Paper ID **5401**

Learning Privacy-preserving Optics For Human Pose Estimation

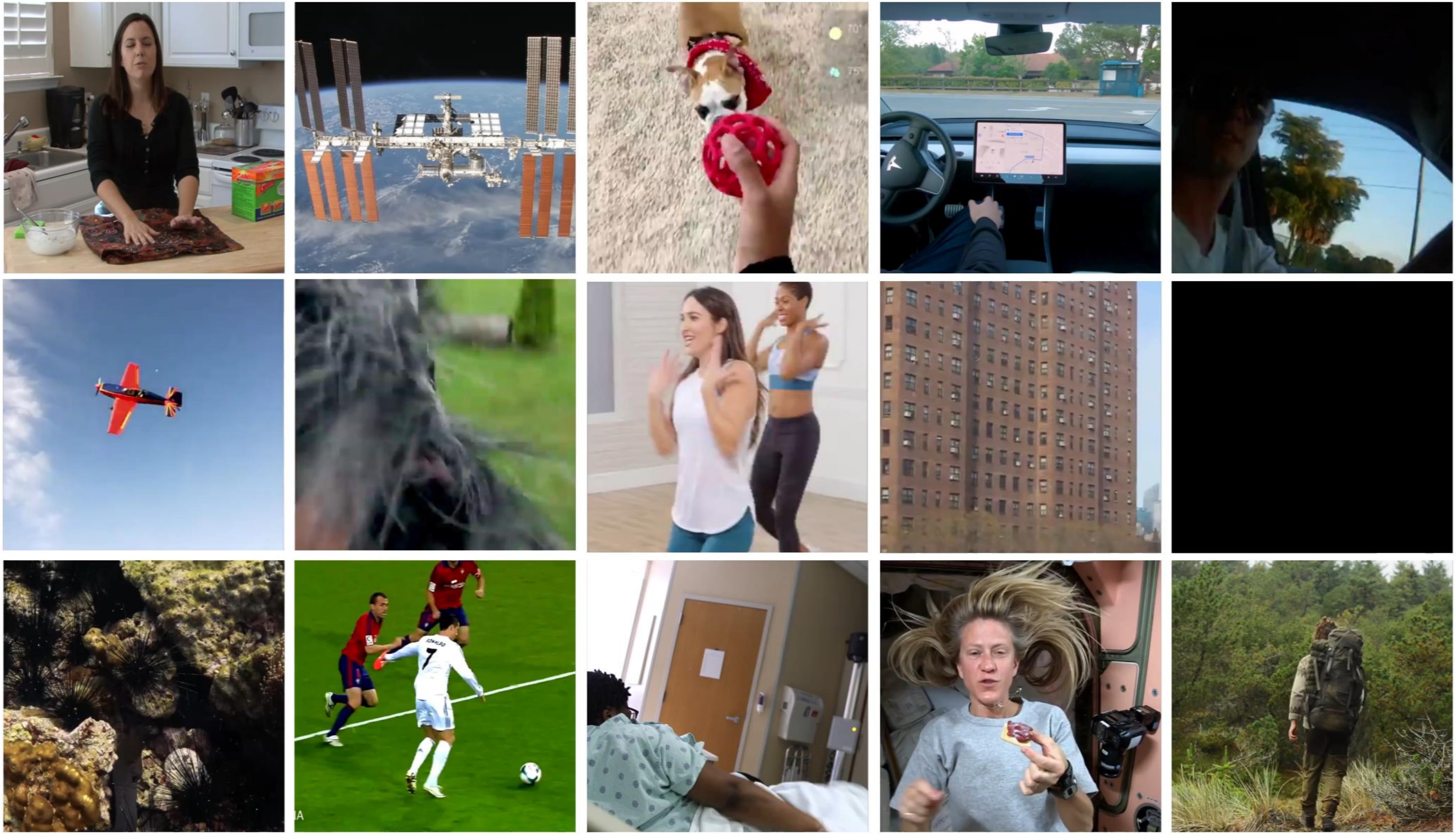
Carlos Hinojosa

Juan Carlos Niebles

Henry Arguello

Universidad Industrial de Santander

Stanford University

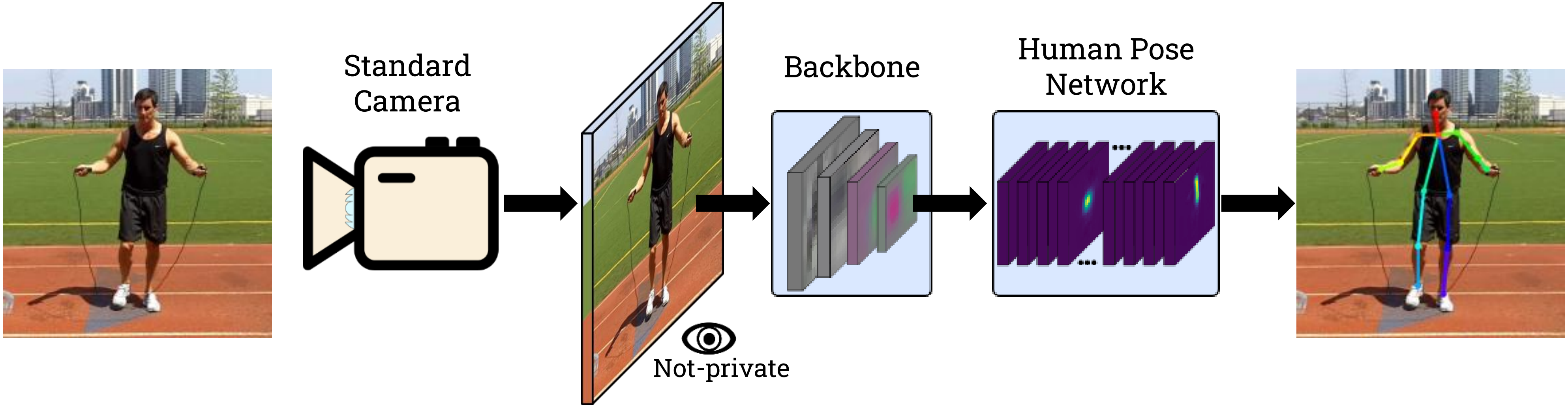

RONALDO
7

Not-private

Private

Let’s perform human pose estimation!

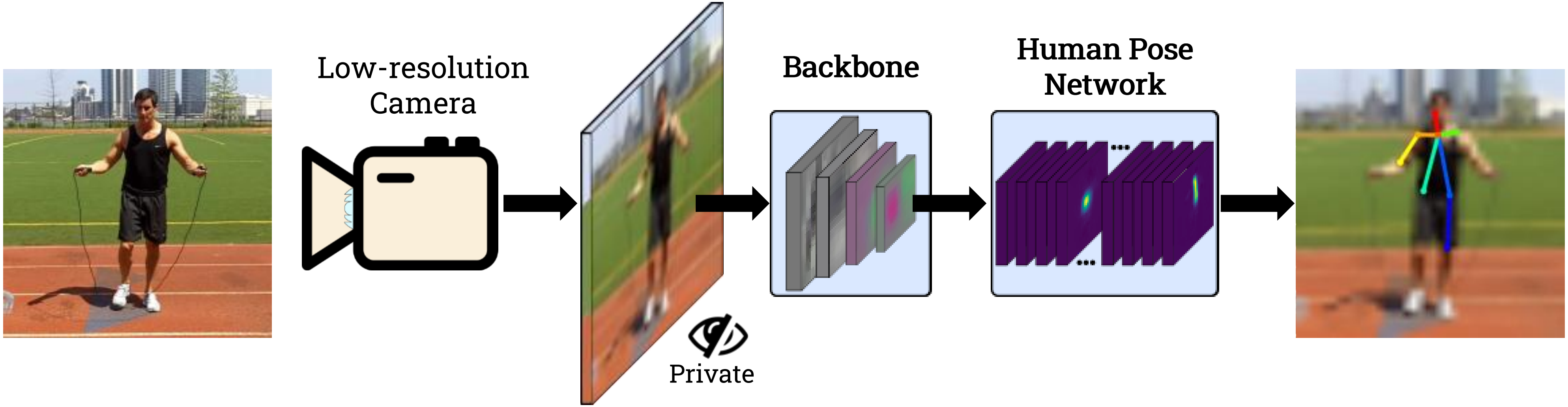
Prior work on privacy preserving vision



- Traditional Cameras
- Low-resolution
- De-focusing Cameras
- Depth Cameras

Instead of fixed/manually define the optics, we'll generate distortions considering both: camera's lens and HPE's outputs and their interaction.

