Image Transforms

J. He, B. Liu, D. Kong, X. Bao, N. Wang, H. Jin, G. Kesidis

IEEE/IFIP International Conference on Dependable Systems and Networks, 2016

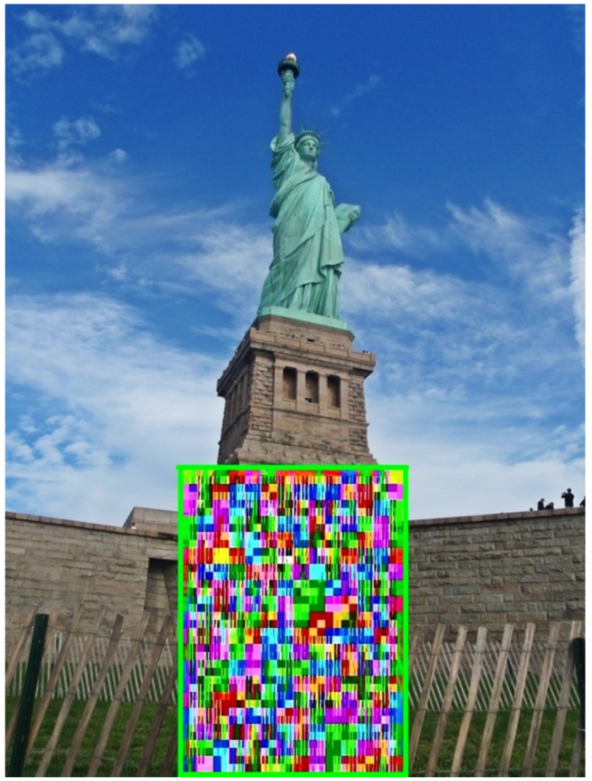






Challenges for Image Encryption on PSPs

- Maximal Usability
- Transformation Supported
- Personalized Privacy Flexibility



RGB to JPEG

RGB to JPEG

1) RGB to YUV representation

RGB to JPEG

1) RGB to YUV representation
2) DCT Transformation
   - YUV is divided into 8x8 pixel blocks where DCT transform is applied
   - 8x8 DCT coefficient matrix (First entry is DC, rest are AC)

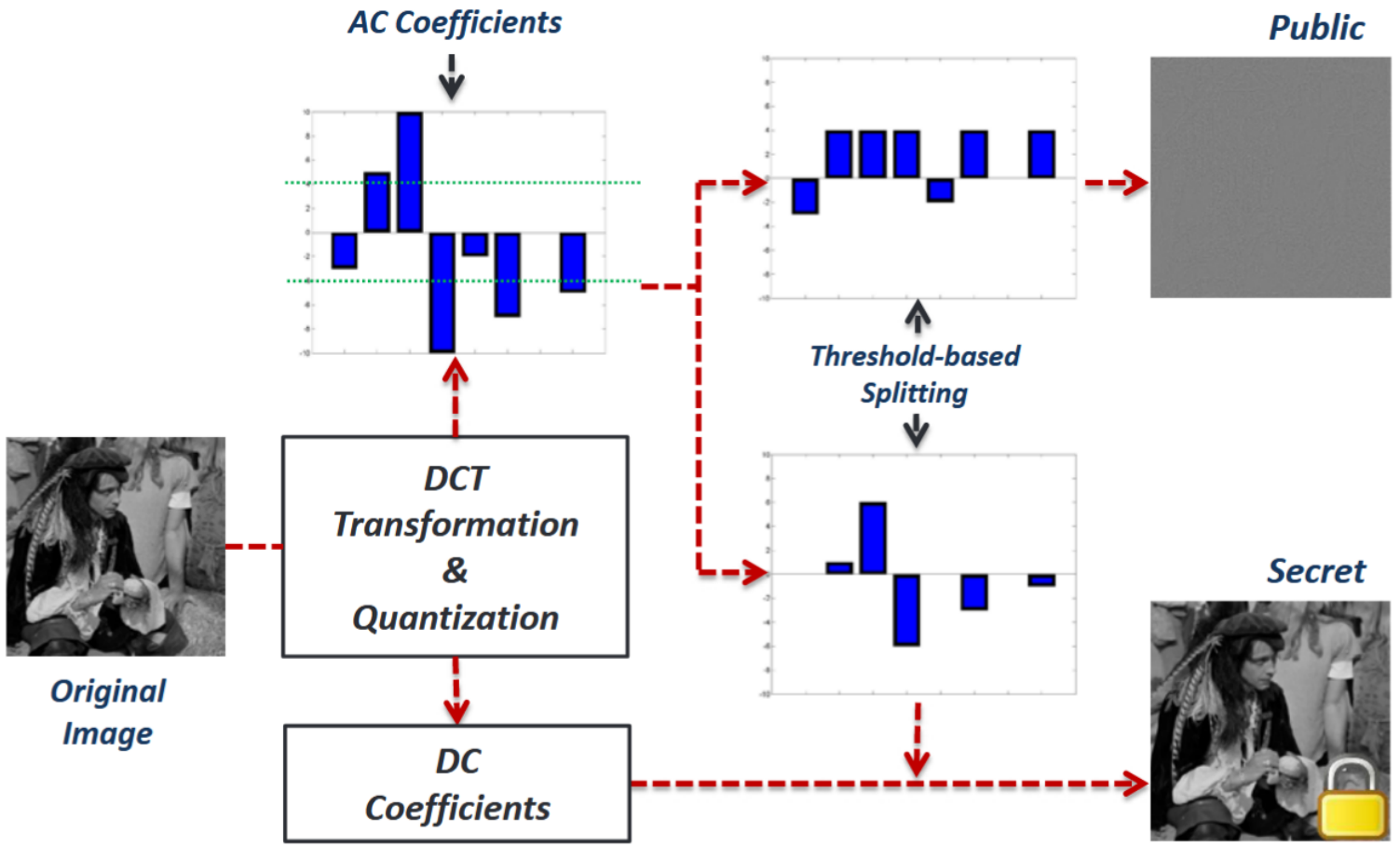
RGB to JPEG

1) RGB to YUV representation
2) DCT Transformation
   - YUV is divided into 8x8 pixel blocks where DCT transform is applied
   - 8x8 DCT coefficient matrix (First entry is DC, rest are AC)
3) Quantization
4) Entropy Coding

RGB to JPEG

1) RGB to YUV representation
2) DCT Transformation
   - YUV is divided into 8x8 pixel blocks where DCT transform is applied
   - 8x8 DCT coefficient matrix (First entry is DC, rest are AC)
3) Quantization
4) Entropy Coding

P3 for Photo Privacy



Ra et al. NSDI 2013

Limitations of P3

Limitations of P3

- Image level encryption

Limitations of P3

- Image level encryption
- No direct support for image transformations on PSPs

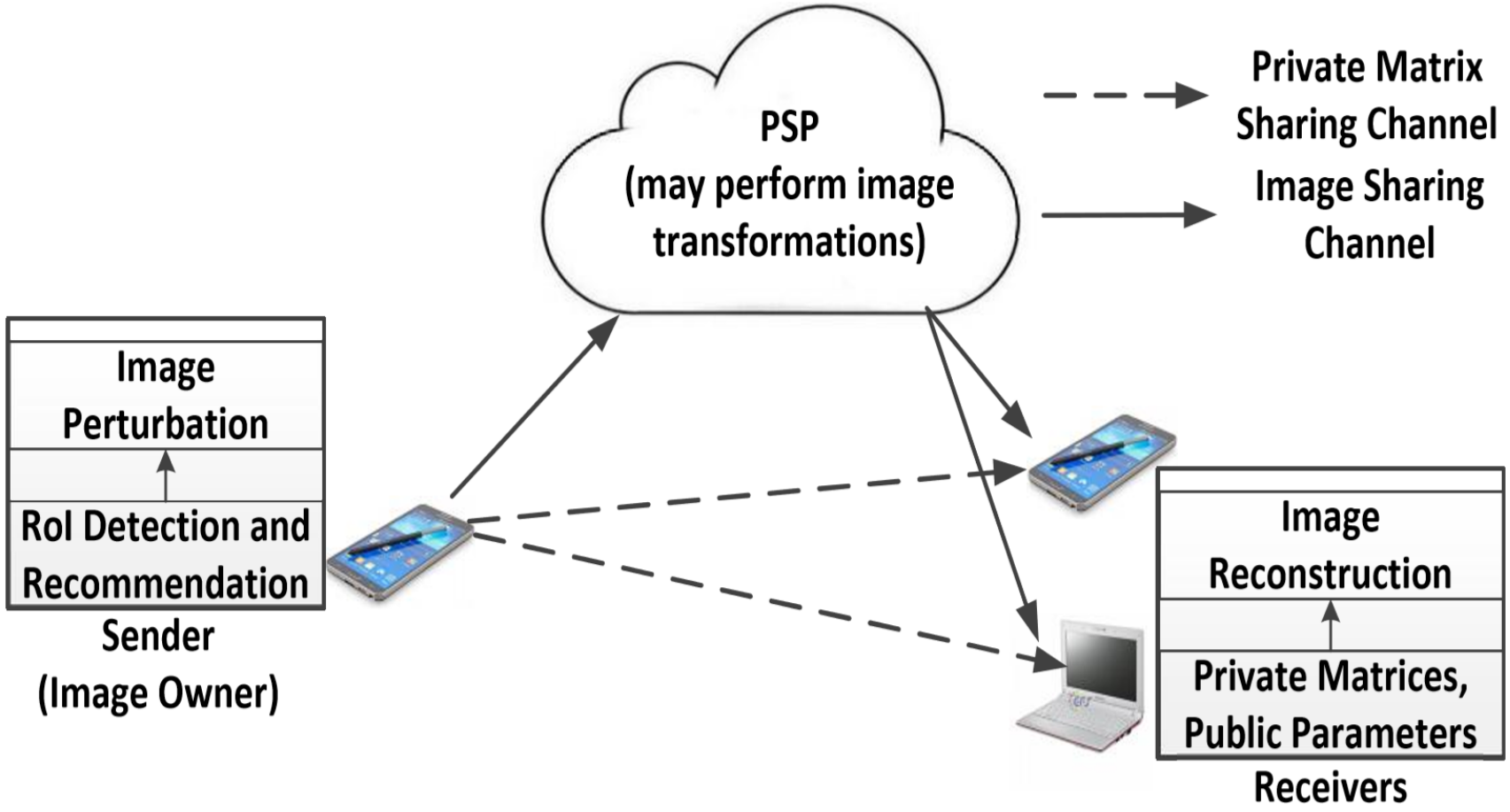
Limitations of P3

- Image level encryption
- No direct support for image transformations on PSPs
- Many fine details are lost in image recovery

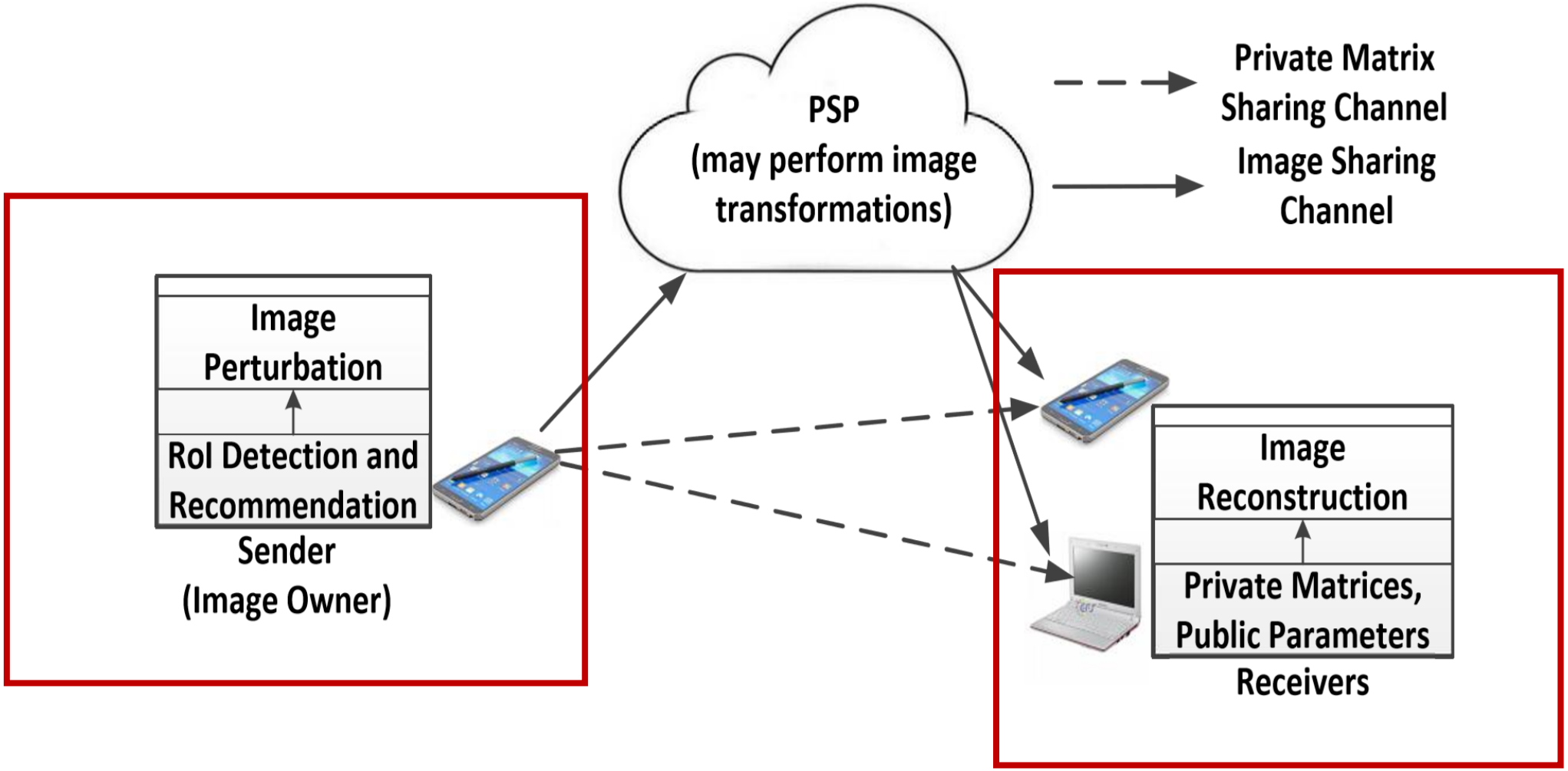
Privacy Preserving Partial Image Sharing (PuPPIeS)

- Addresses the challenges of photo sharing on PSPs
- Recovers better image quality compared to P3

