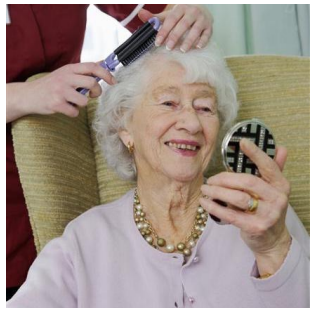
CHI23
Hamburg, Germany | Hybrid
April 23-28, 2023
reCHInnecting

Modeling the Trade-off between Privacy Preservation and Activity Recognition on Low-Resolution Images

Yuntao Wang*[1], **Zirui Cheng***[1], Xin Yi[1], Yan Kong[1], Xueyang Wang[1], Xuhai Xu[2], Yukang Yan[1], Chun Yu[1], Shwetak Patel[2], Yuanchun Shi[1]

[1] Tsinghua University, China
[2] University of Washington, USA

Motivation






Visual Privacy Exposure

Identifiable Face, Nudity, Valuable Property, Social Relationship, etc.

Motivation

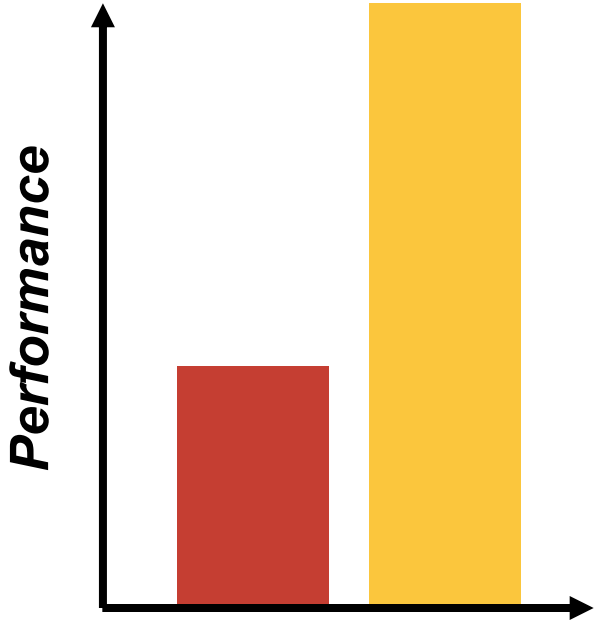
Researchers in the computer vision filed proposed a fundamental solution towards the construction of a privacy preserving vision-based system is lowering the image sensor's resolution from the hardware level [10, 36, 44, 46, 56, 57].