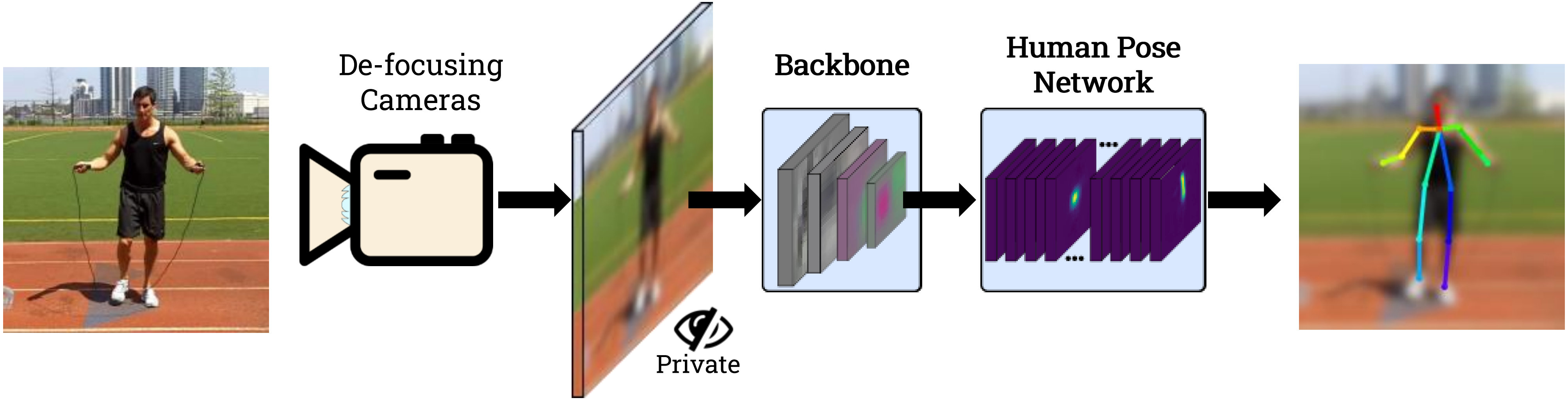
Prior work on privacy preserving vision



- Traditional Cameras
- Low-resolution
- De-focusing Cameras
- Depth Cameras

Instead of fixed/manually define the optics, we'll generate distortions considering both: camera's lens and HPE's outputs and their interaction.

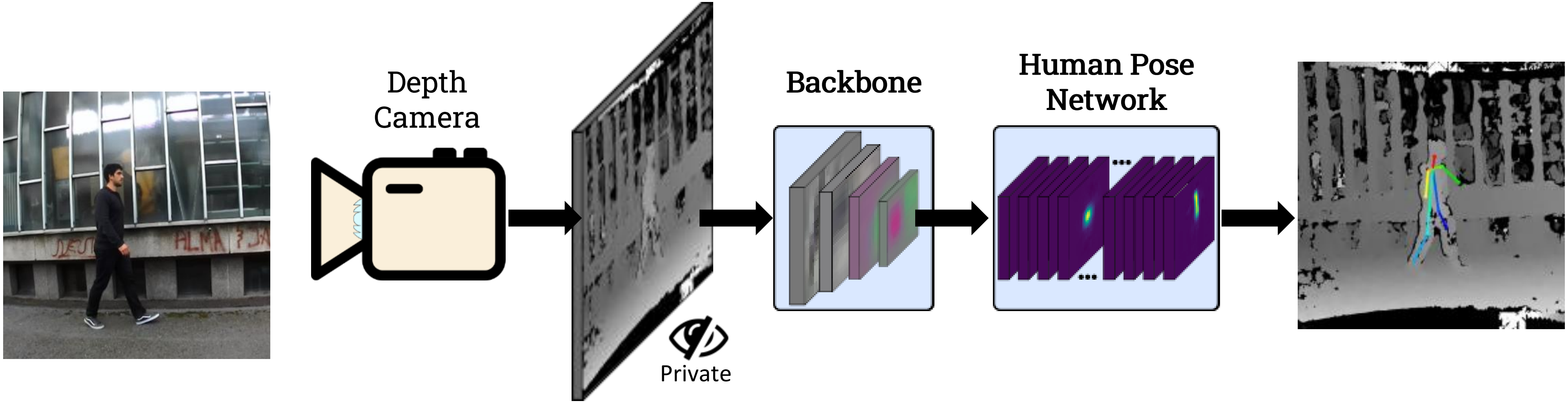
Prior work on privacy preserving vision



- Traditional Cameras
- Low-resolution
- De-focusing Cameras
- Depth Cameras

Instead of fixed/manually define the optics, we'll generate distortions considering both: camera's lens and HPE's outputs and their interaction.