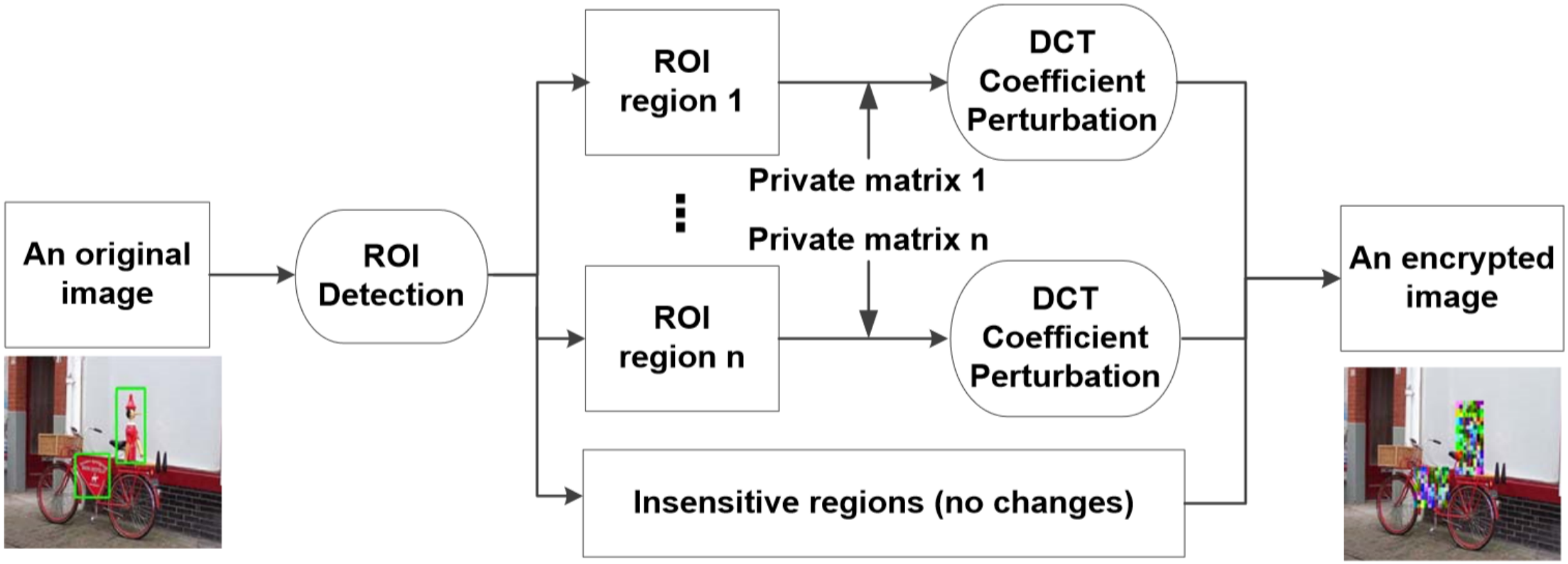
PuPPIeS


PSP
(may perform image transformations)
Private Matrix Sharing Channel
Image Sharing Channel
Image Perturbation
RoI Detection and Recommendation
Sender
(Image Owner)
Image Reconstruction
Private Matrices, Public Parameters
Receivers

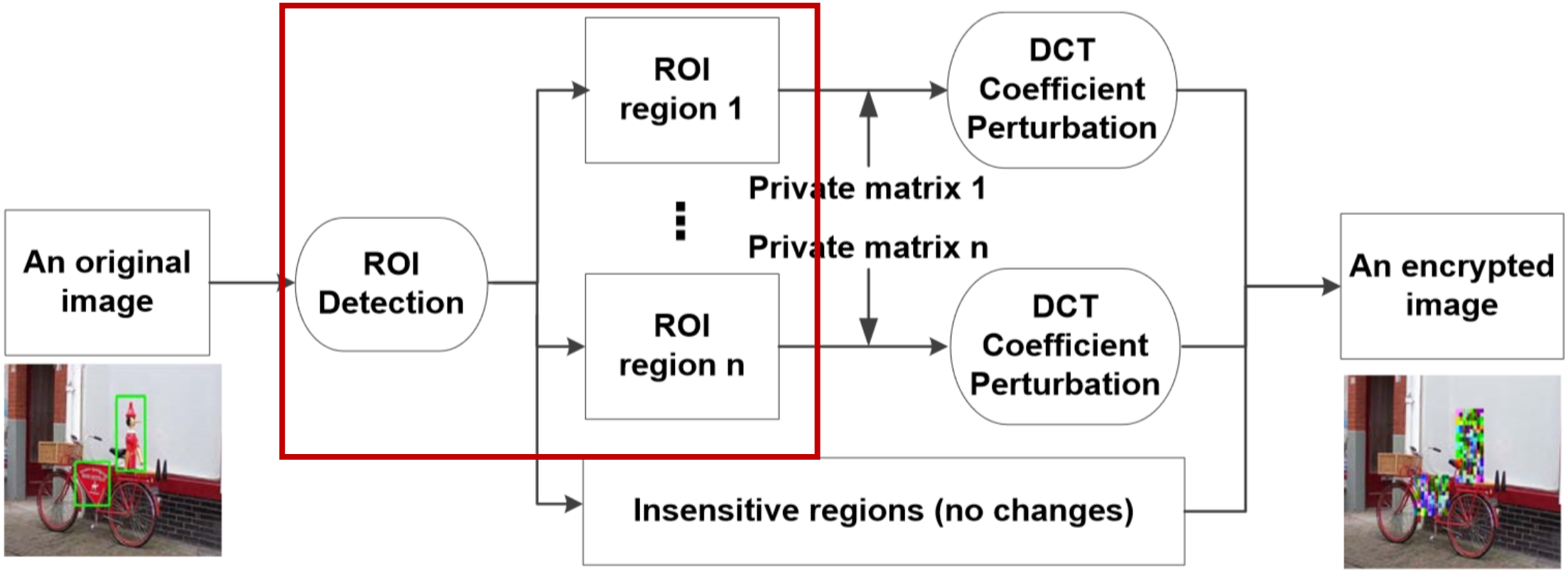
PuPPIeS


PSP
(may perform image transformations)
Private Matrix Sharing Channel
Image Sharing Channel
Image Perturbation
RoI Detection and Recommendation
Sender
(Image Owner)
Image Reconstruction
Private Matrices, Public Parameters
Receivers

Sender

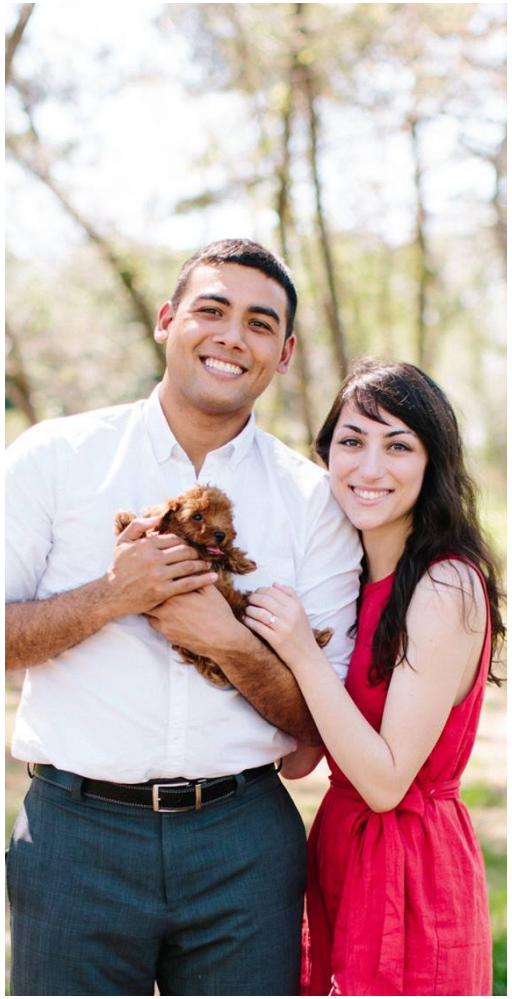

An original image
ROI Detection
ROI region 1
ROI region n
Private matrix 1
Private matrix n
DCT Coefficient Perturbation
DCT Coefficient Perturbation
Insensitive regions (no changes)
An encrypted image

Sender

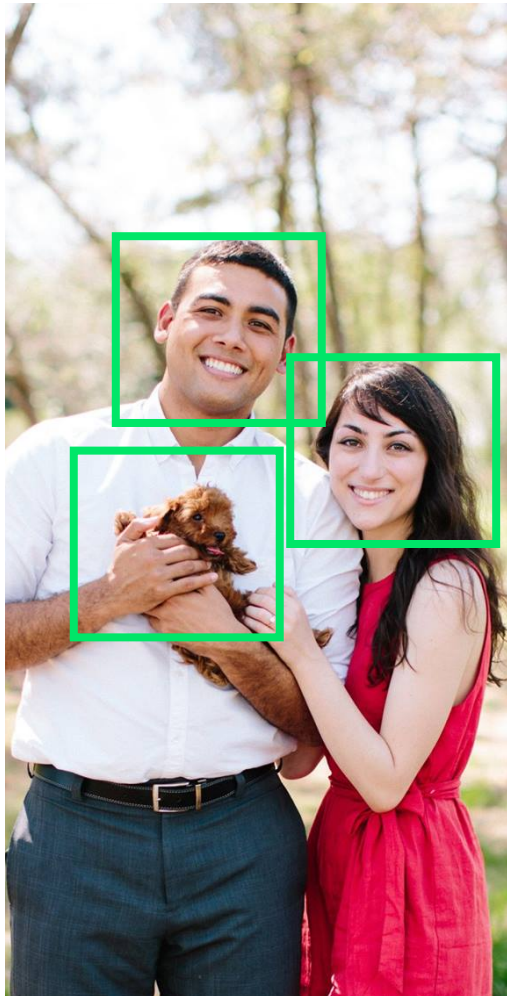

An original image
ROI Detection
ROI region 1
ROI region n
Private matrix 1
Private matrix n
DCT Coefficient Perturbation
DCT Coefficient Perturbation
Insensitive regions (no changes)
An encrypted image

Sender

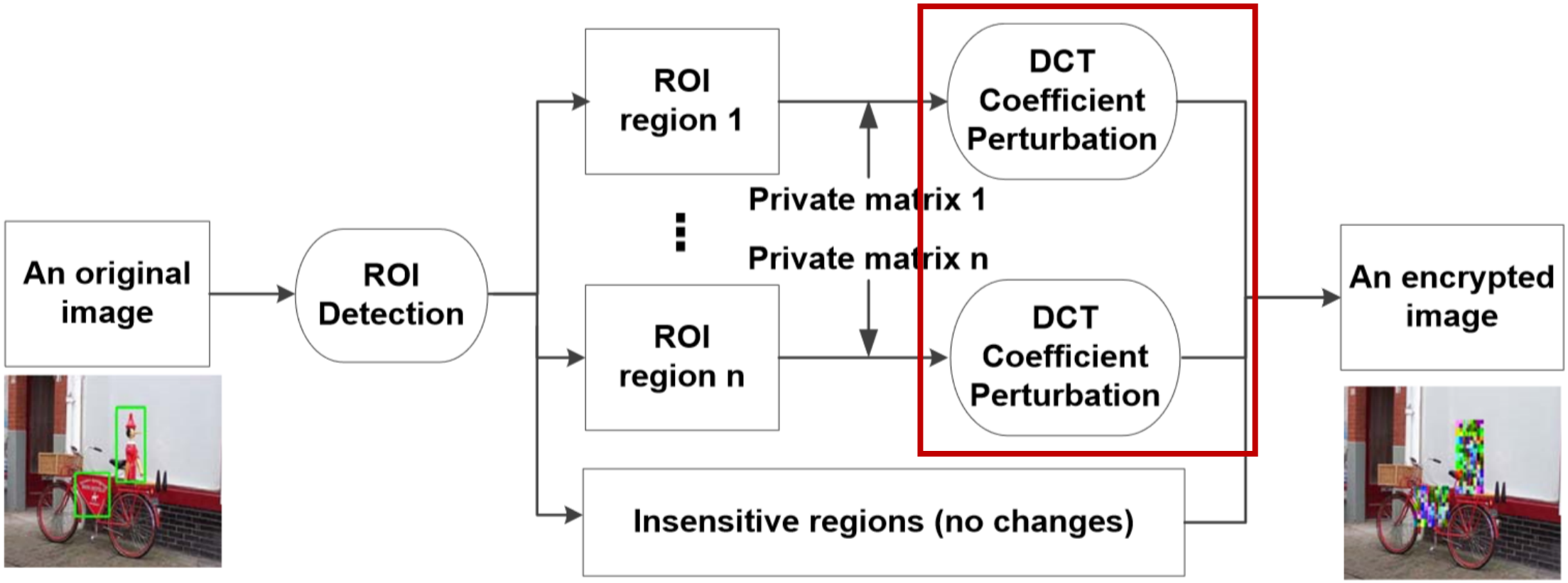
Sender



Sender



Sender


An original image
ROI Detection
ROI region 1
ROI region n
Private matrix 1
Private matrix n
DCT Coefficient Perturbation
DCT Coefficient Perturbation
Insensitive regions (no changes)
An encrypted image

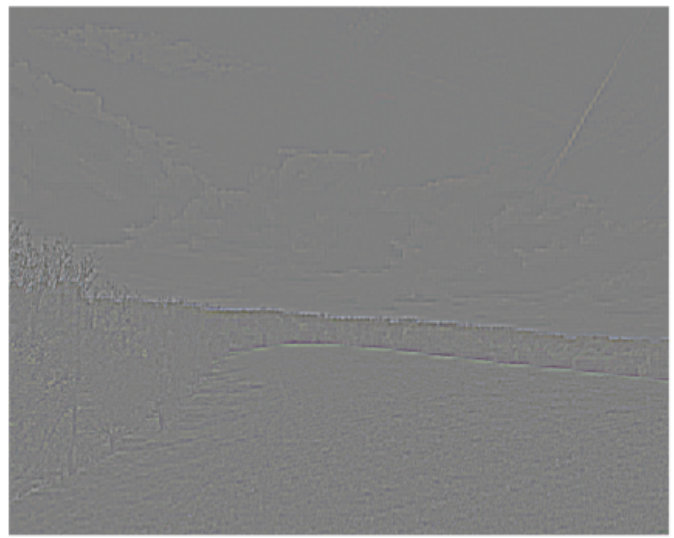
PuPPIeS-*N*

- Given:
  - R – the region to be perturbed, divided into 8x8 blocks
  - B^k – one DCT coefficient matrix in region R, $\left(-1024 \leq b_i^k \leq 1023\right)$
  - P' – a private matrix, $(-1024 \leq p_i \leq 1023)$
  - E^k – the encrypted DCT coefficient vector

$$e_i^k = b_i^k + p_i'$$

(a) Original image.

(b) Preserve DC component only.



(c) Preserve AC component only.

PuPPIeS-*Base*

For DC components: $e_0^k = b_0^k + p'_\ell,\ \ell = (k \mod 64)$

For AC components: $e_i^k = b_i^k + p'_i,\ \text{for } 1 \leq i \leq 63$

PuPPIeS-*Compressed*

- Huffman coding tables become less optimized
- Privacy range vector Q' introducted
  - Controls the range of each entry in P'
- In practice, Q is used to perturb the AC components

For DC components:

$$e_0^k = b_0^k + p'_\ell, \ \ell = (k \bmod 64)$$

For AC components:

$$e_i^k = b_i^k + \left(p'_i \bmod q'_i\right), \text{ for } 1 \leq i \leq 63$$

PuPPIeS-*Zero*

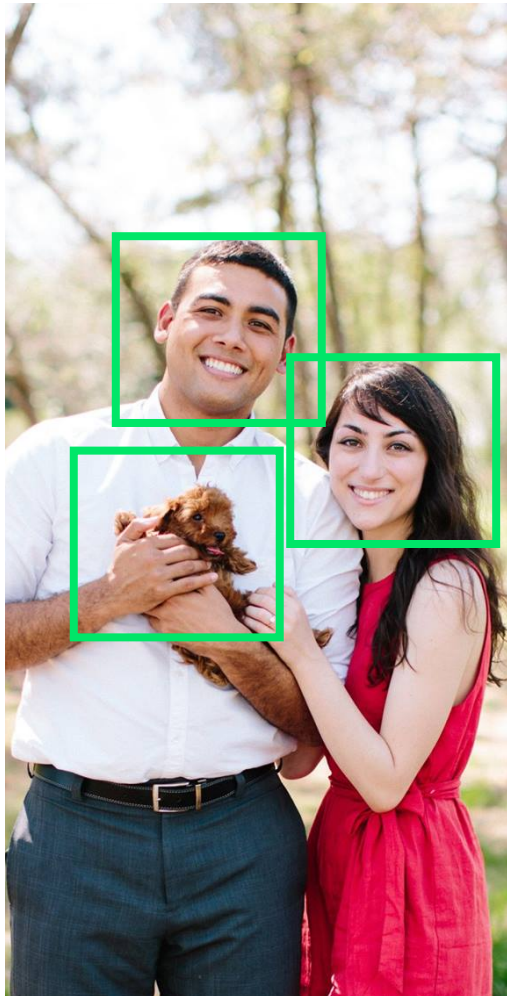
- Skip perturbing zeros in AC coefficients
- Perturbations may cause AC coefficients to become zero
- Introduce new variable stored with public image, $ZInd$