Motivation

Low Resolution

Main Recognition Task

Visual Privacy Preservation

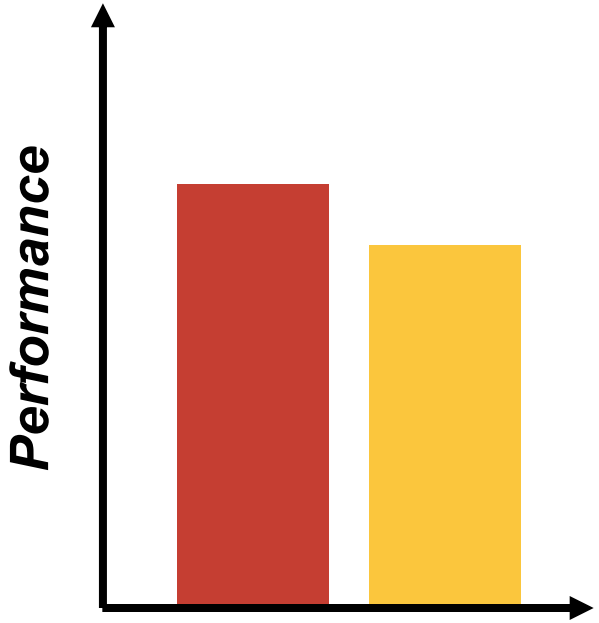


Motivation

Middle Resolution

Main Recognition Task

Visual Privacy Preservation

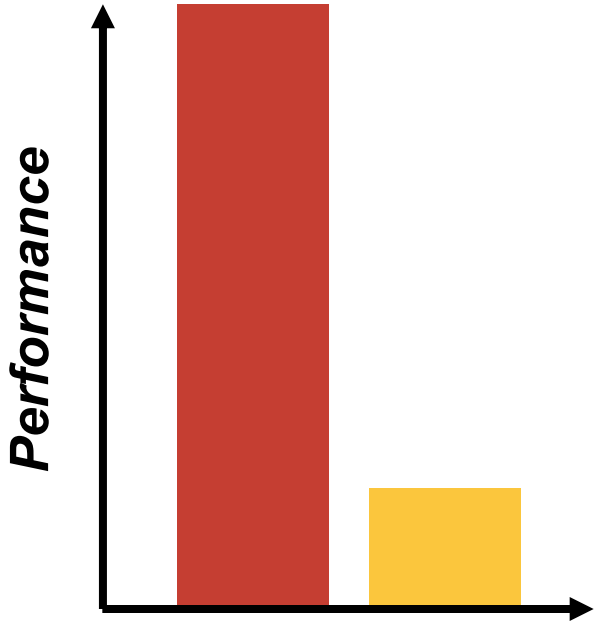


Motivation

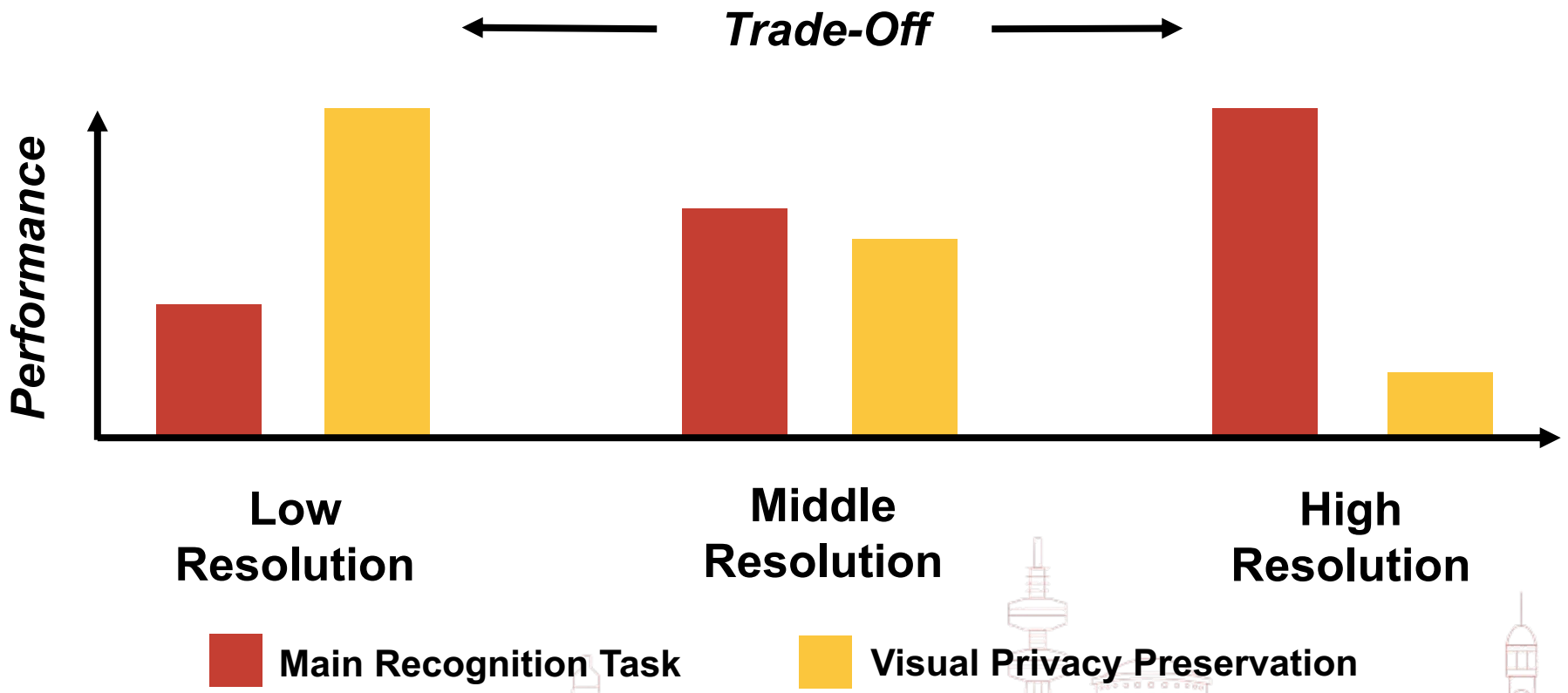
High Resolution

Main Recognition Task

Visual Privacy Preservation



Motivation


Trade-Off
Performance
Low Resolution
Middle Resolution
High Resolution
Main Recognition Task
Visual Privacy Preservation