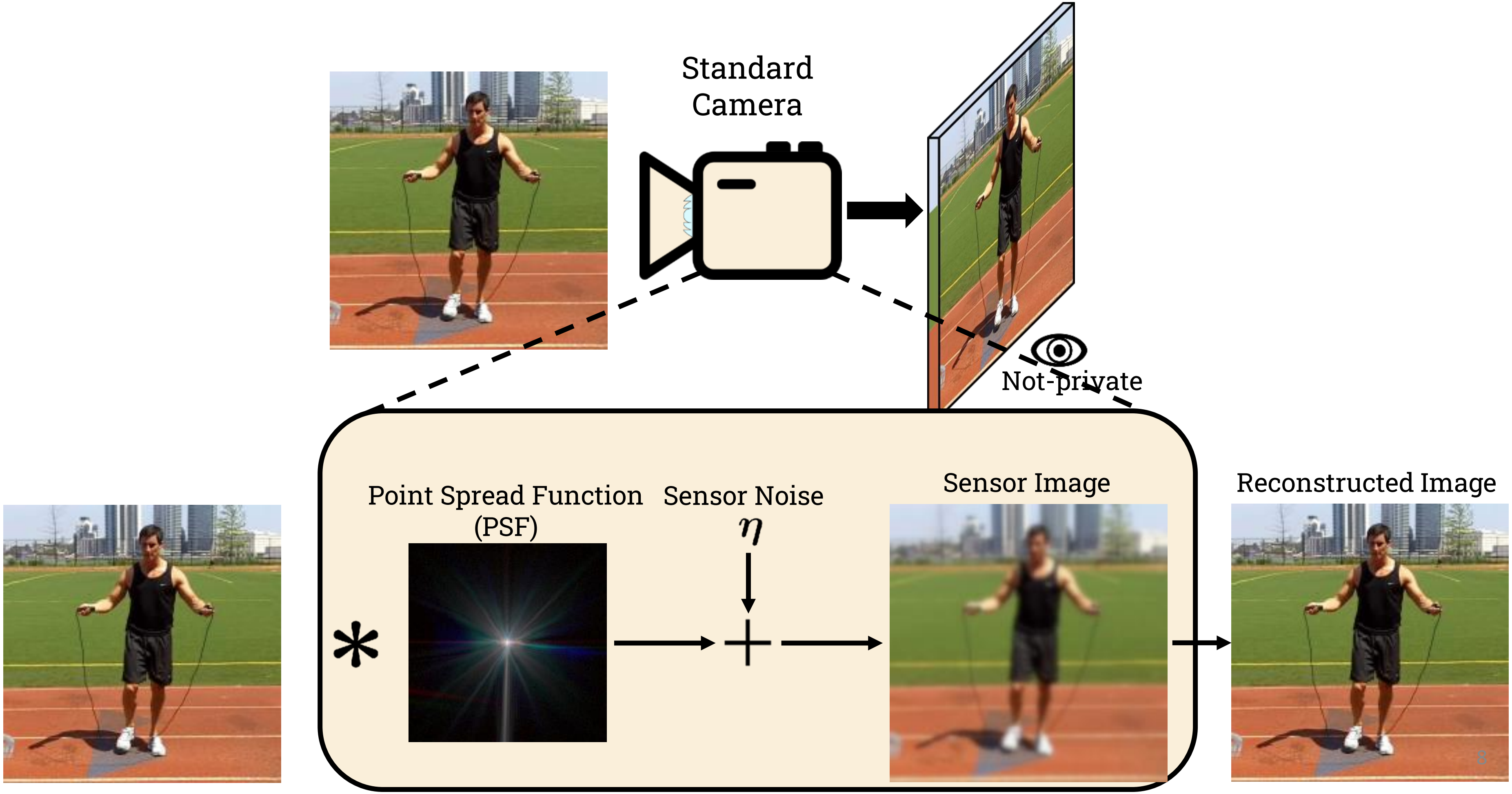
Prior work on privacy preserving vision



- Traditional Cameras
- Low-resolution
- De-focusing Cameras
- Depth Cameras

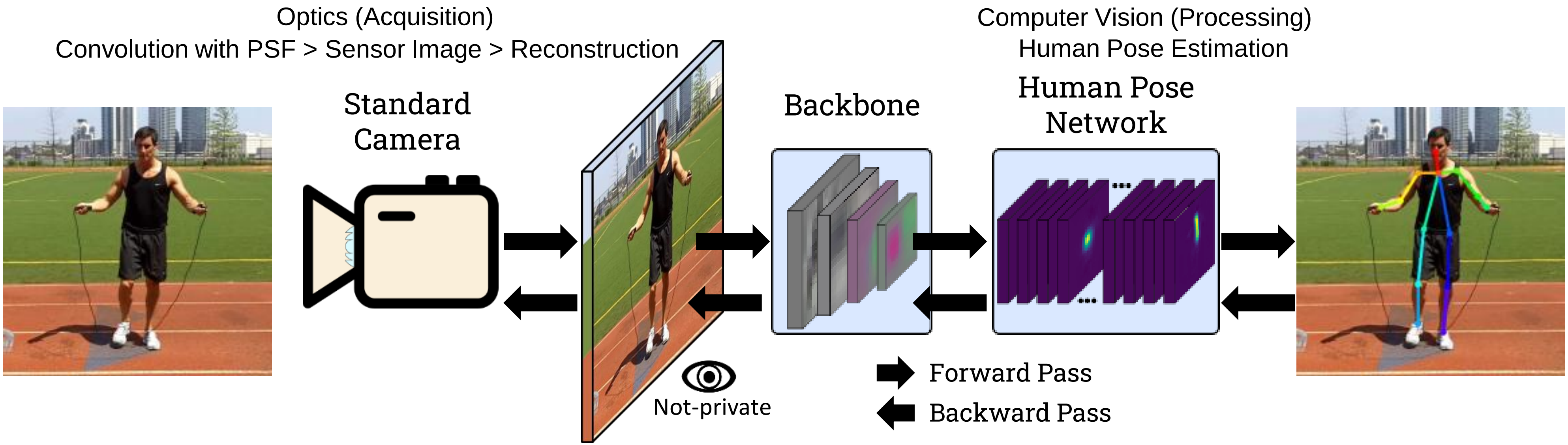
Instead of fixed/manually define the optics, we'll generate distortions considering both: camera's lens and HPE's outputs and their interaction.

Computational Cameras



Non-privacy-preserving Human Pose Estimation

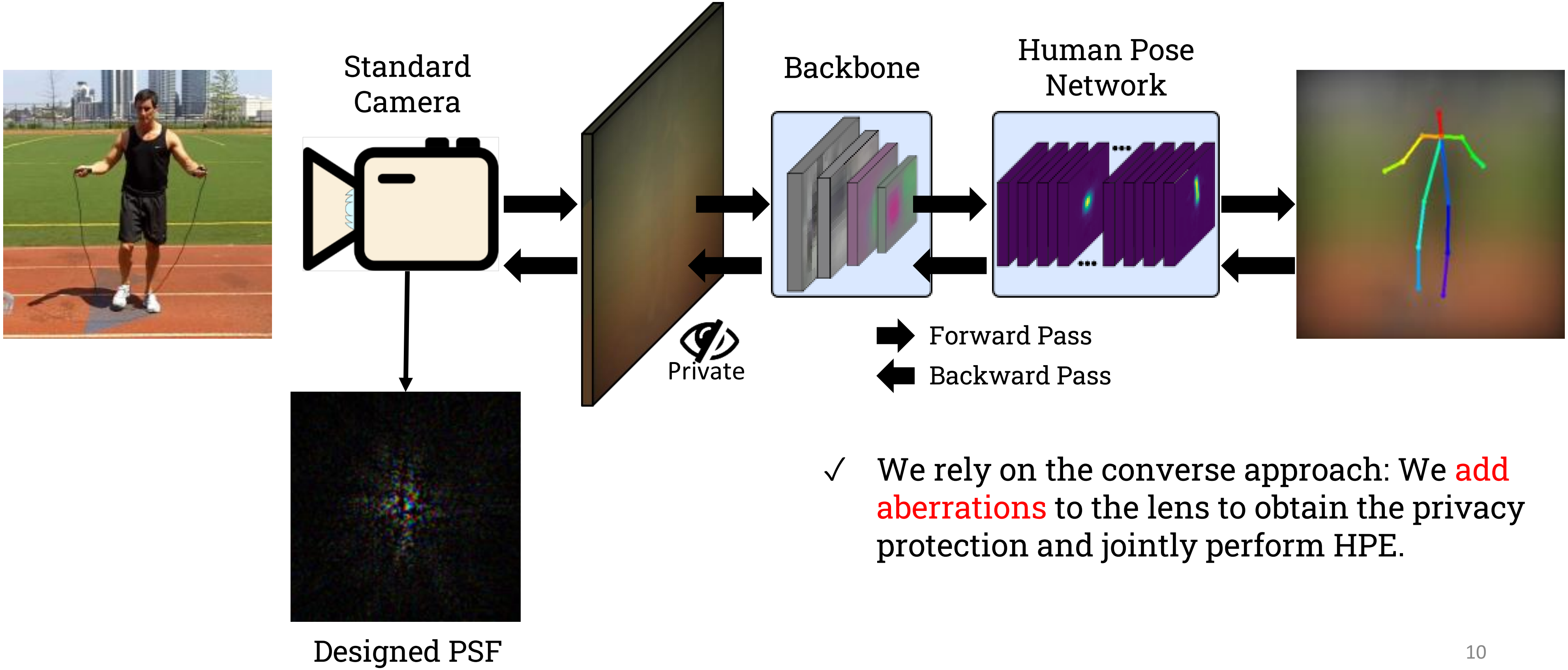
Each part of the pipeline is optimized separately.