PuPPIeS-*Zero*

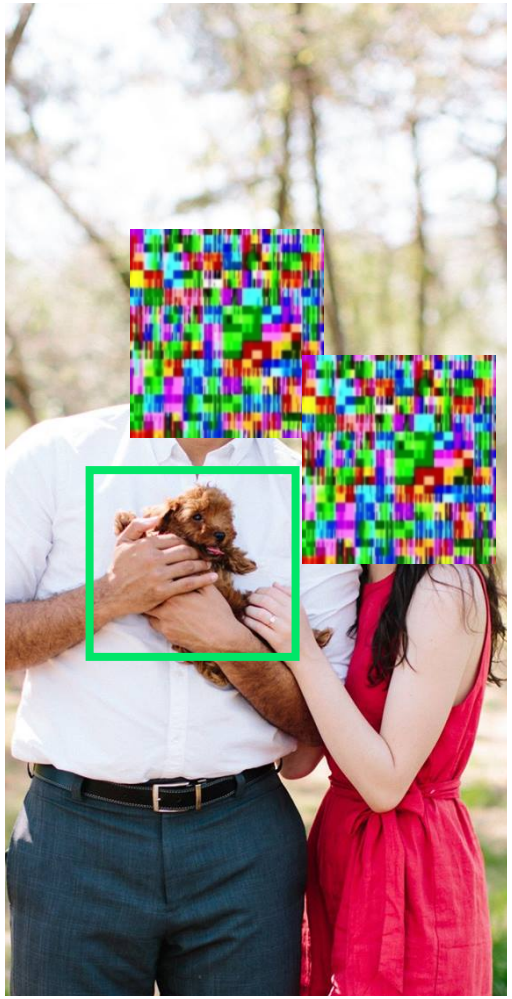
- Skip perturbing zeros in AC coefficients
- Perturbations may cause AC coefficients to become zero
- Introduce new variable stored with public image, $ZInd$

scheme	mean	median	std	min	max
PuPPIeS-$Base$	10.45	9.69	3.88	5.01	85.8
PuPPIeS-$Compression$	1.46	1.41	0.230	1.15	6.26
PuPPIeS-$Zero$	1.23	1.22	0.064	1.10	1.80

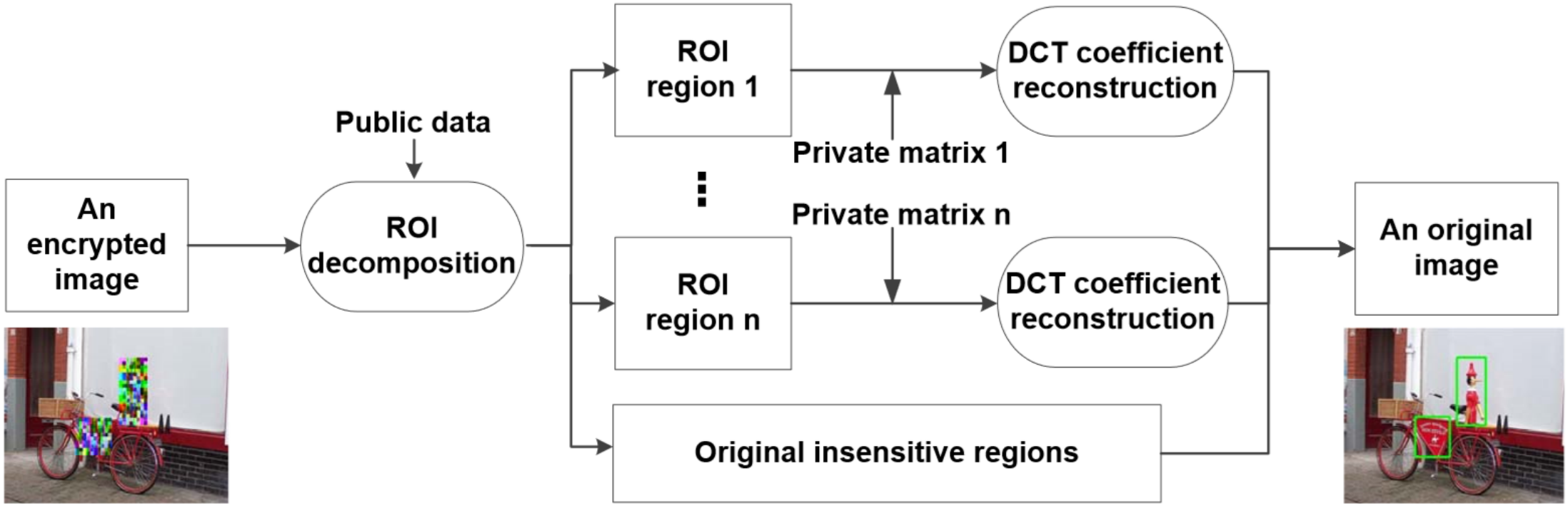
Sender



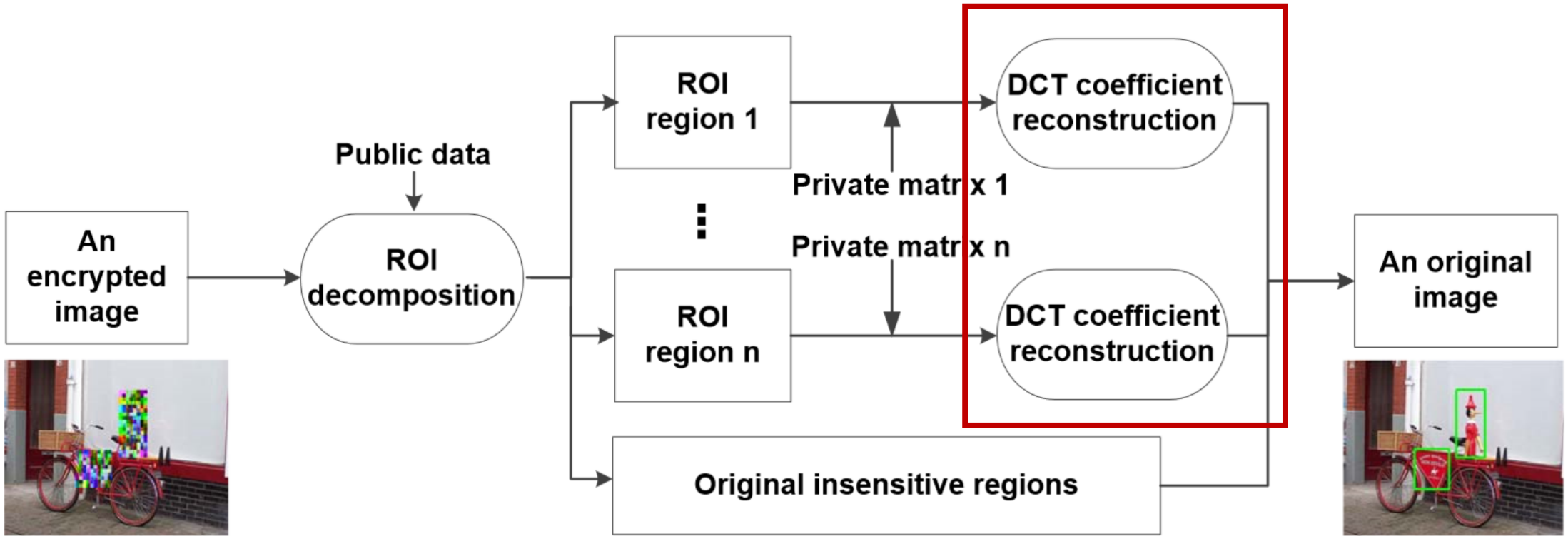
Sender



Receiver – Scenario 1



Receiver – Scenario 1

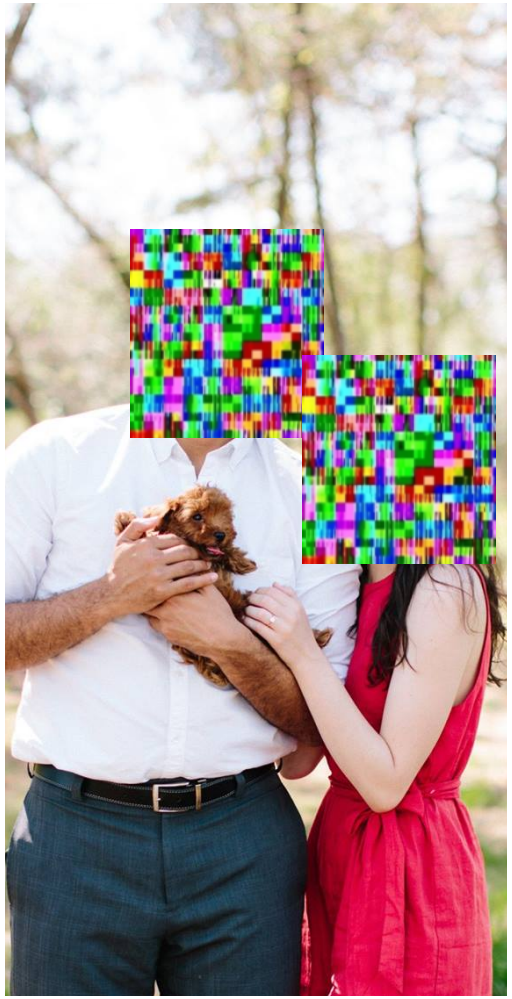


DCT Reconstruction

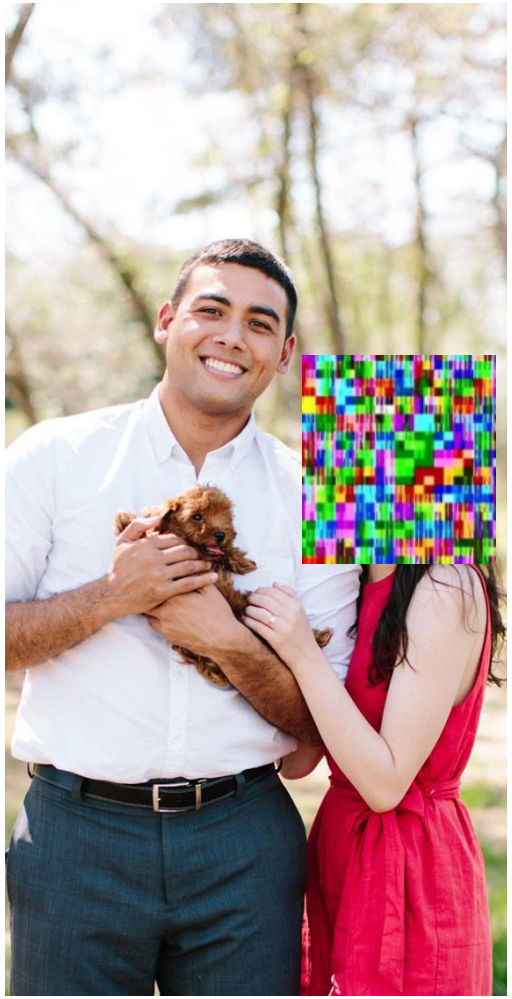
- Given a perturbed block E, privacy vector P', the reconstructed DCT coefficient vector B, is defined as:

$$\bar{b}_i = \Big((e_i - \bar{p}_i + 1024) \mod 2048 \Big) - 1024$$

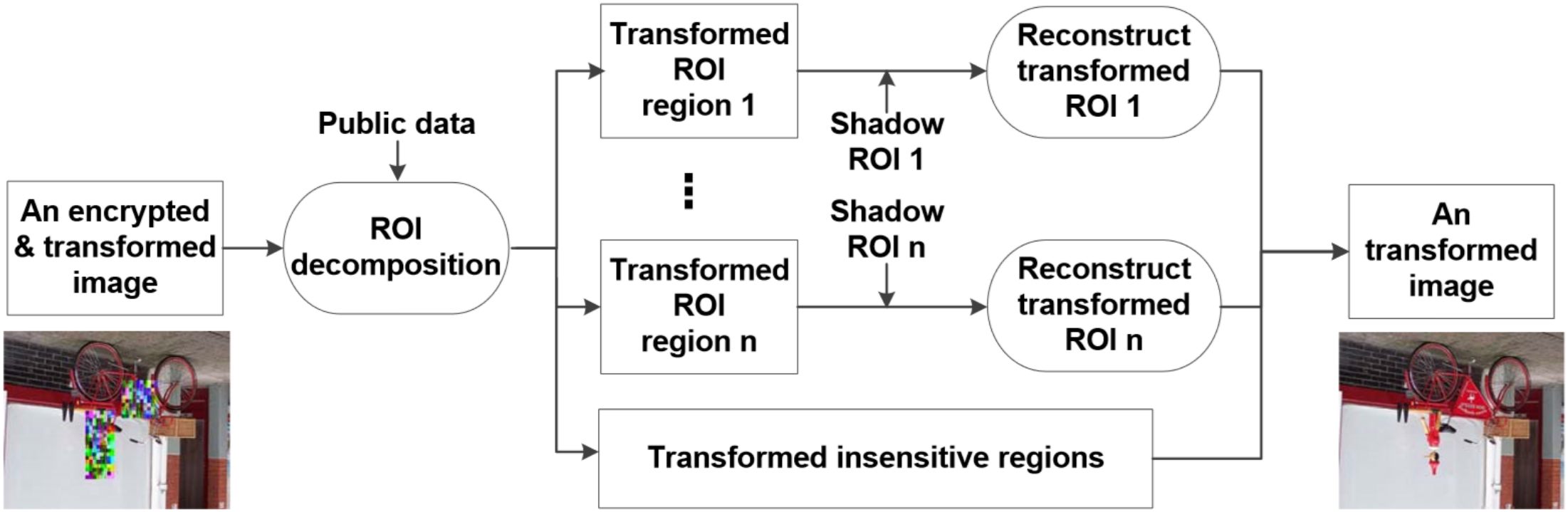
DCT Reconstruction



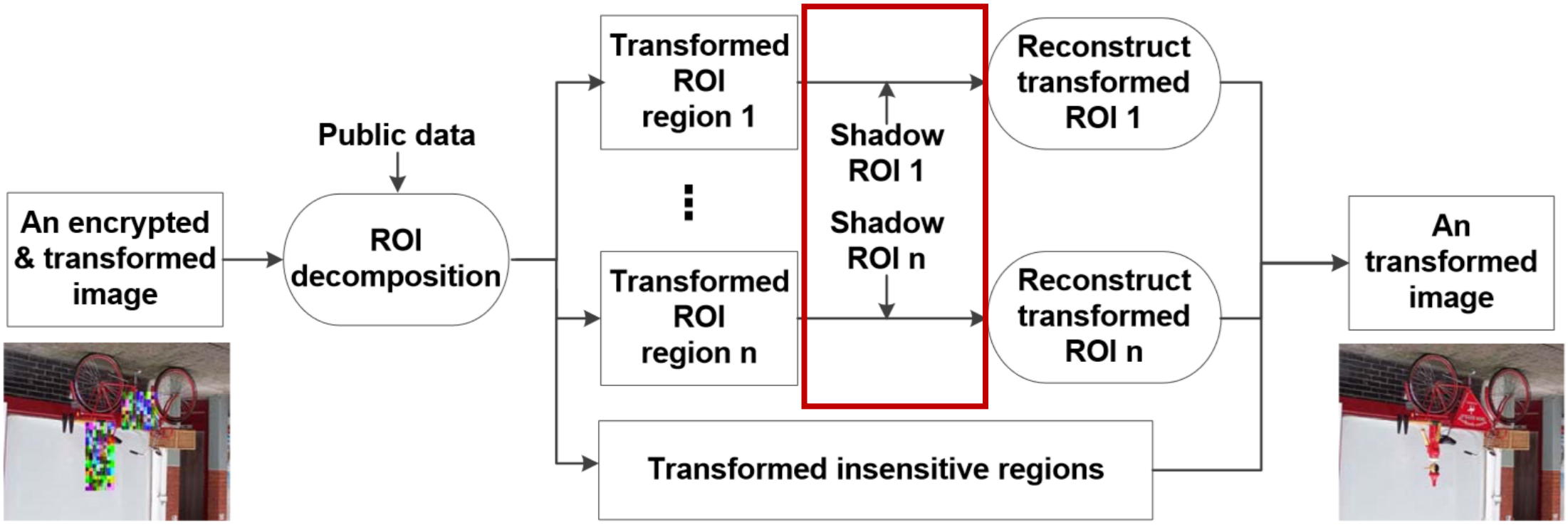
DCT Reconstruction



Receiver – Scenario 2



Receiver – Scenario 2



Transformations

- Consider a block in the YUV domain b, of a DCT coefficient block B
- Let $f(B) = b$
- After perturbation we have $B + P$ in the frequency domain

$$f(B + P) = f(B) + f(P) = b'$$

Critique

- Pros
  - Partial image sharing
  - Separate ROIs for decryption

Critique

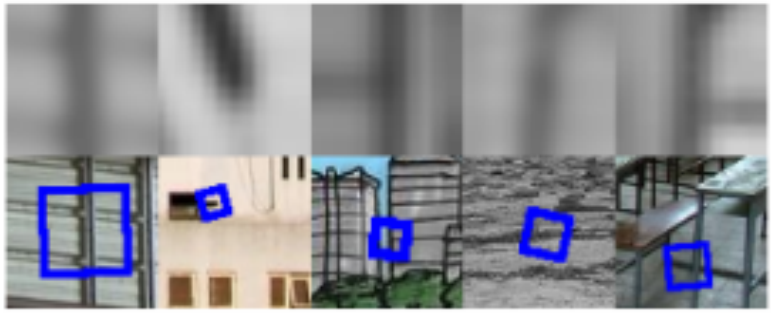
- Pros
  - Partial image sharing
  - Separate ROIs for decryption
- Cons
  - Subjective user privacy preference
  - Low-level features