Research Scenario

Activities of Daily Living

Feeding

Dressing

Personal Hygiene

Toilet Hygiene

Functional Mobility

Problem Definition

$$S(r) = L_T\left(f_T(f_r(X)), g_T(X)\right) - \lambda \sum_{i=1}^{n} \omega_i L_P^i\left(f_{Pi}(f_r(X)), g_{Pi}(X)\right)$$

Recognition Function f_T and f_P

Recognize main activities and privacy features on images of varying resolutions.

Evaluation Function L_T and L_P

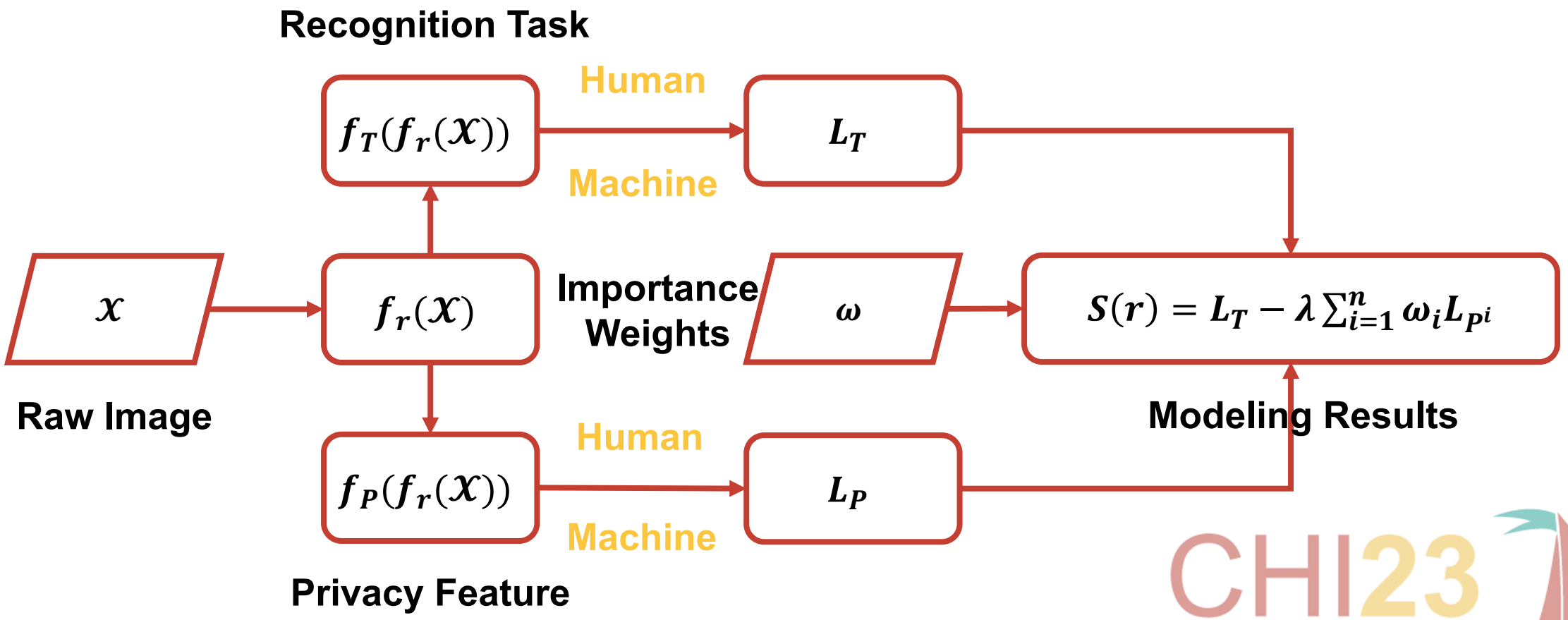
Evaluate the recognition performance of the recognition function.