- **Deep Optics:** the joint design of optics and algorithms to boost performance of the final task [1].
- All Deep Optics methods rely on the same approach: to **remove** the aberrations from the lens to obtain high-quality reconstructed images.

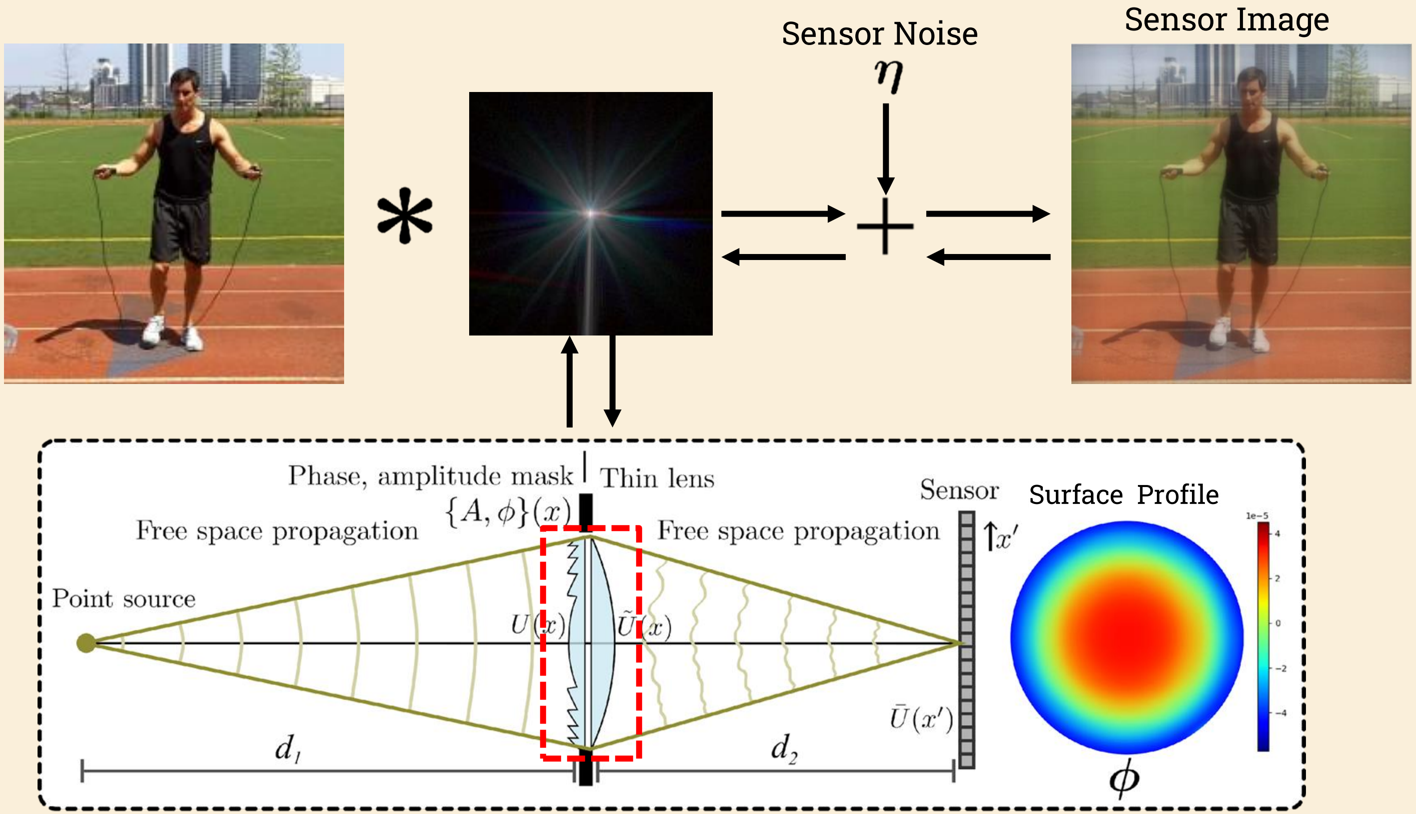
[1] V. Sitzmann, S. Diamond, Y. Peng, X. Dun, S. Boyd, W. Heidrich, F. Heide, and G. Wetzstein. "End-to-end optimization of optics and image processing for achromatic extended depth of field and superresolution imaging. ACM Transactions on Graphics.

Our privacy-preserving Human Pose Estimation Approach



✓ We rely on the converse approach: We add aberrations to the lens to obtain the privacy protection and jointly perform HPE.

Our privacy-preserving Human Pose Estimation Approach

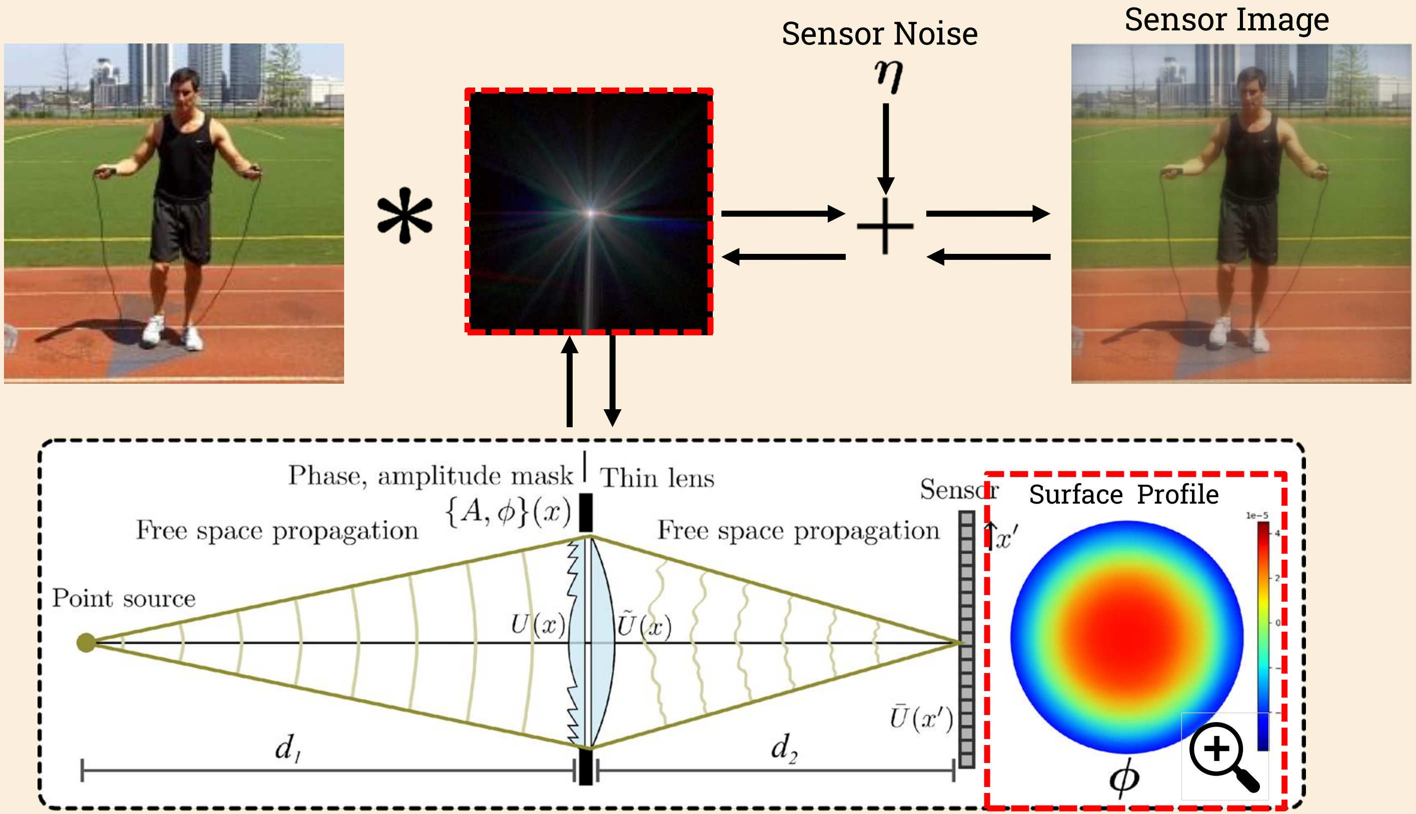


Our optical system consists of a convex thin lens and a refractive optical element (freeform lens) add-on.

