A Study of Face Obfuscation in ImageNet

Kaiyu Yang¹, Jacqueline Yau², Li Fei-Fei¹, Jia Deng¹, and Olga Russakovsky¹

1. Department of Computer Science, Princeton University
2. Department of Computer Science, Stanford University

Privacy Issues with Visual Datasets

How to protect the privacy of incidental people in images?

- **Problem**
  1. The ImageNet Challenge has only 3 people-centric categories (scuba diver, bridegroom, baseball player) among its 1000 categories. But people show up incidentally in the images.
  2. Similar issues for other visual datasets such as Open Images, Places, and COCO.
  3. People’s privacy is at risk since these datasets are freely available and widely used.

- **Private information in images**
  1. Faces, addresses, credit cards, etc.
  2. We focus on faces.

- **Contributions**
  1. Annotate faces in ImageNet, facilitating subsequent research on privacy protection.
  2. Empirically demonstrate that face obfuscation does not hurt large-scale visual recognition.

Faces in ImageNet

1. Annotated face bounding boxes on 1,431,093 images.
2. 243,198 images have at least one face (17%).
3. 562,626 faces in total.
4. 106 categories have more than half images with faces.

Face Obfuscation

- **Problem**
  1. Simple, widely used in practice.
  2. Without any formal guarantee of privacy.

Effects on Image Classification

- **Experiment setup**
  3. Train and evaluate on original/blurred/overlaid images.

- **Results**
  1. Overall top-1 accuracy: original > blurred > overlaid.
  2. Marginal accuracy drop (<1% on average).

![Accuracy Comparison](image)

Effects on Transfer Learning

- **Object recognition on CIFAR-10**

- **Scene recognition on SUN**

- **Object detection on PASCAL-VOC**

- **Face attribute classification on Celeb-A**

Effects on Transfer Learning

- **Conclusion**: Face obfuscation does not hurt feature transferability to downstream tasks.