Importance Weights ω

Represent the users' perceived importance of privacy features.

CHI23
Hamburg, Germany | Hybrid
April 23-28, 2023
reCHInnecting

Implementation Pipeline



Study 1: Quantifying the Importance Weights

Modeling the Trade-off of Privacy Preservation and Activity Recognition on Low-Resolution Images

Online User Study

Category	Feature	High Resolution		Low Resolution		Significance
		avg.	std.	avg.	std.	
Biometric Identification	Identifiable Face	60.2	24.3	**57.5**	26.0	$p = 0.13$
	Gender	43.5	29.2	43.4	29.4	$p = 0.81$
	Skin Color	42.0	28.6	43.1	27.3	$p = 0.94$
	Age Group	42.9	25.1	41.2	25.8	$p = 0.35$
	Weight Group	43.9	27.2	40.9	27.2	$p = 0.16$
	Hair Color	36.2	27.4	40.9	28.1	$p = 0.05$
	Eye Color	40.4	28.9	40.3	28.4	$p = 0.90$
	Height Group	37.3	25.8	40.0	27.7	$p = 0.30$
Personal Marker / Information	Nudity	61.6	30.9	**62.9**	29.4	$p = 0.71$
	Home Address	62.8	23.1	55.6	26.1	$\mathbf{p = 0.01}$
	Number/code	57.5	25.5	55.6	26.6	$p = 0.79$
	Medical Treatment	60.4	23.2	51.7	25.9	$\mathbf{p < 0.001}$
	Physical Disability	52.1	25.1	49.4	26.0	$p = 0.25$
	Hand Writing	52.6	26.4	44.9	27.7	$\mathbf{p < 0.01}$
	Birthday	54.2	26.8	44.7	28.5	$\mathbf{p < 0.01}$
	Clothing	40.5	27.9	41.5	27.5	$p = 0.94$
	Tattoo	42.2	28.7	39.2	28.6	$p = 0.34$
Ethnicity	Religion	41.8	27.7	44.6	26.6	$p = 0.29$
	Race	40.1	26.5	42.2	27.7	$p = 0.64$
	Nationality	42.1	28.3	41.3	27.5	$p = 0.46$
Society	Relationship	60.3	24.8	**52.9**	25.7	$\mathbf{p < 0.001}$
	Employment	58.2	22.8	52.1	25.8	$p = 0.05$
	Pet	37.3	24.4	39.1	27.8	$p = 0.46$
Safety	Valuable Property	64.0	25.0	**59.6**	26.1	$p = 0.34$
	Living Schedule	59.3	24.4	59.1	26.3	$p = 0.10$

Online User Study

Identifiable Face

Nudity

Relationship

Valuable Property

Privacy Features

Study 2: Evaluating Humans' Recognition Performance

Modeling the Trade-off of Privacy Preservation and Activity Recognition on Low-Resolution Images

Online User Study

1. What is the main character doing?
☐ Dressing. ☐ Feeding. ☐ Toileting.
☐ Moving. ☐ Personal hygiene (including brushing/combing/styling hair). ☐ No person.
2. Who is the main character?
☐  ☐  ☐ 
☐  ☐  ☐ No person.
3. Is there any valuable properties (e.g., safe box, jewelry, watch, ring, cash, necklace)?
☐ Yes. ☐ No.
4. Is the main character fully or semi naked? ☐ Yes. ☐ No.
5. What's the relationship between the characters?
☐ Family or friend. ☐ Physician-patients. ☐ No relationship.
☐ Only one person. ☐ No person.
6. Please choose 6. ☐ 1. ☐ 2. ☐ 3. ☐ 4. ☐ 5. ☐ 6.