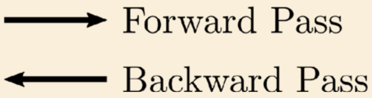
→ Forward Pass

← Backward Pass

Our privacy-preserving Human Pose Estimation Approach



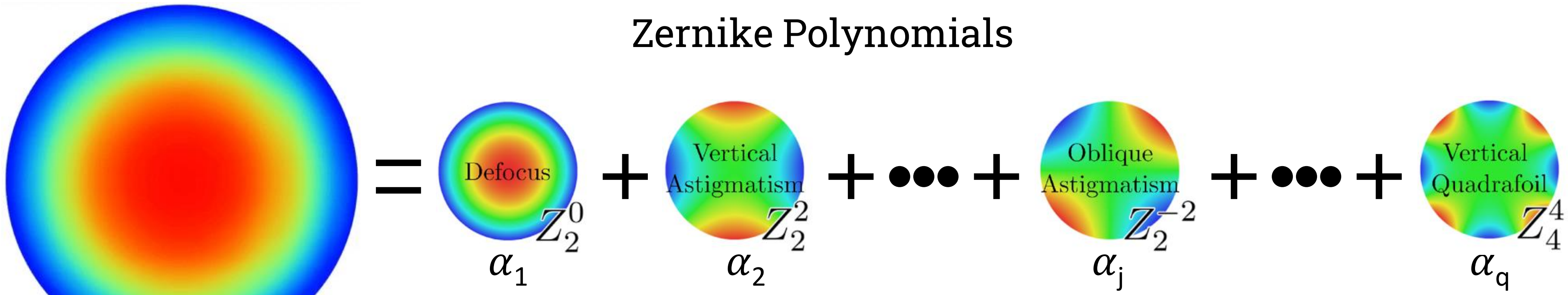
The PSF can be manipulated by modifying the **surface profile** of the freeform lens.



