Learning Privacy-preserving Optics For Human Pose Estimation
Carlos Hinojosa 1, Juan Carlos Niebles2, Henry Arguello1
1Universidad Industrial de Santander 2Stanford University
carlos.hinojosa@saber.uis.edu.co

Motivation
Cameras are everywhere! How to develop privacy-preserving vision systems?

We want to prevent the camera from obtaining detailed visual data that may contain private information, desirably at the hardware level.

Prior work on Privacy-preserving vision

Low-resolution • Lose information. • Pose estimation fails.

De-focusing • Susceptible to reverse engineering attacks.

Depth cameras • Bright sunlight degrades depth estimation quality.

Our key idea: instead of fixed/manually define optics, we'll design optical distortion in a way that doesn't degrade the vision algorithm performance.

Traditional Deep-optics-based Computational Cameras

• All Deep Optics methods rely on the same approach: to remove the aberrations from the lens to obtain high-quality reconstructed images.

The concept of Deep Optics refers to the joint design of optics and algorithms to boost the performance of the final task.

Model and Approach

We rely on the converse approach of deep optics: we add aberrations to the lens to obtain privacy protection and jointly perform HPE.

Our optimization process has two parts: an optical encoder, which provides hardware-level privacy protection by degrading the image quality, and a CNN decoder that learns features from the highly degraded images to perform HPE.

Datasets and Metrics

Dataset
We train our proposed end-to-end approach on the COCO 2017 keypoints dataset and evaluate our approach on the val2017 set.

We compare our method against two traditional privacy-preserving approaches: Defocus and Low-resolution cameras. OPPS stands for the original OpenPose network. The PP prefix stands for our proposed approach.

Qualitative Results on Example COCO Images

Experiments: Ablation Studies

Datasets and Metrics

Dataset
We train our proposed end-to-end approach on the COCO 2017 keypoints dataset and evaluate our approach on the val2017 set.

Metrics
We use the standard COCO evaluation metric: Object Keypoint Similarity (OKS). To make a fair comparison, we slightly modify the COCO evaluation script to not consider the face keypoints.

HPE Face Recognition Image Quality
We implement the ArcFace network to measure privacy. We train ArcFace on three face recognition datasets. We measure its performance in terms of the area under ROC curves (AUC) of the ROC.

We use the peak-signal-to-noise ratio (PSNR) and the structural similarity index measure (SSIM) to measure image degradation, we expect to achieve lower PSNR and SSIM values.

Quantitative Experiments: Comparison with Prior Works

Method PSNR SSIM AP AR OPPS (upper Bound) - - 0.421 0.506
Defocus Lens 16.614 0.598 0.197 0.256
Low-Resolution 18.54 0.476 0.067 0.106
PP-OPPS (Ours) 14.851 0.567 0.302 0.363

Caracteristicas

- Cálculo
- Información
- Comunicación
- Desarrollo
- Innovación
- Tecnología
- Sostenibilidad
- Competitividad
- Calidad
- Innovación
- Tecnología
- Sostenibilidad
- Competitividad
- Calidad