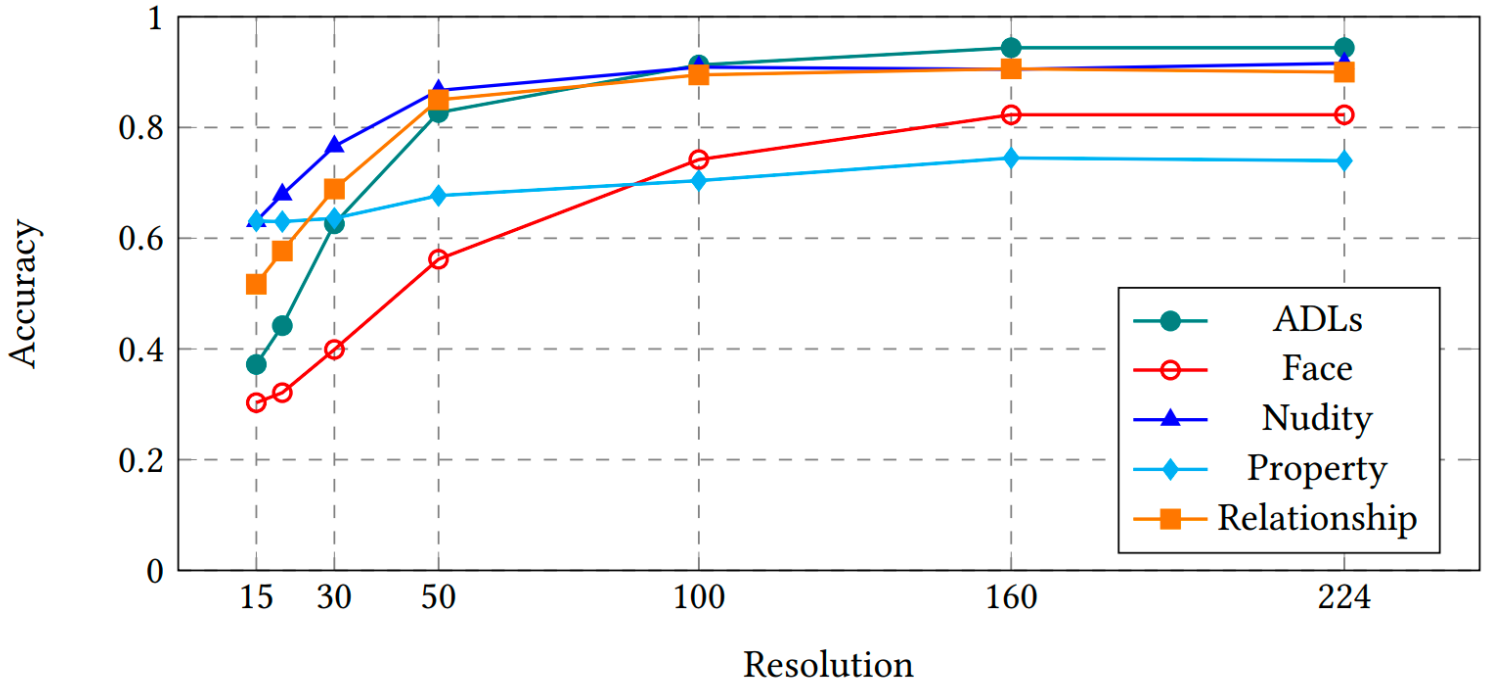
Web-Based User Interface

Online User Study

Humans' Recognition Performance

457 **Participants**

9,597 **Valid Answers**



Study 3: Evaluating Machines' Recognition Performance

Modeling the Trade-off of Privacy Preservation and Activity Recognition on Low-Resolution Images