Our privacy-preserving Human Pose Estimation Approach

Surface Profile

Zernike Polynomials



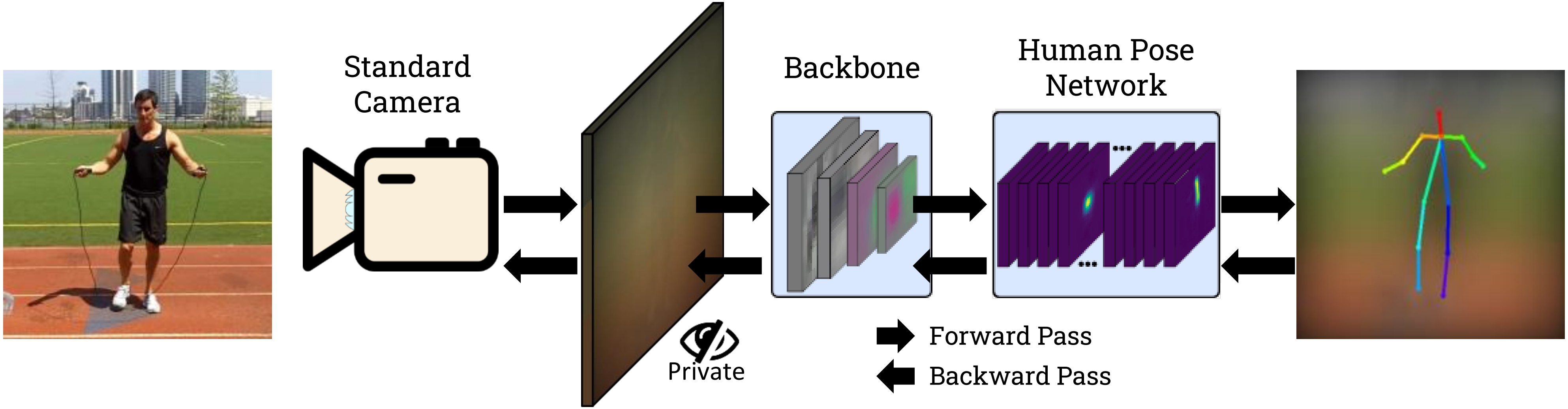
ϕ

$$\phi = \sum_{j=1}^{q} \alpha_j \mathbf{Z}_j \,,$$

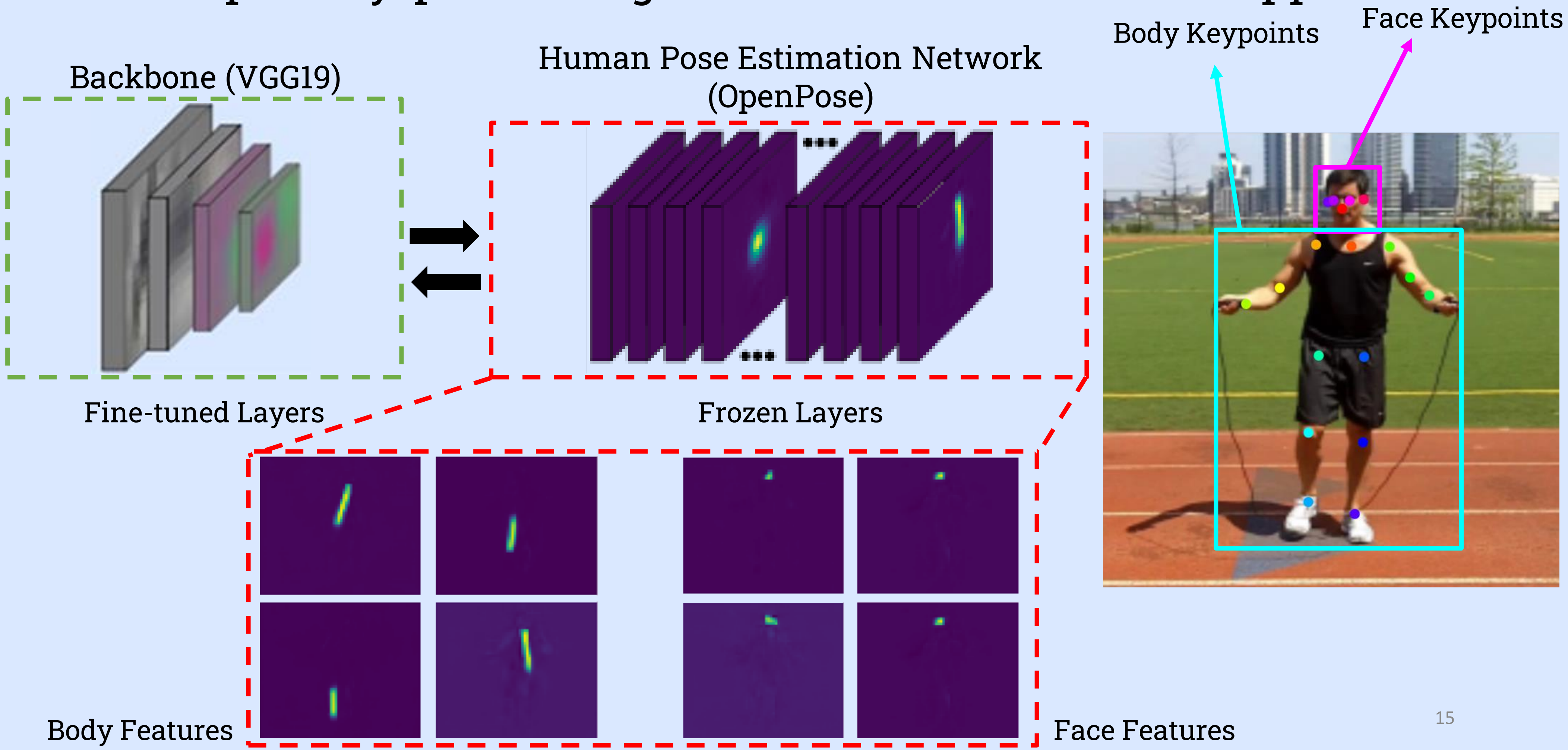
* We learn α_j

We optimize the PSF by learning to add optical aberrations to the system.

Our privacy-preserving Human Pose Estimation Approach



Our privacy-preserving Human Pose Estimation Approach



Our Learning Approach

Our optimization problem combines two goals: to visually distort the image while still performing HPE with high accuracy.

Lens parameters (Zernike Polynomials)

HPE Parameters

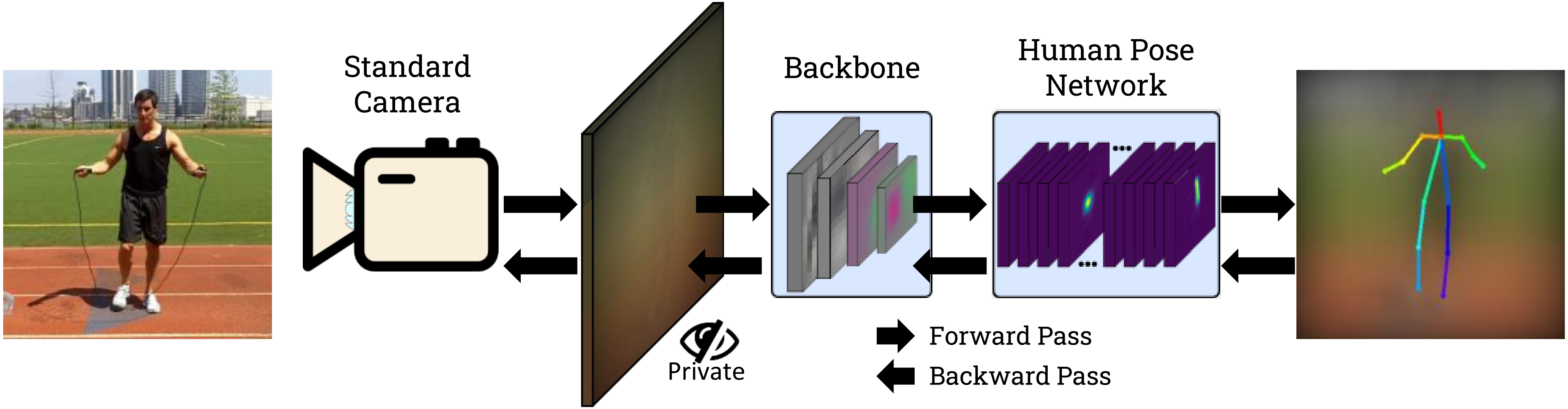
$$\boxed{\alpha^*}, \boxed{h^*} = \arg\min_{\alpha,h} \boxed{L_T(h)} + \boxed{L_P(\alpha)}$$

HPE Loss

Our proposed privacy preserving Loss

Visualization of the Optimization

Our privacy-preserving Human Pose Estimation Approach



Dataset and Metrics

- Human Pose Estimation

COCO 2017 Dataset

Metric: Object Keypoint Similarity (OKS)

- Face Recognition

ArcFace trained on MS-Celeb-1M

Metric: area under curve (AUC) of the ROC curve

- Image Quality

Original

PSNR: 15.21
SSIM: 0.58

Metric: Peak signal-to-noise ratio (PSNR) and Structural Similarity Index (SSIM).

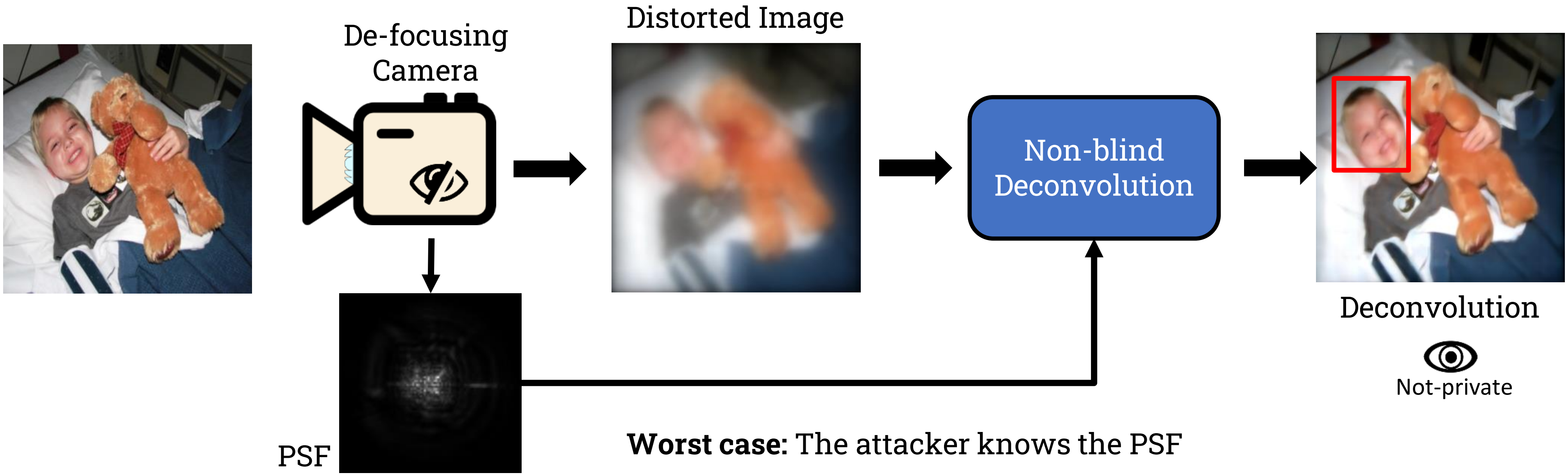
Quantitative Results

Method	PSNR	SSIM	AP	AP^{50}	AP^{75}	AP^{M}	AP^{L}	AR
OPPS	-	-	0.421	0.655	0.439	0.444	0.428	0.506
Defocus Lens	16.614	0.598	0.197	0.432	0.155	0.126	0.299	0.256
Low-Resolution	18.54	0.476	0.067	0.197	0.032	0.031	0.123	0.106
PP-OPPS (Ours)	**14.851**	**0.567**	**0.302**	**0.555**	**0.266**	**0.276**	**0.359**	**0.363**