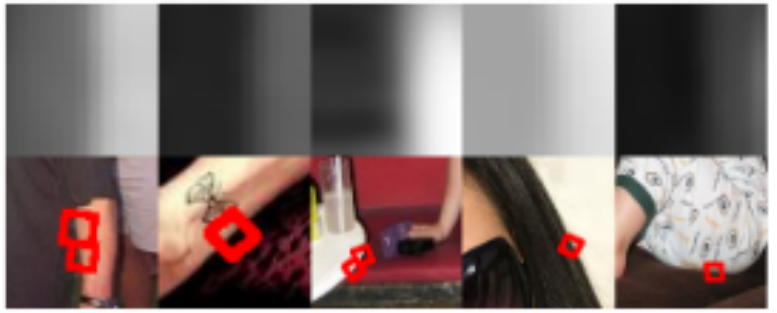
Automatic Privacy Settings

J. Yu, B. Zhang, Z. Kuang, D. Lin, J. Fan

IEEE Transactions on Information Forensics and Security, 2017

Related Work





Terms for Private photos				
studio	photograph	sexi	strobist	februari
blond	kid	hat	love	woman
year	smile	black	eye	famili
white	fun	portrait	selfportr	peopl
dress	valentin	day	friend	parti
femal	boy	birthday	face	model
fashion	daughter	children	coupl	self
babi	cute	child	girl	beauti
me	nikon	pretti	hair	man
photographi	young	lip	happi	wed

Terms for Public photos				
craft	mountain	natur	rock	draw
sky	tree	snow	jan	flower
januari	art	paint	lake	winter
view	citi	car	moon	landscap
anim	cat	road	north	build
frozen	island	full	ice	bridg
water	abstract	hdr	park	sea
hous	boat	fire	bird	handmad
architectur	sunset	sunris	cloud	macro
night	dog	illustr	design	river

Zerr et al. SIGIR 2012

Related Work

Features	Accuracy	F1-Measure	Precision	Recall
Test ($PiCalert_{783}$)				
FC6	81.10%	0.800	0.801	0.811
FC7	81.23%	0.805	0.804	0.812
FC8	**82.63%**	**0.823**	**0.822**	**0.826**
Prob	79.69%	0.794	0.792	0.797
SIFT + GIST	72.67%	0.661	0.672	0.727

Tonge and Caragea, 2015

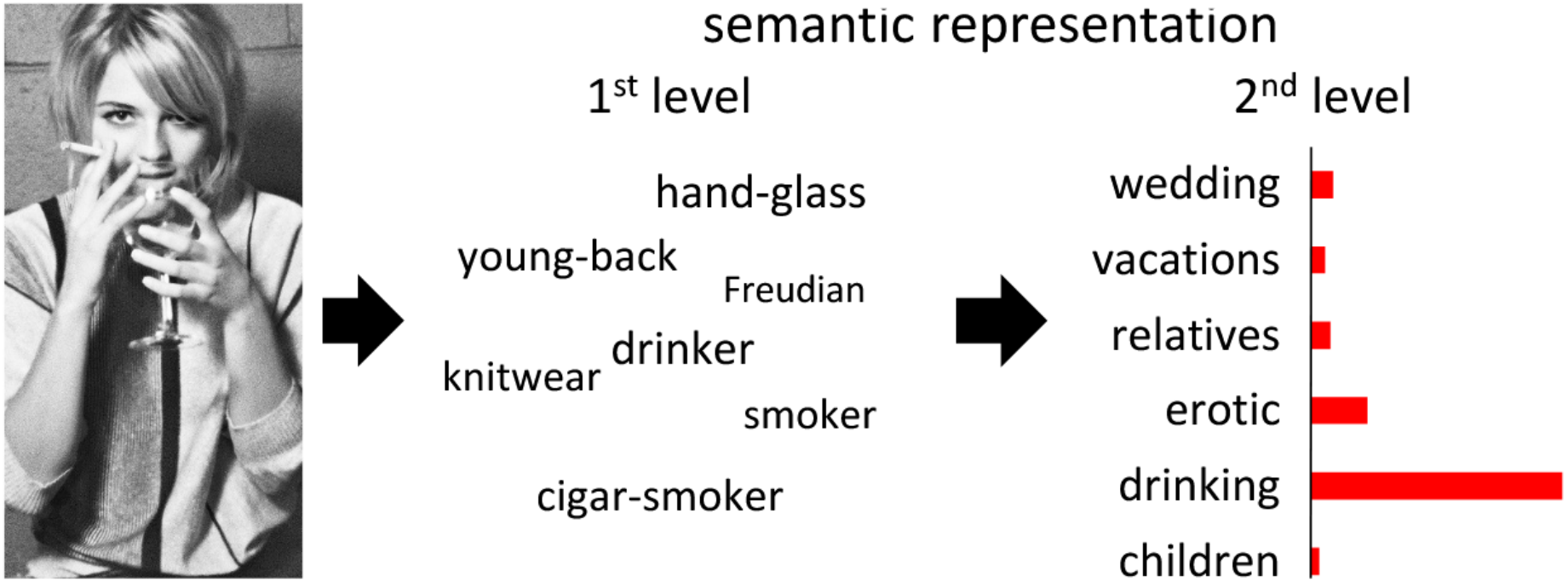
Related Work

(a) Private

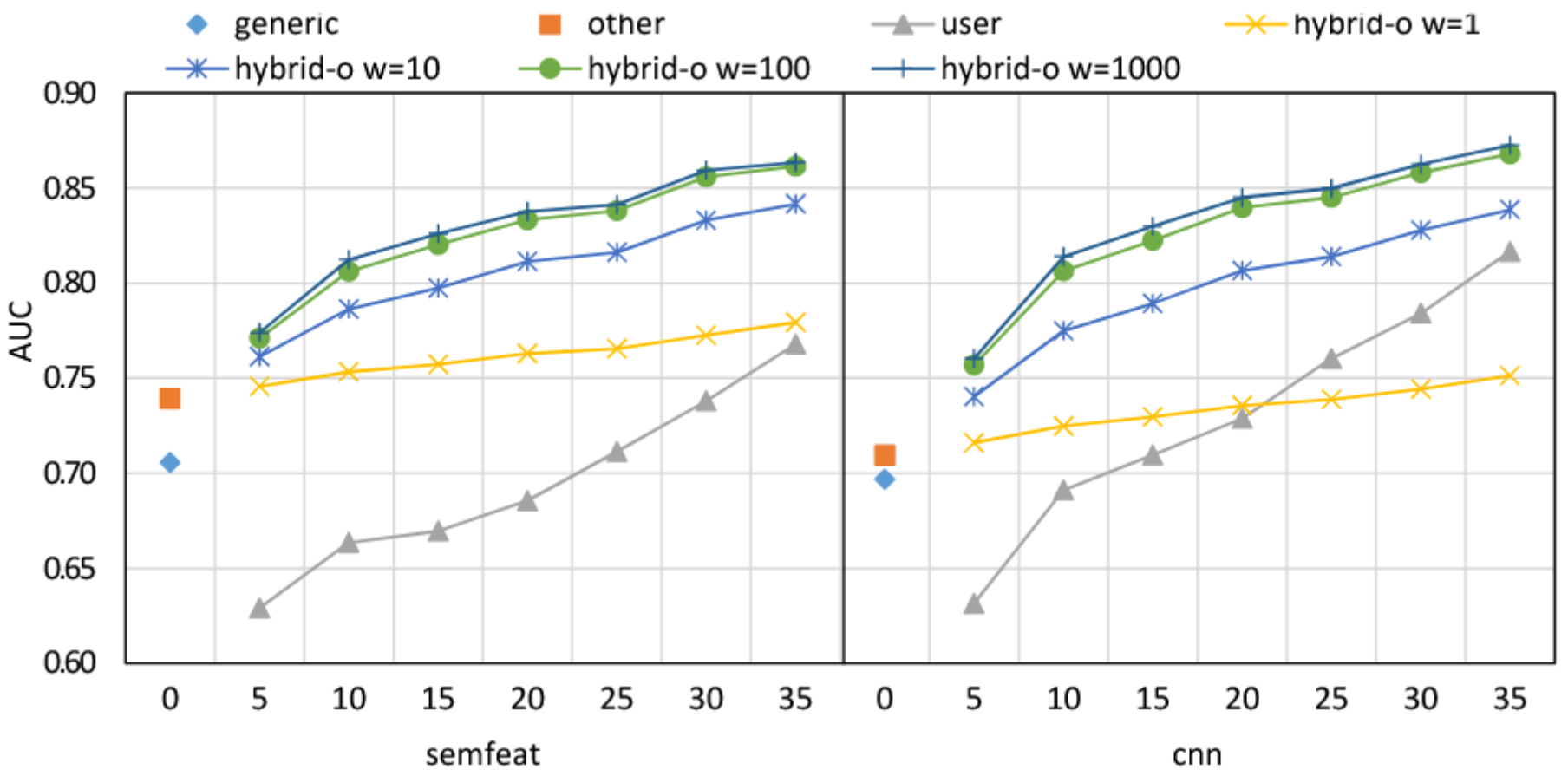
(b) Public

Tonge and Caragea, 2015

Related Work



Related Work



Spyromitros-Xioufis et al. ICMR 2016

iPrivacy

1) Deep CNNs for image segmentation and object classes
2) Object privacy-alignment developed based on privacy settings
3) Coarse-to-fine representation of privacy-sensitive objects
4) Hierarchical deep multi-task learning
5) Soft prediction method for predicting privacy settings

Image Segmentation

LC. Chen et al. *IEEE Trans. Pattern Anal. 2018*

Object Privacy Alignment

- 1000 object classes
- Cluster images based on similarity of objects

$$\kappa_I(X_i, X_j) = \sum_{l=1}^{1000} \delta(X_i^l, X_j^l)$$

$$\delta(X_i^l, X_j^l) = \begin{cases} 1, & if \quad X_i^l = X_j^l = 1; \\ 0, & otherwise \end{cases}$$

Object Privacy Alignment

- 1000 object classes
- Cluster images based on similarity of objects

Sparse vector of object classes in image i, j

$$\kappa_I(X_i, X_j) = \sum_{l=1}^{1000} \delta(X_i^l, X_j^l)$$

$$\delta(X_i^l, X_j^l) = \begin{cases} 1, & if \quad X_i^l = X_j^l = 1; \\ 0, & otherwise \end{cases}$$

Object Privacy Alignment

- For a given cluster C, denote the common list of privacy-settings P
- Relevance score for class C_i, given a setting $t \in P$

$$\gamma(C_i, t) = \frac{\| \Psi(C_i, t) \|}{\| \Psi(C, P) \|}$$

Object Privacy Alignment

- For a given cluster C, denote the common list of privacy-settings P
- Relevance score for class C_i, given a setting $t \in P$

Set of images with object class C_i and privacy setting t

$$\gamma(C_i, t) = \frac{\| \Psi(C_i, t) \|}{\| \Psi(C, P) \|}$$

Object Privacy Alignment

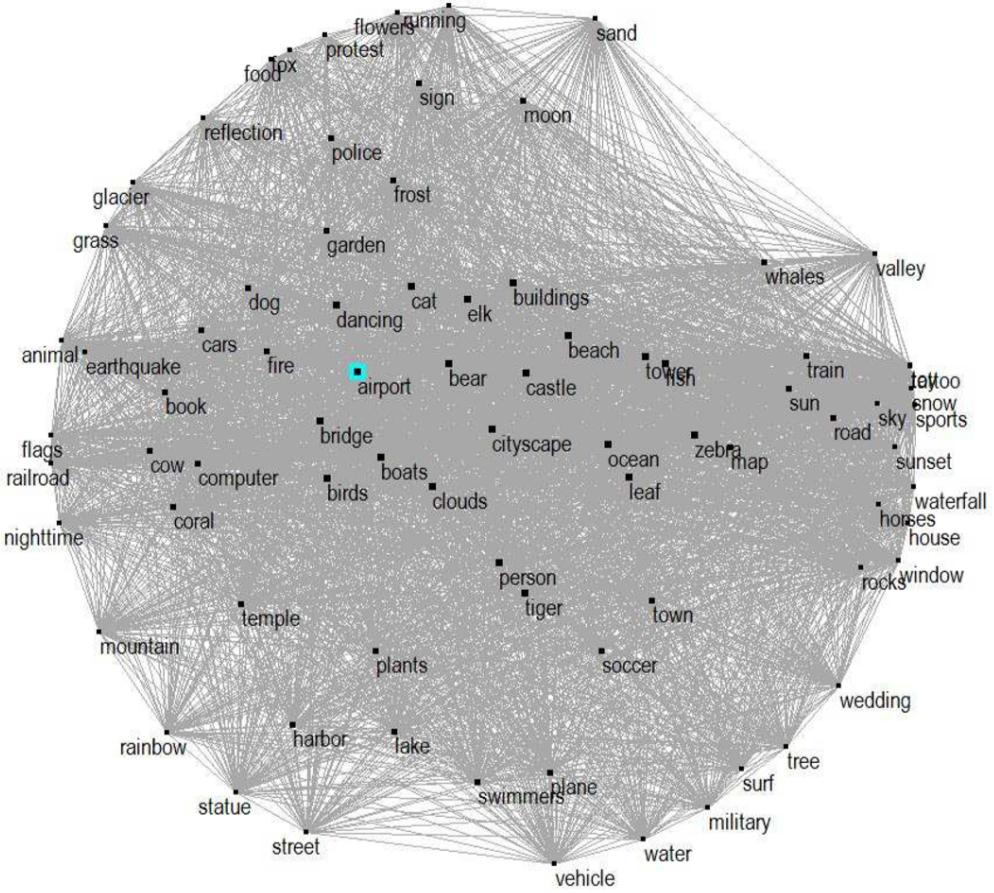
- For a given cluster C, denote the common list of privacy-settings P
- Relevance score for class C_i, given a setting $t \in P$

$$\gamma(C_i, t) = \frac{\| \Psi(C_i, t) \|}{\| \Psi(C, P) \|}$$

Set of images with object class C_i and privacy setting t

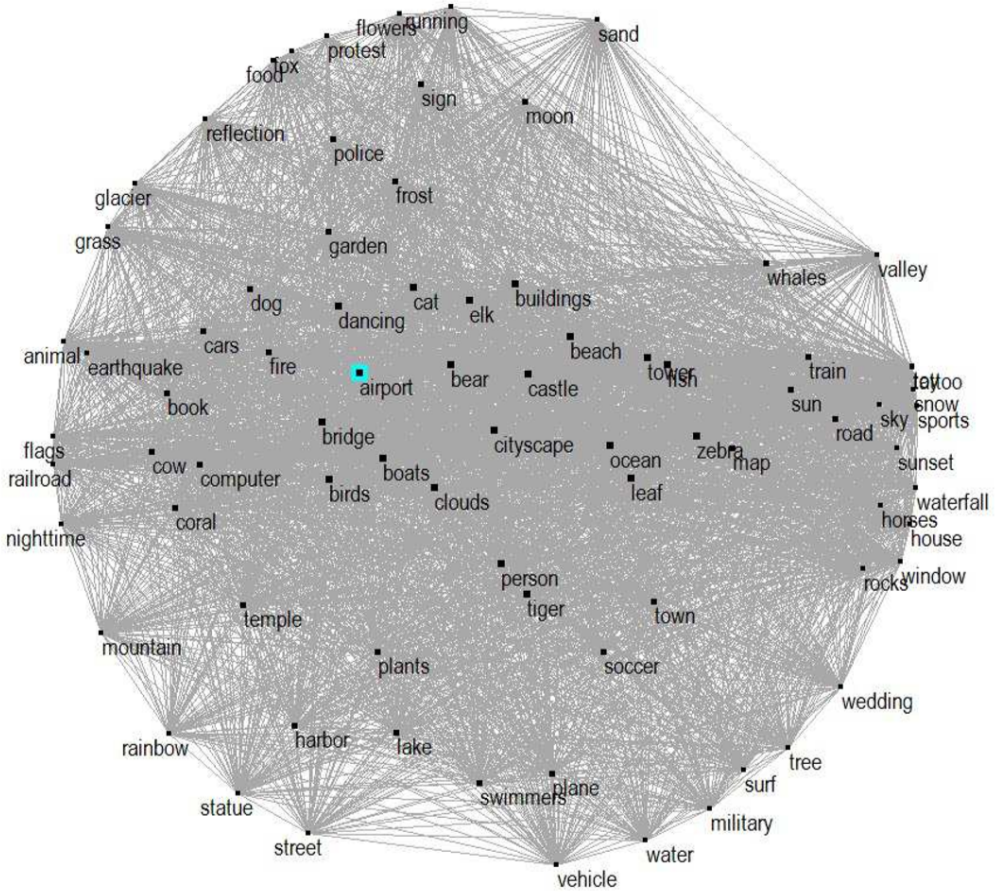
Full set of similar images in cluster C with privacy settings list P