Computer Vision Experiments

ADLs Classification: *Vision Transformer, ResNet.*

Nudity Recognition: *NudeNet.*

Facial Identification: *InsightFace.*

Computer Vision Experiments

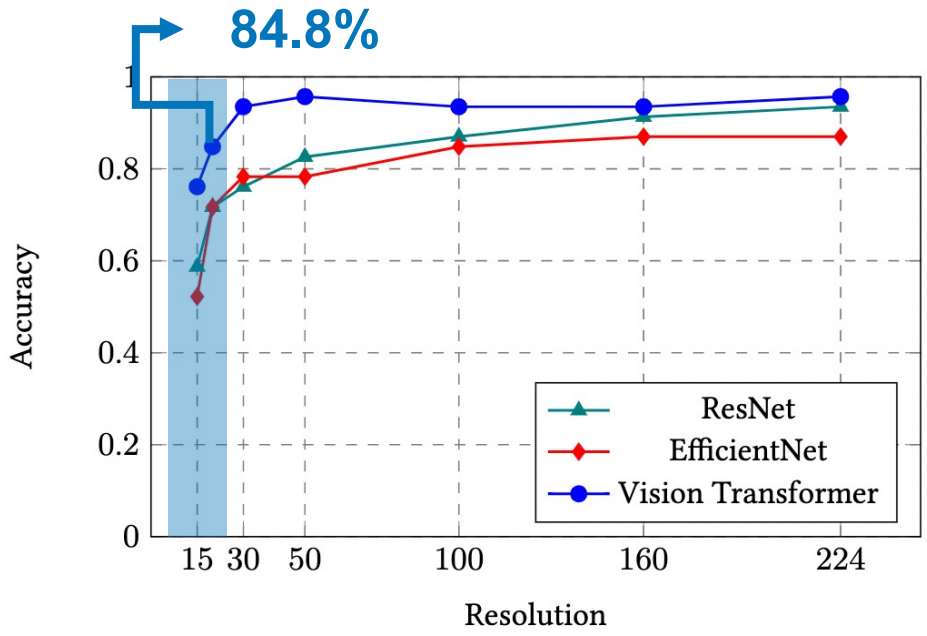
Property and Object Detection:

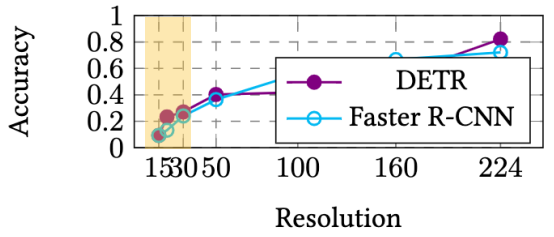
Faster R-CNN, DETR.

Relationship Classification:

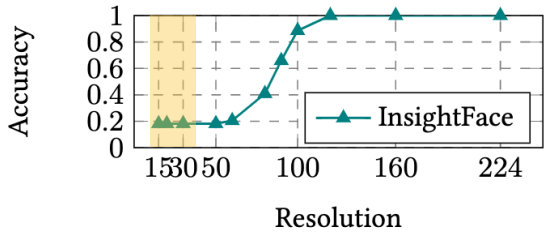
Graph Reasoning Model.

Computer Vision Experiments

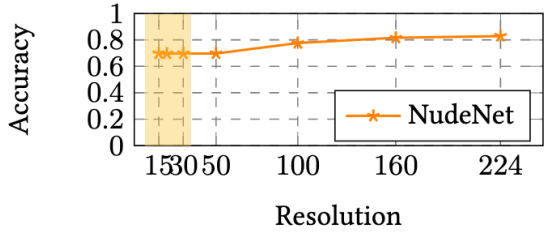




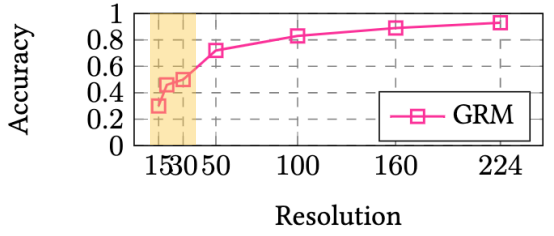
(a) Accuracy of objects detection results.



(b) Accuracy of facial recognition results.