Lower image quality

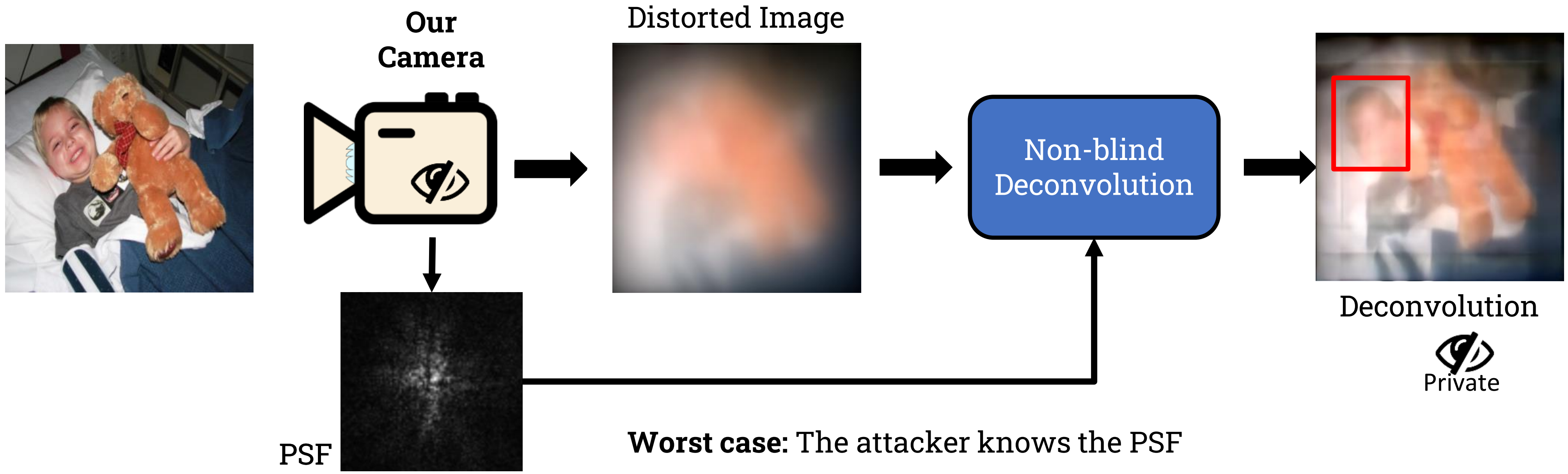
Good HPE accuracy

Deconvolution Attack Robustness



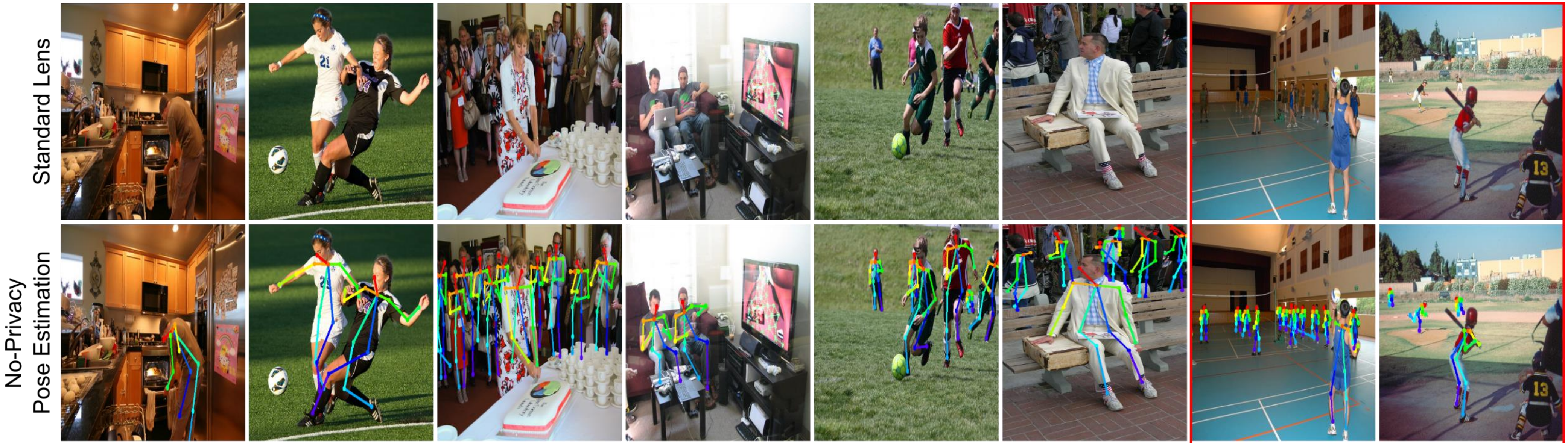
Worst case: The attacker knows the PSF

Deconvolution Attack Robustness



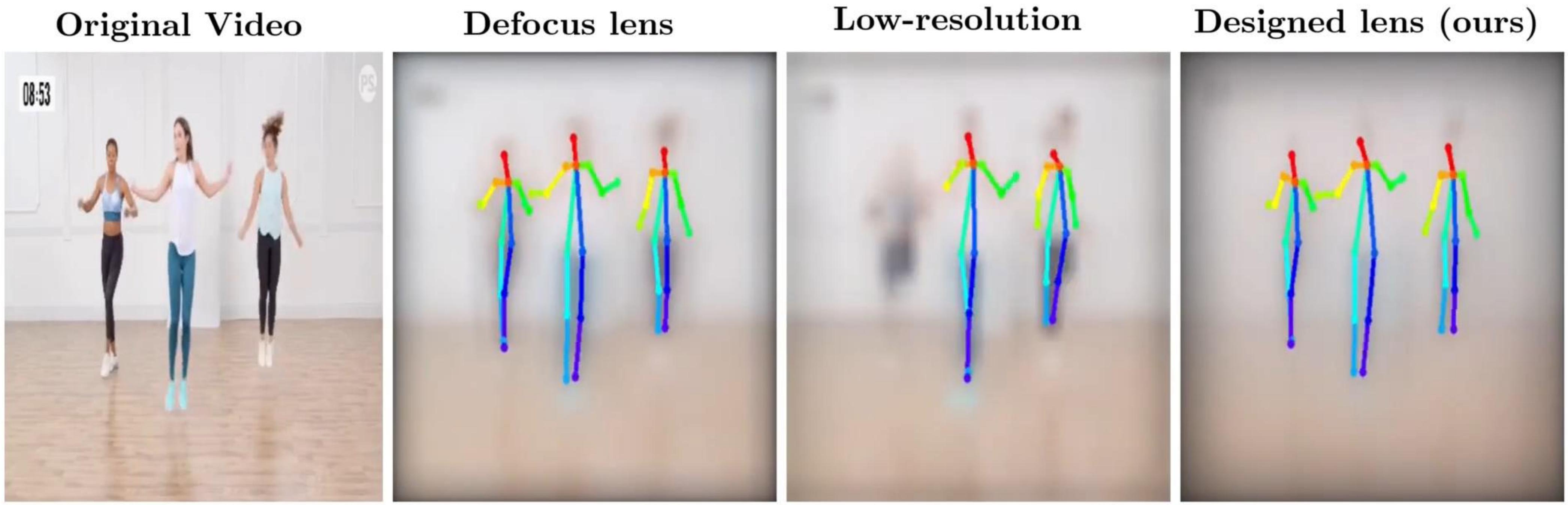
Worst case: The attacker knows the PSF

Qualitative Results



Qualitative Results

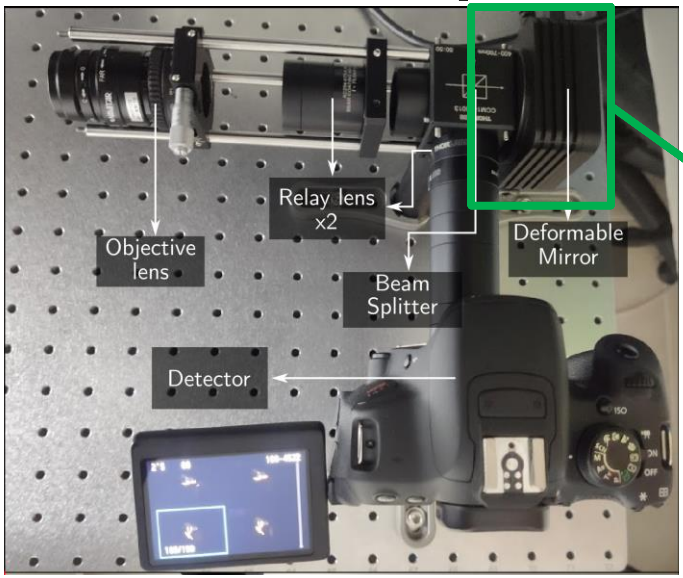
Qualitative Results

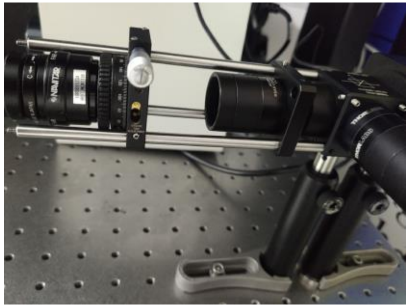


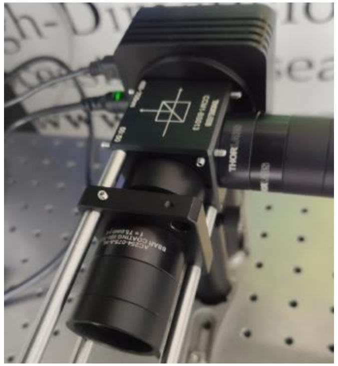
Source: https://youtu.be/Rj2IubFfEqY?t=360

Lab Experiments

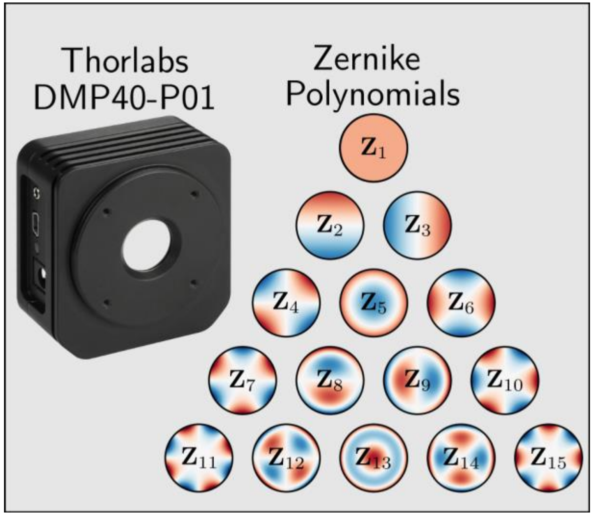
Hardware Setup