Object Privacy Alignment



$$\phi(C_i, C_j) = \rho(C_i, C_j) \log \frac{\rho(C_i, C_j)}{\rho(C_i) + \rho(C_j)}$$

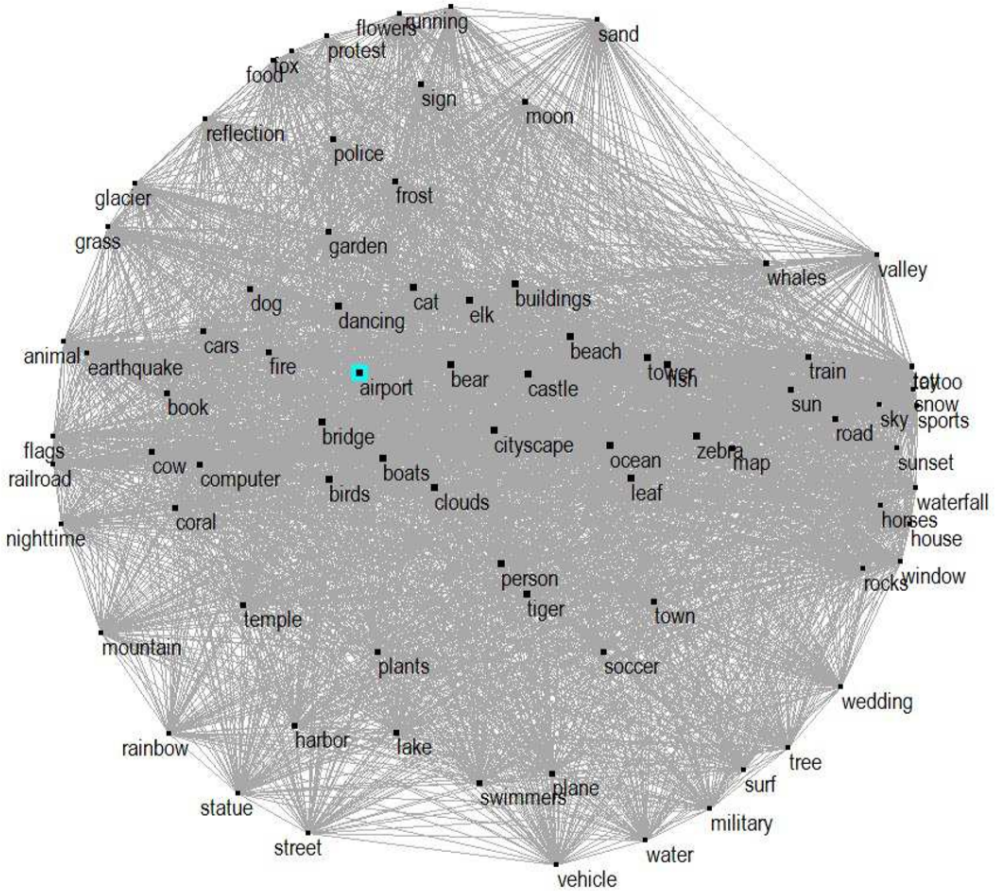
Object Privacy Alignment



Occurrence probability of object class C_i and C_j

$$\phi(C_i, C_j) = \rho(C_i, C_j) \log \frac{\rho(C_i, C_j)}{\rho(C_i) + \rho(C_j)}$$

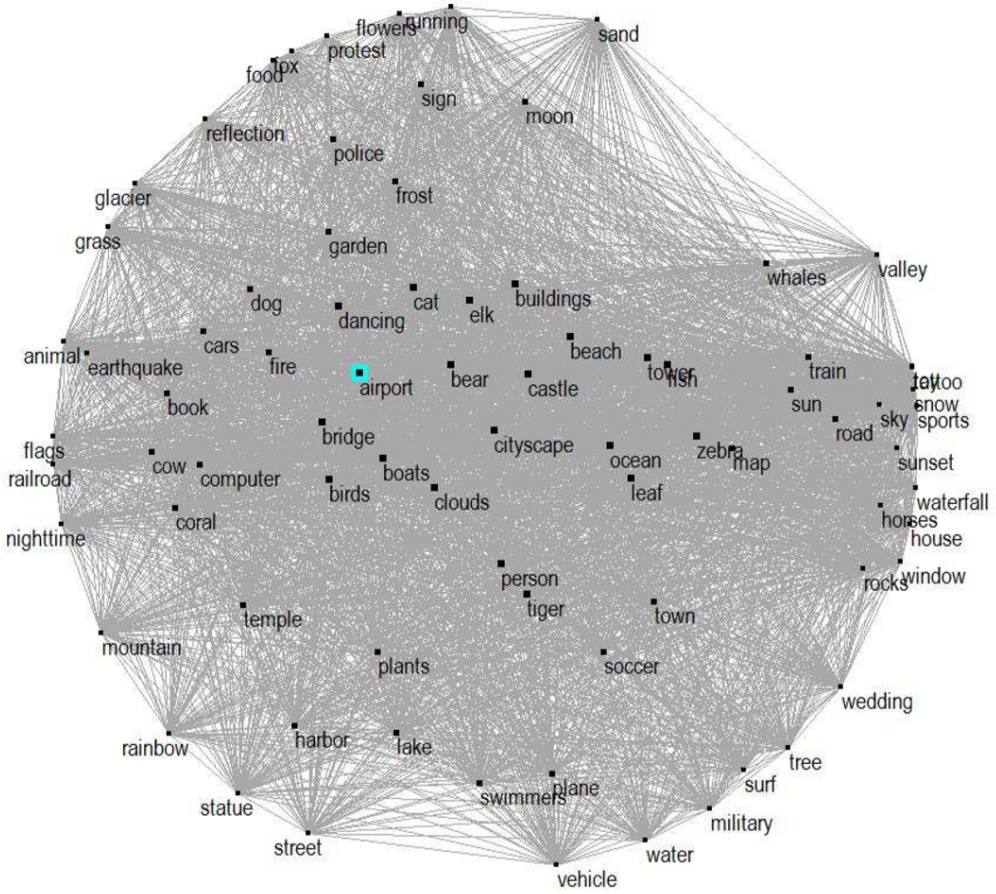
Object Privacy Alignment



Occurrence probability of object class C_i and C_j

$$\phi(C_i, C_j) = \rho(C_i, C_j) \log \frac{\rho(C_i, C_j)}{\rho(C_i) + \rho(C_j)}$$

Object Privacy Alignment

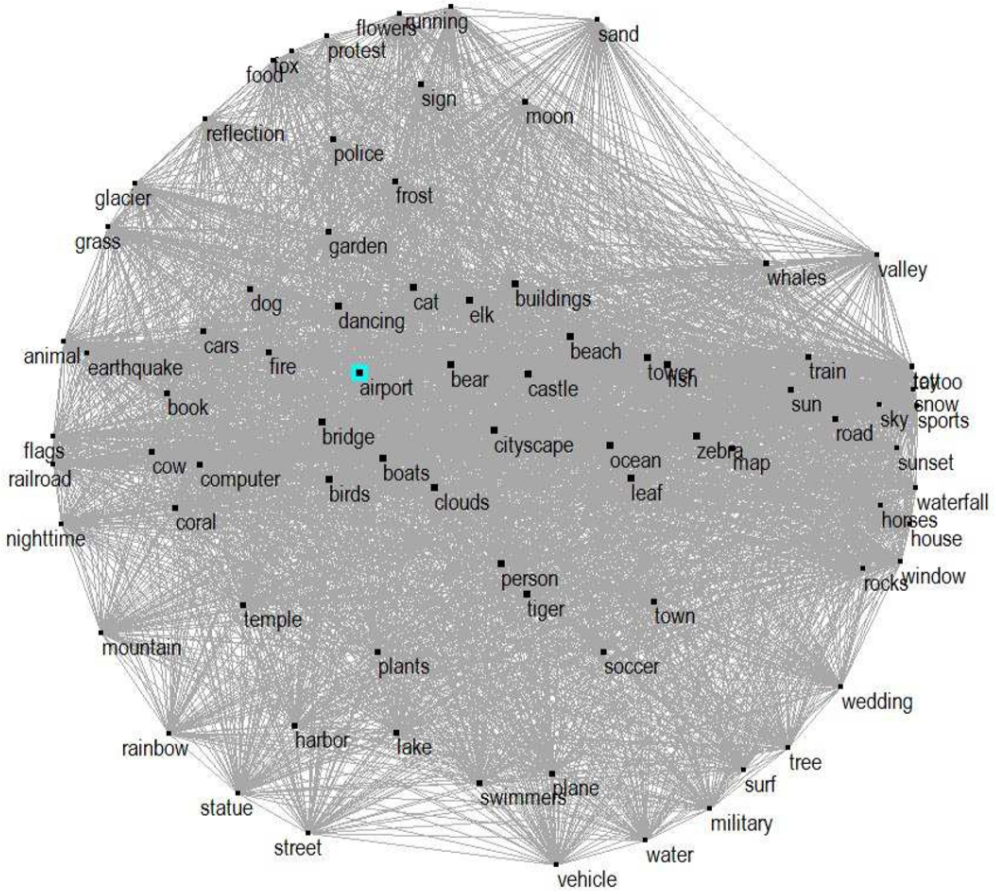


$$\phi(C_i, C_j) = \rho(C_i, C_j) \log \frac{\rho(C_i, C_j)}{\rho(C_i) + \rho(C_j)}$$

$$\psi_{ij} = \frac{\phi(C_i, C_j)}{\sum_{C_k \in \Omega_{C_i}} \phi(C_i, C_k)}$$

Transition probability matrix

Object Privacy Alignment

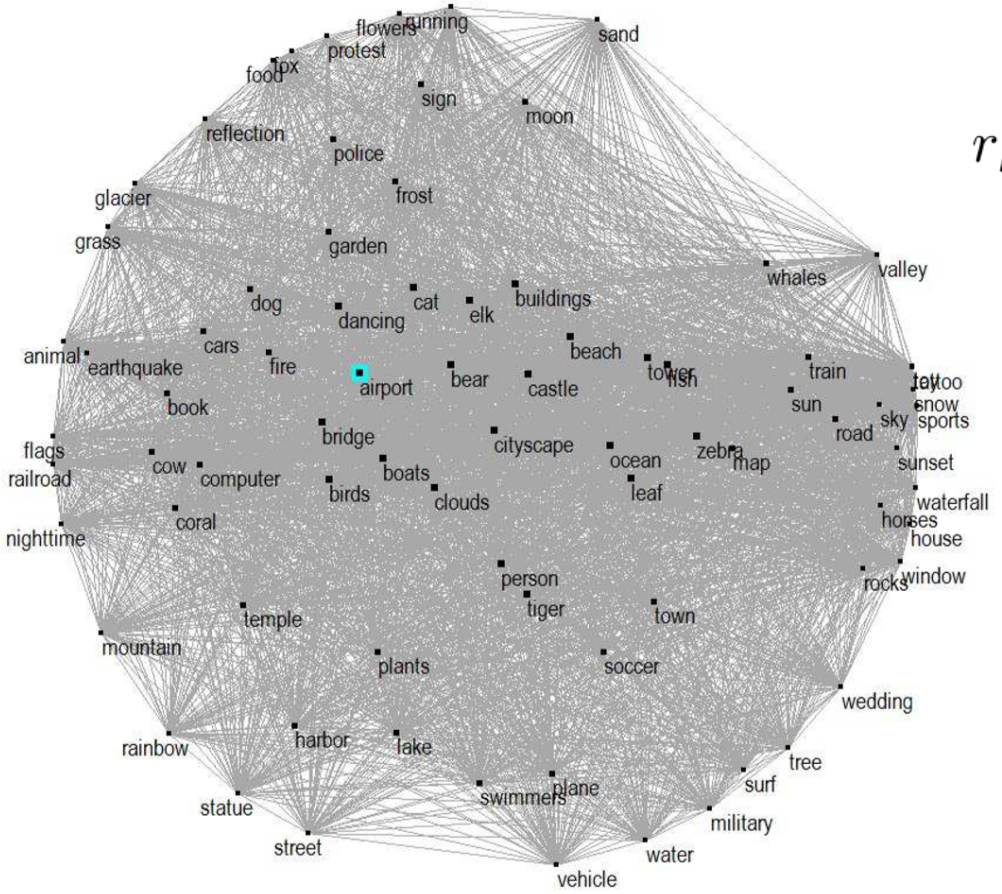


$$\phi(C_i, C_j) = \rho(C_i, C_j) \log \frac{\rho(C_i, C_j)}{\rho(C_i) + \rho(C_j)}$$

$$\psi_{ij} = \frac{\phi(C_i, C_j)}{\sum_{C_k \in \Omega_{C_i}} \phi(C_i, C_k)}$$

