Does a Face Mask Protect my Privacy?: Deep Learning to Predict Protected Attributes from Masked Face Images

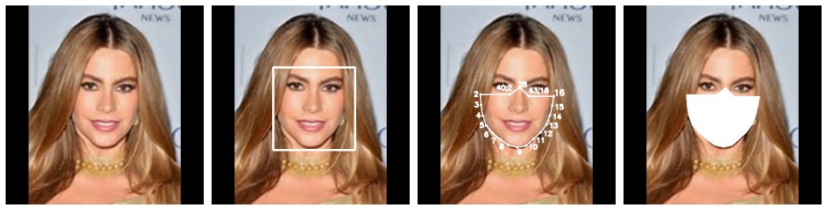
Sachith Seneviratne, Nuran Kasthuriarachchi, Sanka Rasnayaka, Danula Hettiachchi, Ridwan Shariffdeen

Abstract

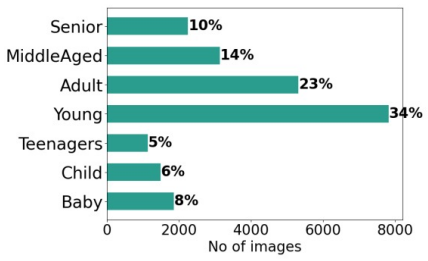
Contactless and efficient systems are implemented rapidly to advocate preventive methods in the fight against the COVID-19 pandemic. Despite the positive benefits of such systems, there is potential for exploitation by invading user privacy. We analyze the privacy invasiveness of face biometric systems by predicting privacy sensitive soft-biometrics using masked face images.

Data

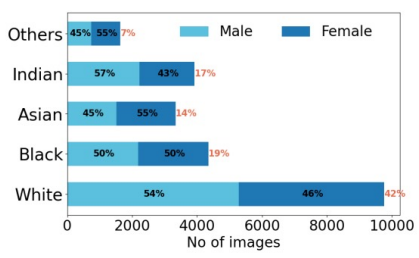
A synthetic mask generation process was implemented and used with the UTK faces dataset to create masked face dataset



(a) Original (b) Localization (c) Key points (d) Digital mask



(a) **Age distribution**



(b) **Race and gender distribution**

Methodology

A self-supervised representation learning step was used to initialize a masked facial representation, and then further specialized for protected attribute prediction.

This allows efficient construction of 4 downstream tasks (3 classification, 1 regression) across 2 different data splits.

Reproducible models, scripts and data can be found at: https://github.com/sachith500/MaskedFaceRepresentation

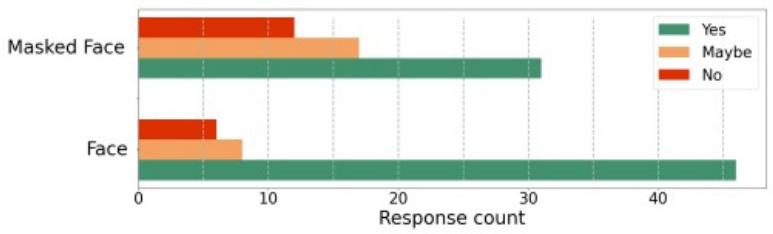
Privacy Vulnerability

The Privacy Vulnerability Index is used to quantify the privacy invasiveness of a biometric modality. This depends on

- Predictability of private attributes
- Importance of each attribute

Perceived privacy protection

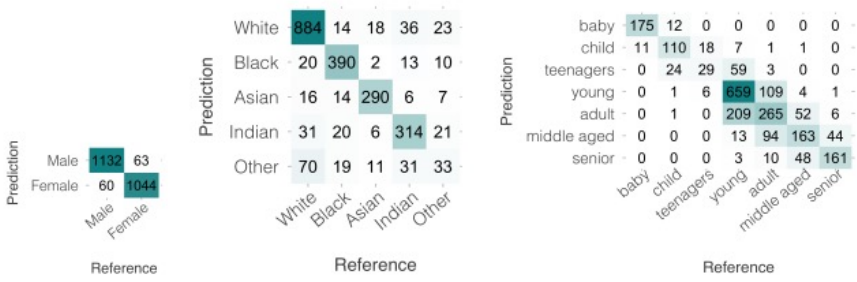
Our survey shows that the perceived privacy of wearing a mask is higher with statistical significance ($P = 0.00964 < 0.05$).



Results

Our models were able to predict sex, race and age to a level comparable to SOTA for unmasked face images

	Unmasked Face - SOTA	Masked Face (Random Split)	Masked Face (Uniform Split)
Sex	[13] **98.23%**	94.01%	**94.65%**
Race	[1] **91.23%**	82.20%	**83.12%**
Age (MAE) - Regression	[26] **5.44**	**6.21**	-
Age - Classification	[13] **70.1%**	-	**67.94%**



(a) **Sex** (b) **Race** (c) **Age**

As quantified by our analysis, the reduction in privacy invasiveness by wearing a mask is only 2.9%. This is very low compared to the 50% of people who thought that wearing a mask would be more private.