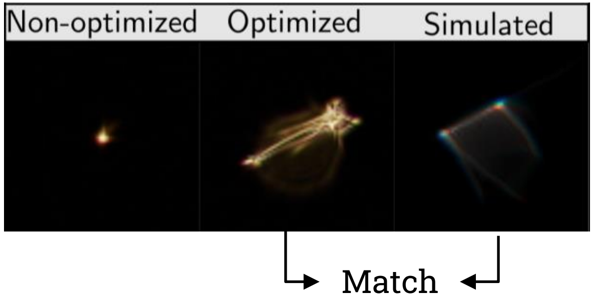




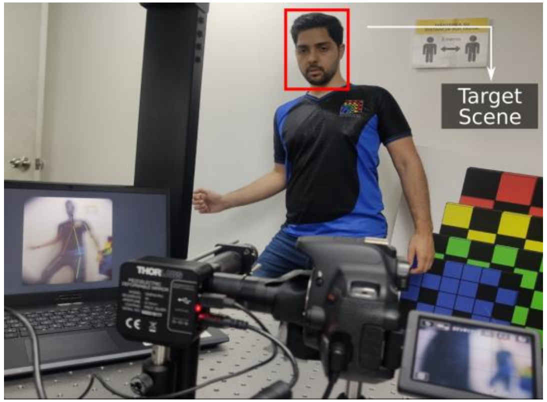
Deformable Mirror

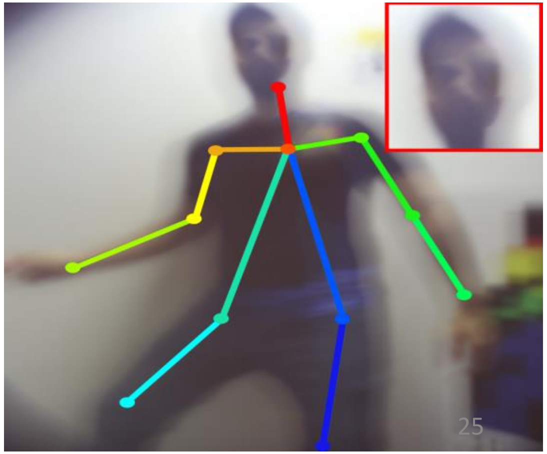


Acquired PSFs



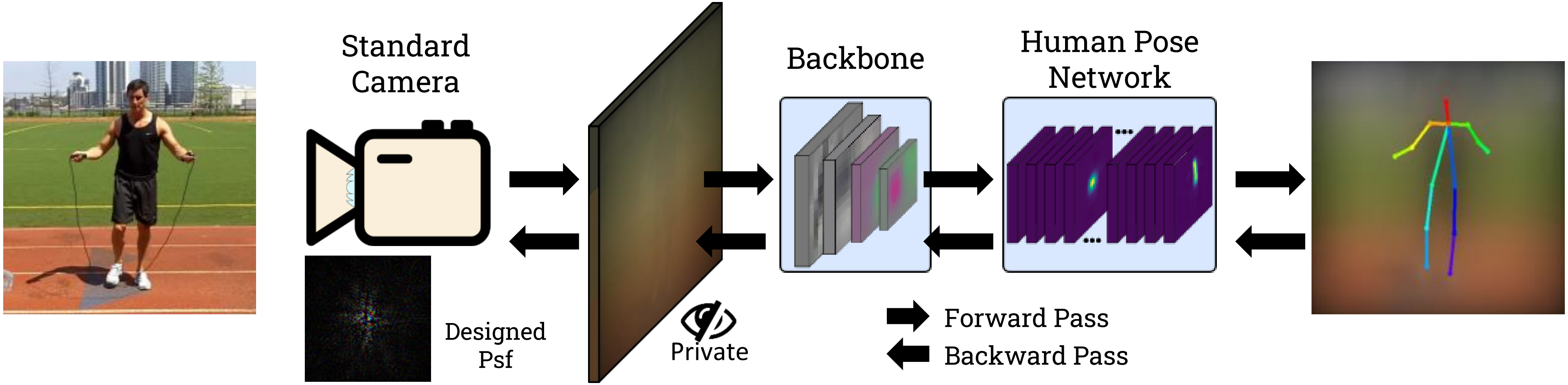
Experimental Results





Conclusions

I. We introduced a privacy-preserving end-to-end optimization framework.



II. We design our lens by adding aberrations using Zernike Polynomials.

III. We built a proof-of-concept optical system.

Universidad Industrial de Santander

2021 ICCV OCTOBER 11-17 VIRTUAL

Stanford University

Thank You!

SCAN ME

Project Page

carloshinojosa.me/project/privacy-hpe/