Transition probability matrix

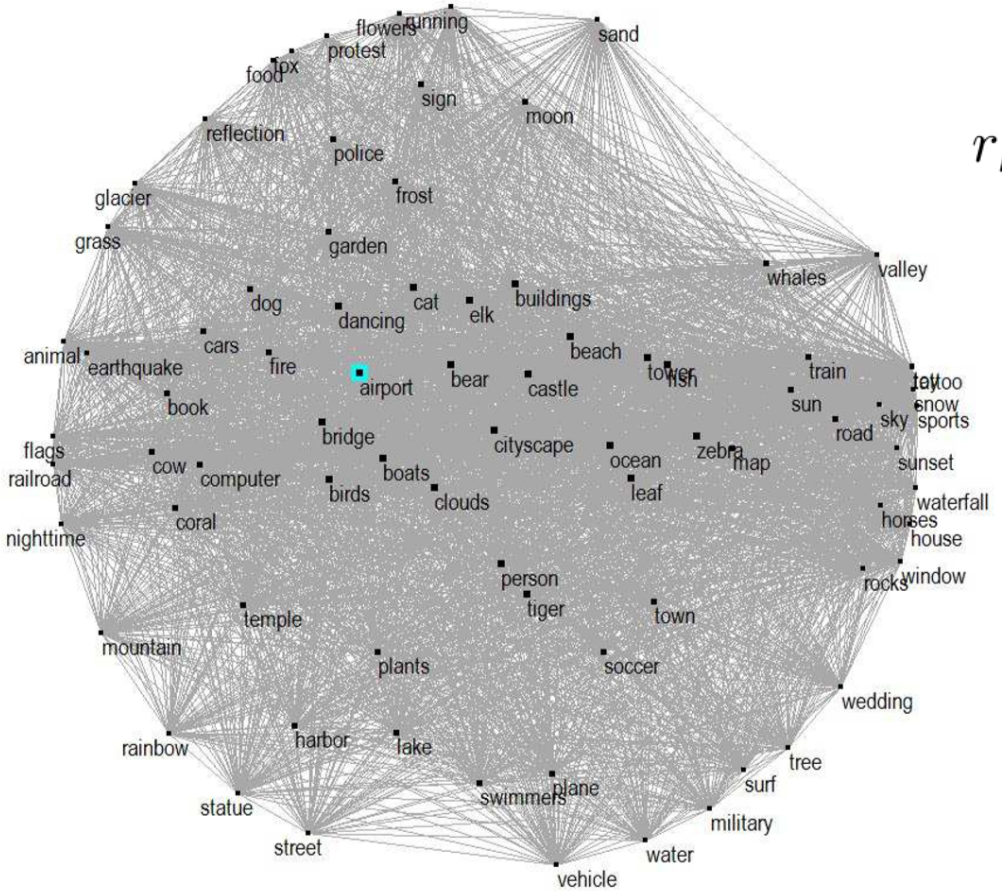
Object Privacy Alignment



$$r_k(C_i,t) = \theta \sum_{C_j \in \Omega_{C_i}} r_{k-1}(C_i,t)\psi_{ij} + (1-\theta)\gamma(C_i,t),$$

$$r_0(C_i,t) = \gamma(C_i,t)$$

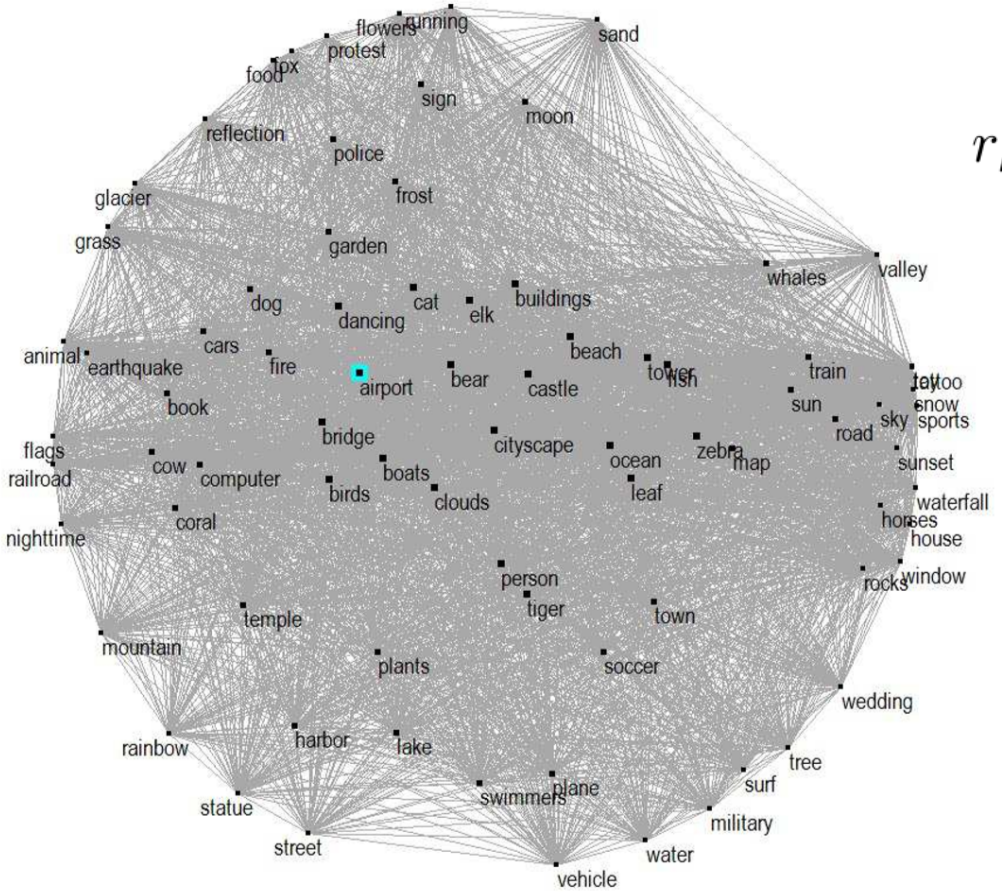
Object Privacy Alignment



$$r_k(C_i,t) = \theta \sum_{C_j \in \Omega_{C_i}} r_{k-1}(C_i,t)\psi_{ij} + (1-\theta)\gamma(C_i,t),$$

$$r_0(C_i,t) = \gamma(C_i,t)$$

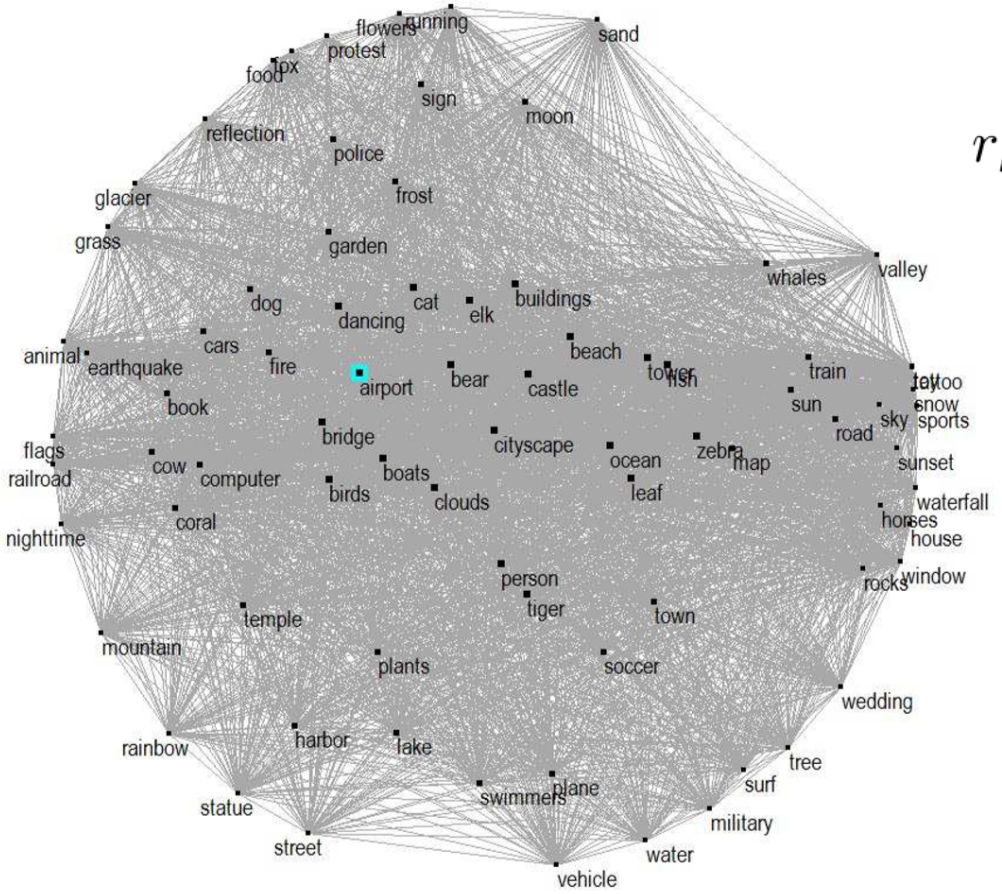
Object Privacy Alignment



$$r_k(C_i,t) = \theta \sum_{C_j \in \Omega_{C_i}} r_{k-1}(C_i,t)\psi_{ij} + (1-\theta)\gamma(C_i,t),$$

$$r_0(C_i,t) = \gamma(C_i,t)$$

Object Privacy Alignment



$$r_k(C_i,t) = \theta \sum_{C_j \in \Omega_{C_i}} r_{k-1}(C_i,t)\psi_{ij} + (1-\theta)\gamma(C_i,t),$$

$$r_0(C_i,t) = \gamma(C_i,t)$$

Visual Tree

- Provide an organization of large number of privacy-sensitive object classes

Visual Tree

- Provide an organization of large number of privacy-sensitive object classes

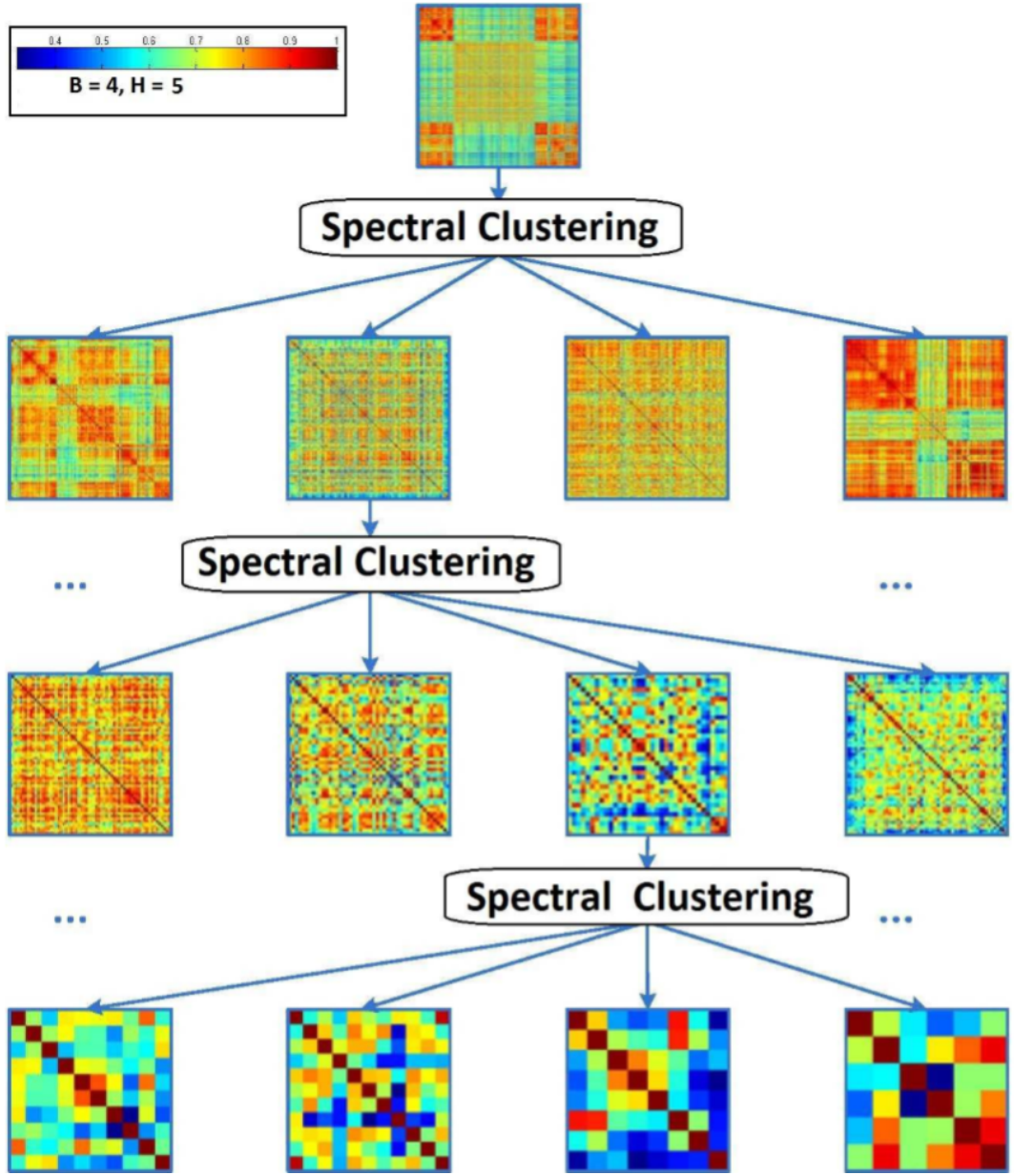
$$S(C_i, C_j) = \frac{1}{R^2} \sum_{x_l \in C_i} \sum_{x_h \in C_j} \kappa_o(x_l, x_h)$$

Visual Tree

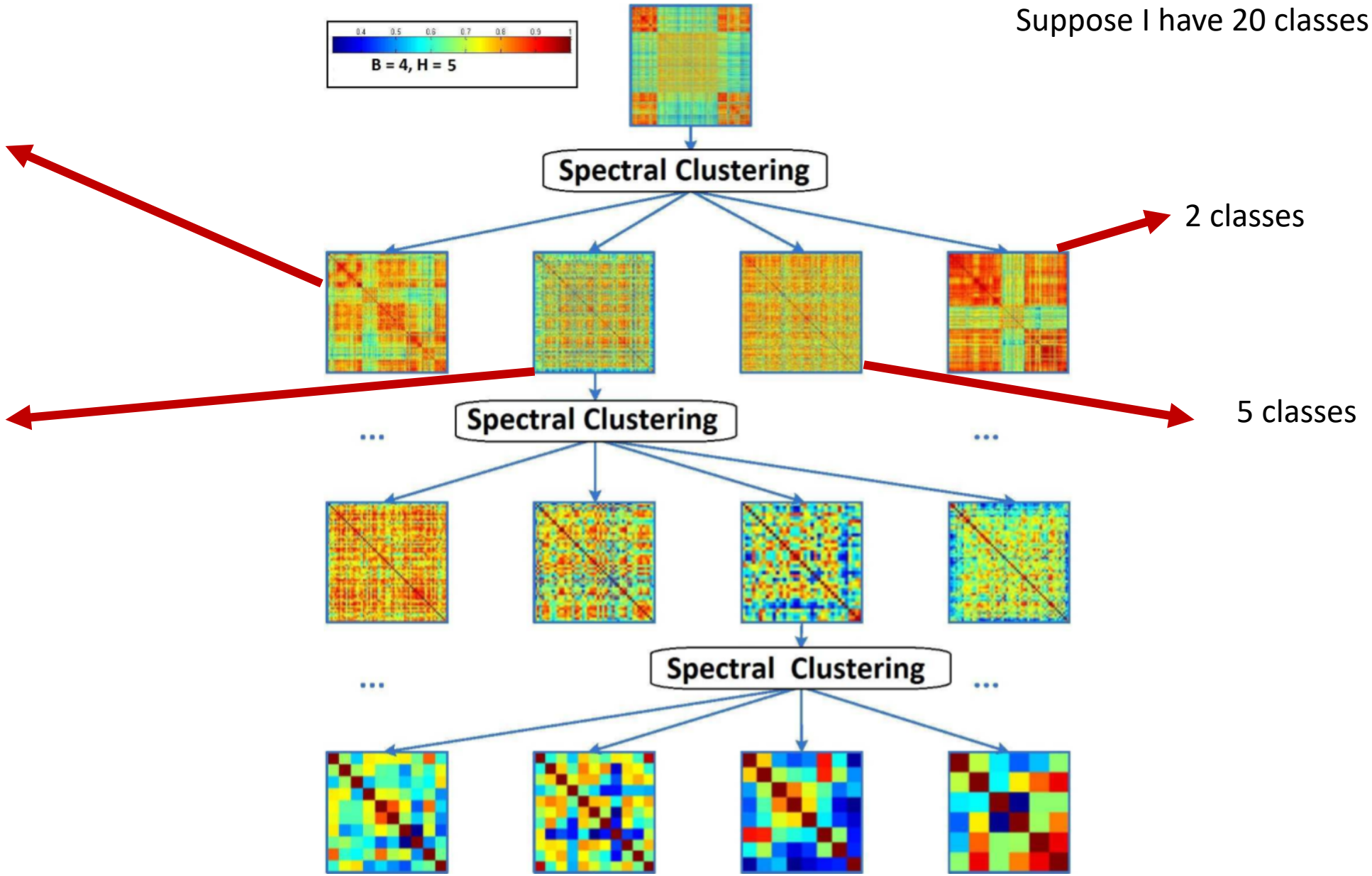
- Provide an organization of large number of privacy-sensitive object classes

$$S(C_i, C_j) = \frac{1}{R^2} \sum_{x_l \in C_i} \sum_{x_h \in C_j} \kappa_o(x_l, x_h)$$

$$\kappa_o(x_l, x_h) = \exp\left(\frac{-\|x_l - x_h\|}{2\sigma^2}\right)$$


0.4
0.5
0.6
0.7
0.8
0.9
1
B = 4, H = 5
Spectral Clustering
Spectral Clustering
Spectral Clustering