(c) Accuracy of nudity recognition results.



(d) Accuracy of relationship classification results.

Machines' Recognition Performance

Method of Modeling the Trade-off

Modeling the Trade-off of Privacy Preservation and Activity Recognition on Low-Resolution Images

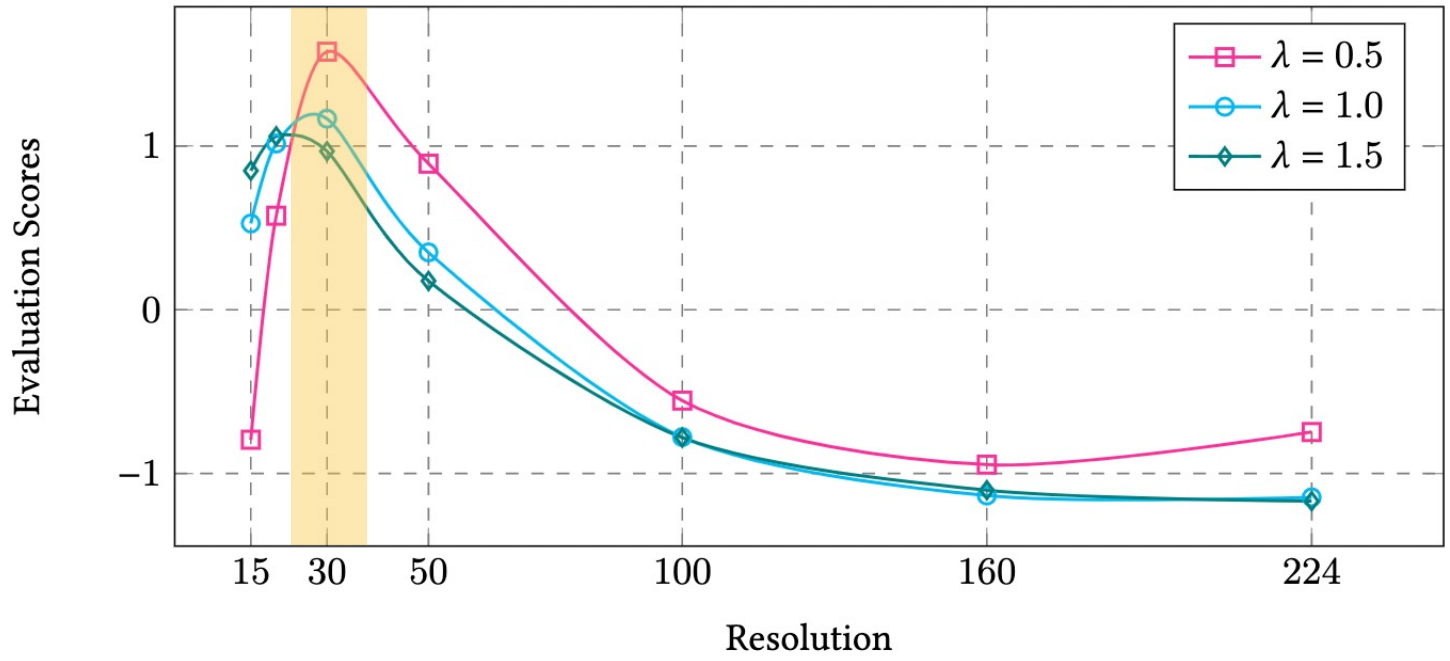
Results Analysis

$$S(r) = L_T\left(f_T\left(f_r(X)\right), g_T(X)\right) - \lambda \sum_{i=1}^{n} \omega_i L_P^i \left(f_{Pi}\left(f_r(X)\right), g_{Pi}(X)\right)$$

Importance Weights ω: Obtained in Study 1.

Evaluation Function L_T and L_P: Obtained in Study 2 and Study 3.

Results Analysis



Depicting the Objective Function $S(r)$

Applying the Model





Fine-tune the main components according to deployment environment and user experience.

Modeling the Trade-off between Privacy Preservation and Activity Recognition on Low-Resolution Images

Thanks for Watching!