Suppose I have 20 classes



Visual Tree

- Provide an organization of large number of privacy-sensitive object classes

$$S(C_i, C_j) = \frac{1}{R^2} \sum_{x_l \in C_i} \sum_{x_h \in C_j} \kappa_o(x_l, x_h)$$

$$min \left\{ \psi(c, B) = \sum_{l=1}^{B} \frac{\sum_{C_i \in G_l} \sum_{C_j \in G^c / G_l} S(C_i, C_j)}{\sum_{C_i \in G_l} \sum_{C_h \in G_l} S(C_i, C_h)} \right\}$$

Visual Tree

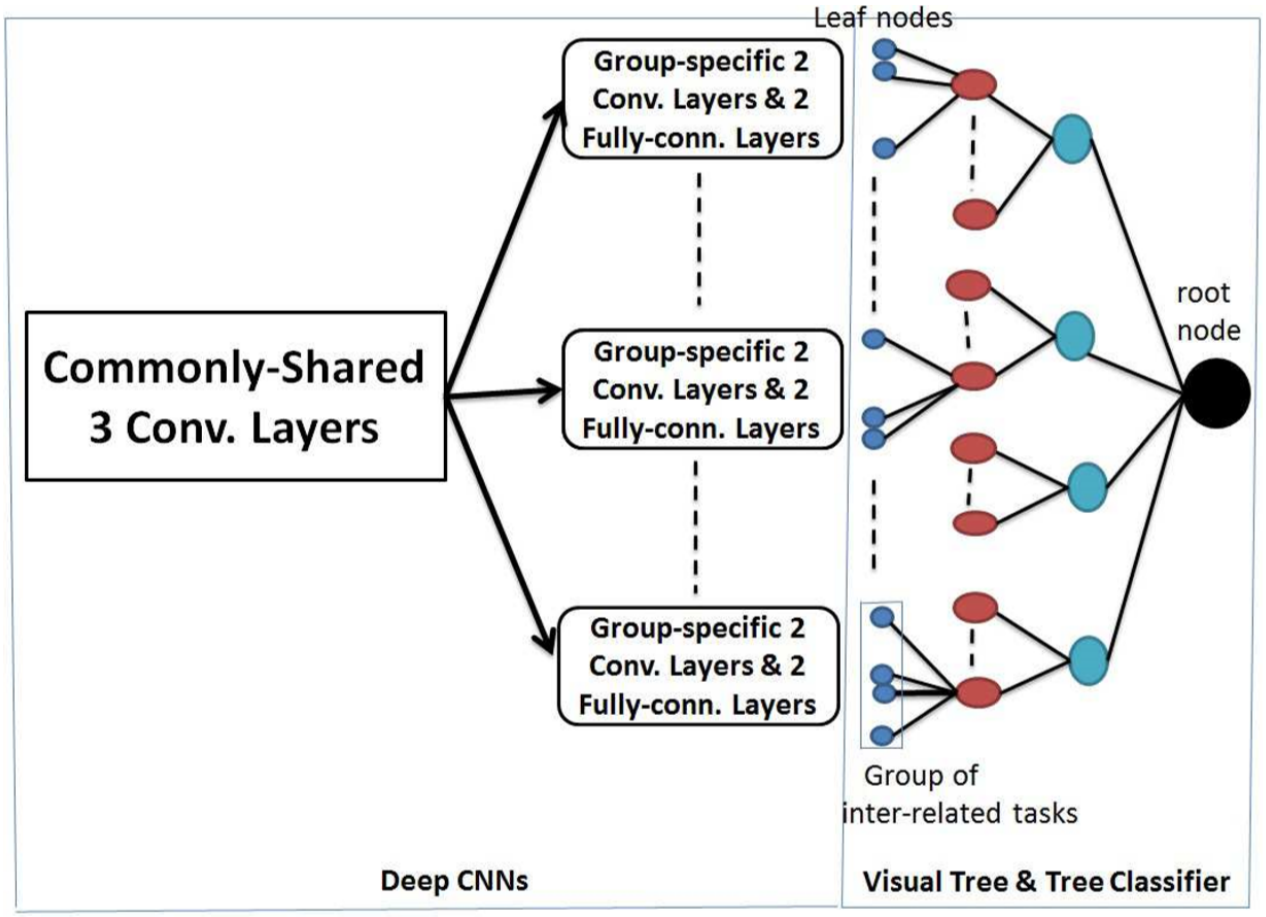
- Provide an organization of large number of privacy-sensitive object classes

$$S(C_i, C_j) = \frac{1}{R^2} \sum_{x_l \in C_i} \sum_{x_h \in C_j} \kappa_o(x_l, x_h)$$

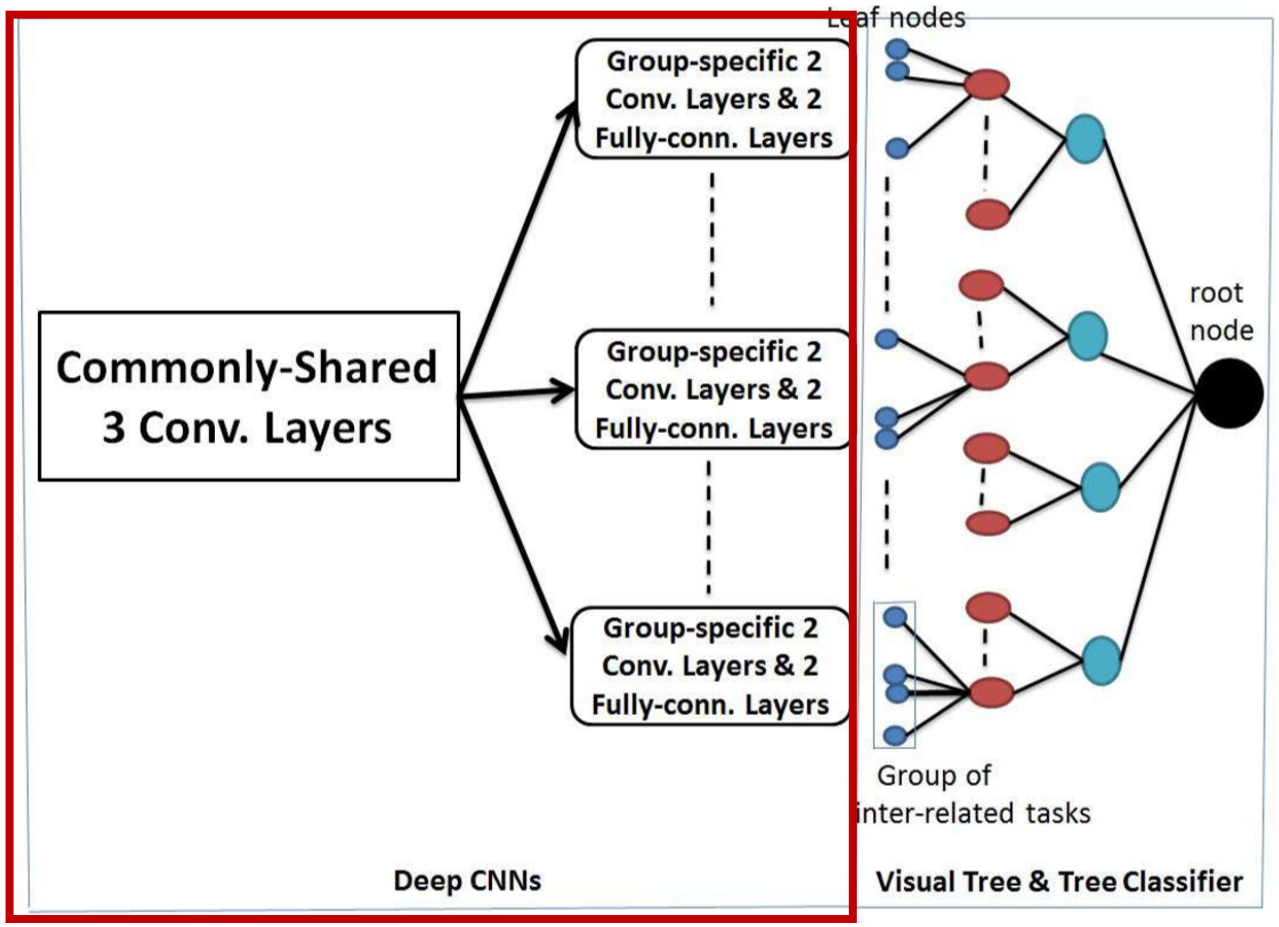
$$min \left\{ \psi(c, B) = \sum_{l=1}^{B} \frac{\sum_{C_i \in G_l} \sum_{C_j \in G^c / G_l} S(C_i, C_j)}{\sum_{C_i \in G_l} \sum_{C_h \in G_l} S(C_i, C_h)} \right\}$$

$$\{ G_l \mid l = 1, ..., B \}$$

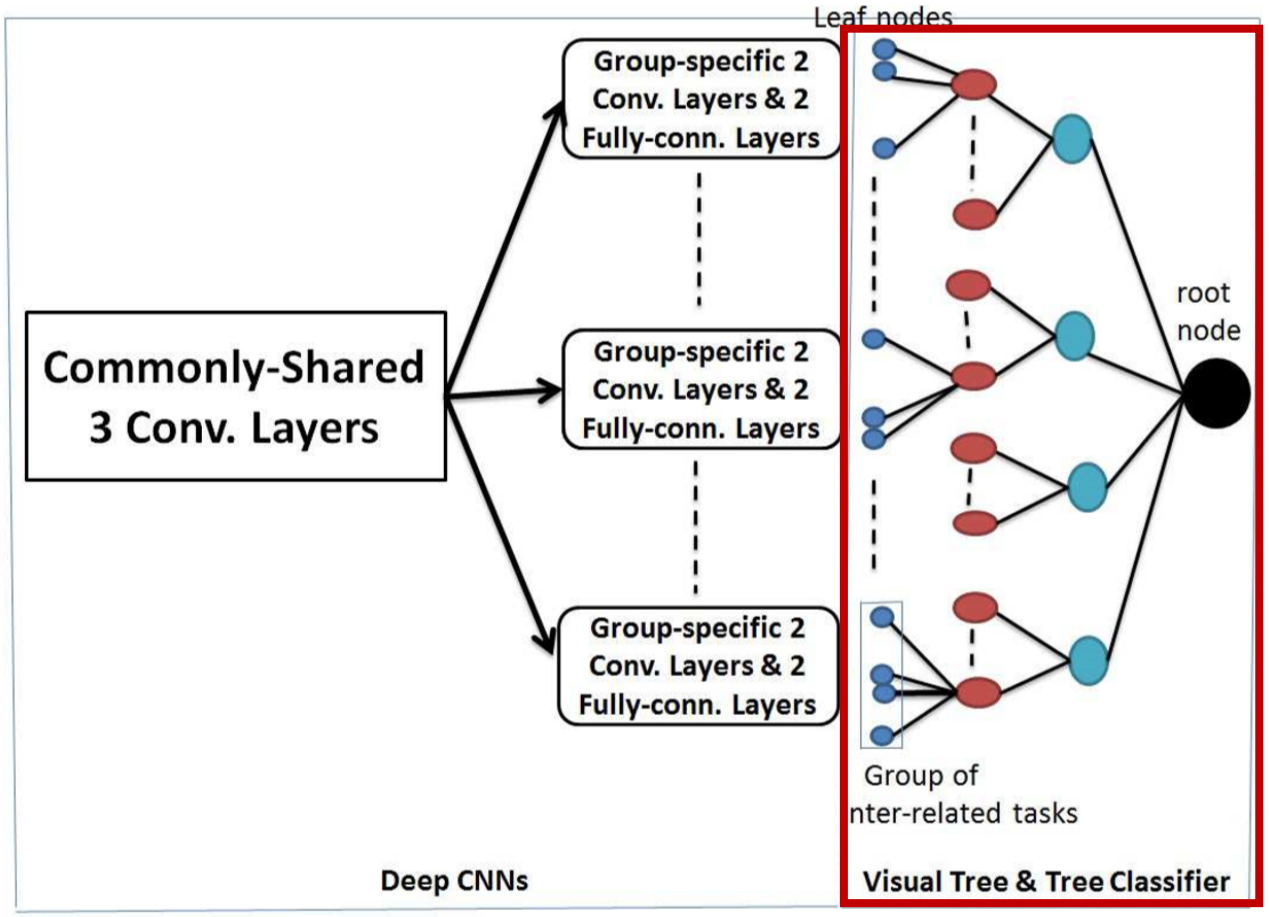
Hierarchical Learning



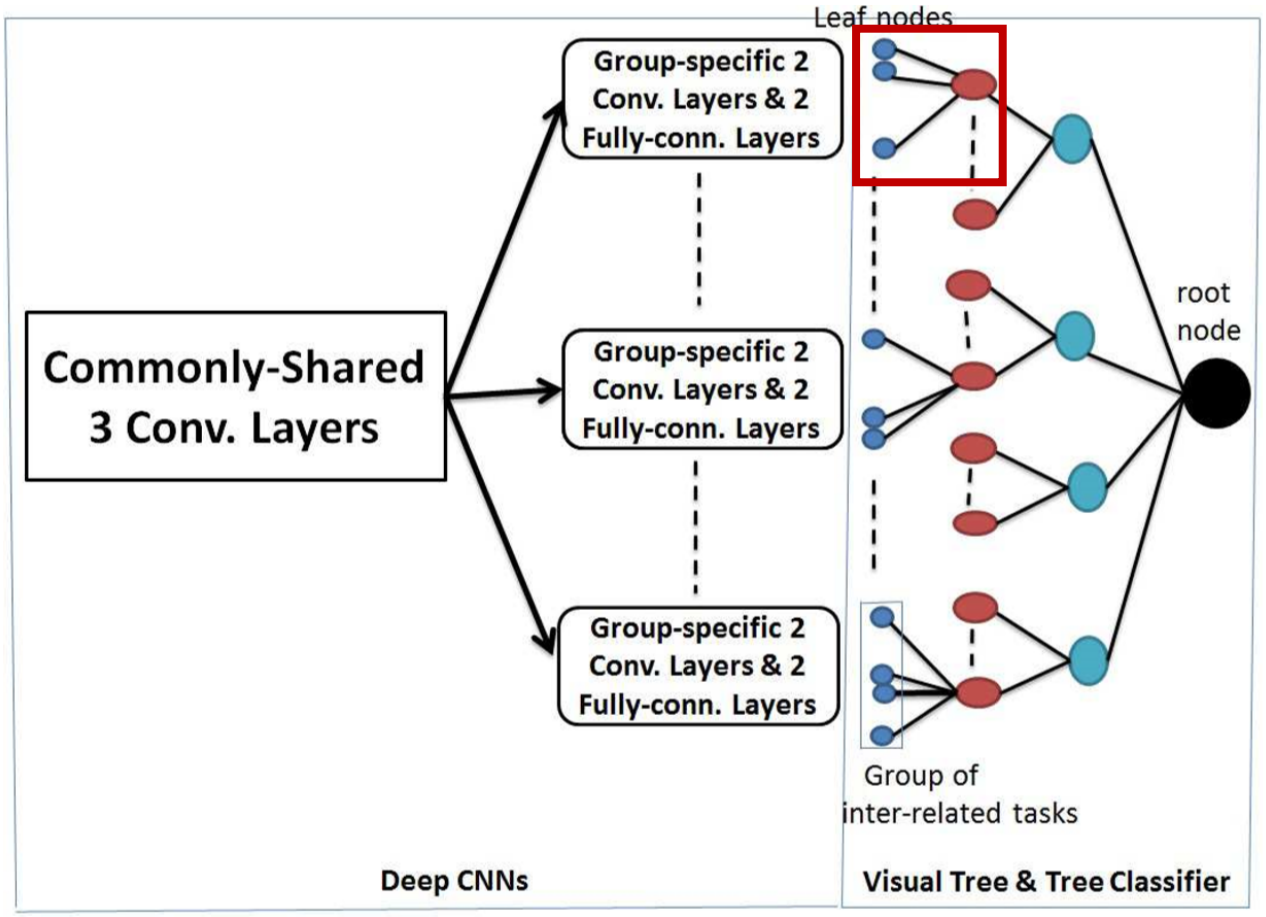
Hierarchical Learning



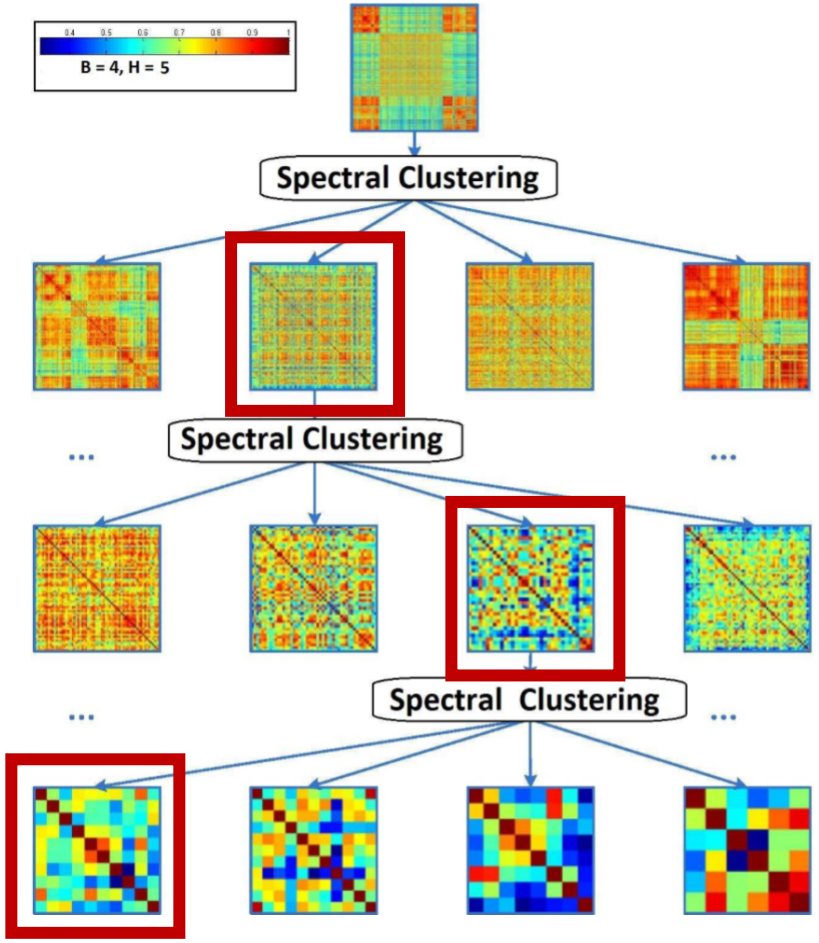
Hierarchical Learning



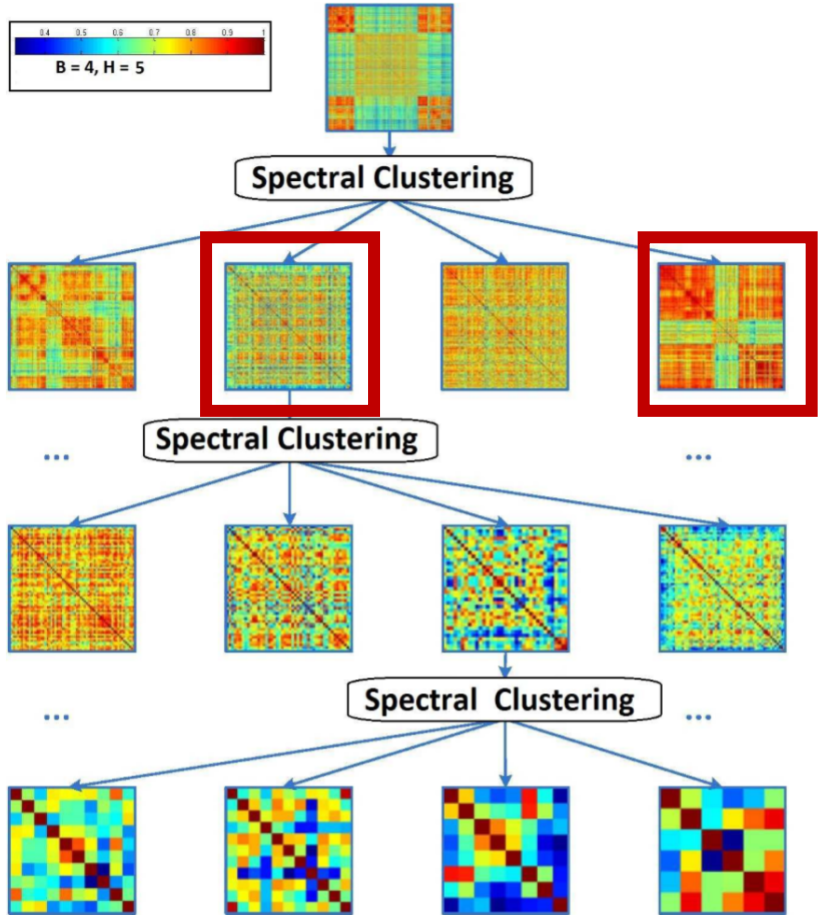
Hierarchical Learning



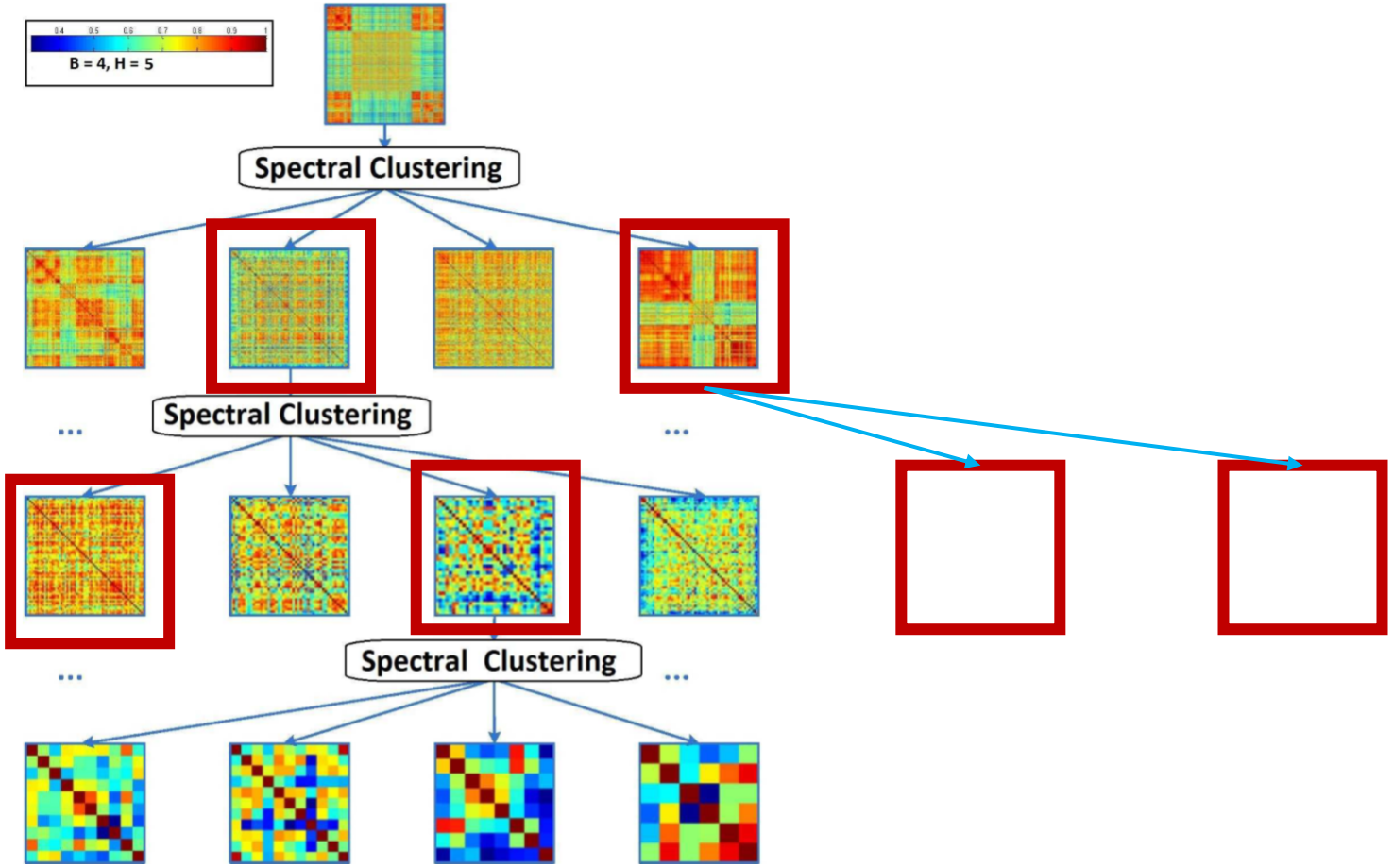
Prediction


B = 4, H = 5
Spectral Clustering
Spectral Clustering
Spectral Clustering

Soft Prediction



Soft Prediction



Critique

- Pros
  - Object-privacy alignment
  - Automatic image-privacy detection

Critique

- Pros
  - Object-privacy alignment
  - Automatic image-privacy detection
- Cons
  - Image features
  - User preference and social network

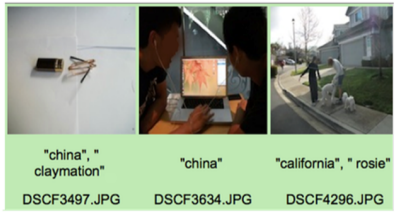
Critique

- Pros
  - Object-privacy alignment
  - Automatic image-privacy detection
- Cons
  - Image features
  - User preference and social network

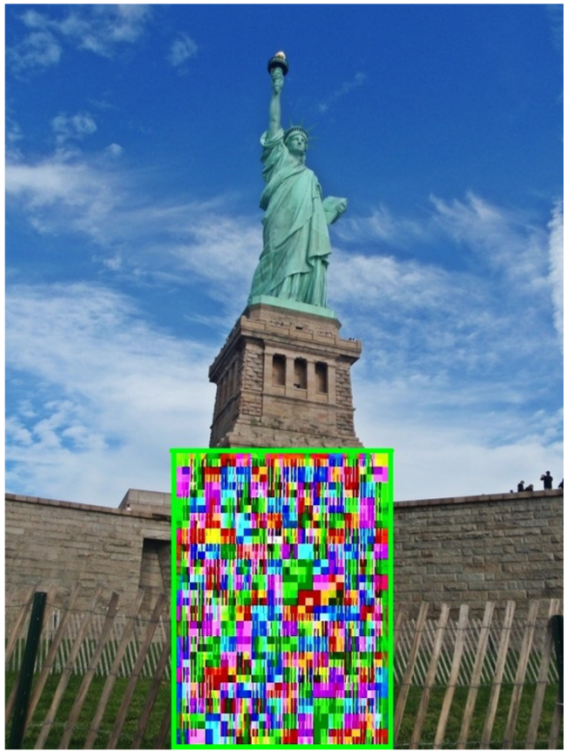
Conclusions

Rules
1. If not tagged with allen then ALLOW ACCESS
2. If not tagged with rosie then ALLOW ACCESS
3. If tagged with rosie AND allen then DENY ACCESS
4. Otherwise ALLOW ACCESS

Stan Can See...



Stan Can't See...



Future Work

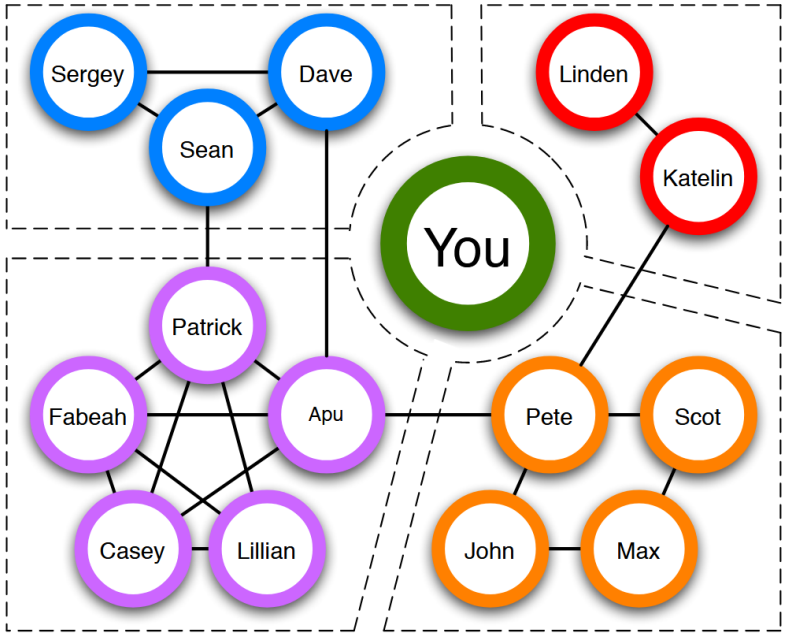
- Incorporate privacy-alignment with other features
  - Profile information
  - Tags and captions

(a) Private

(b) Public

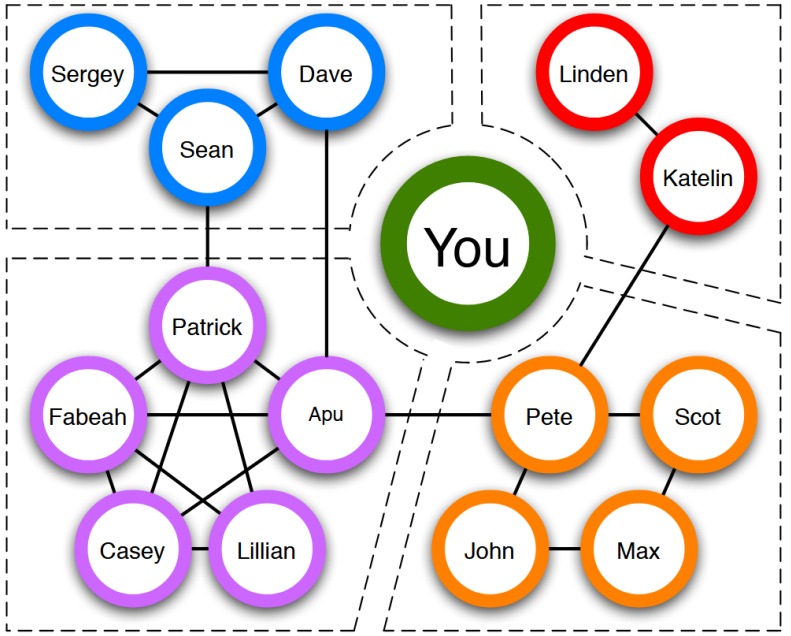
Future Work

- Incorporate privacy-alignment with other features
  - Profile information
  - Tags and captions
- Model user preferences



Future Work

- Incorporate privacy-alignment with other features
  - Profile information
  - Tags and captions
- Model user preferences



Thank You