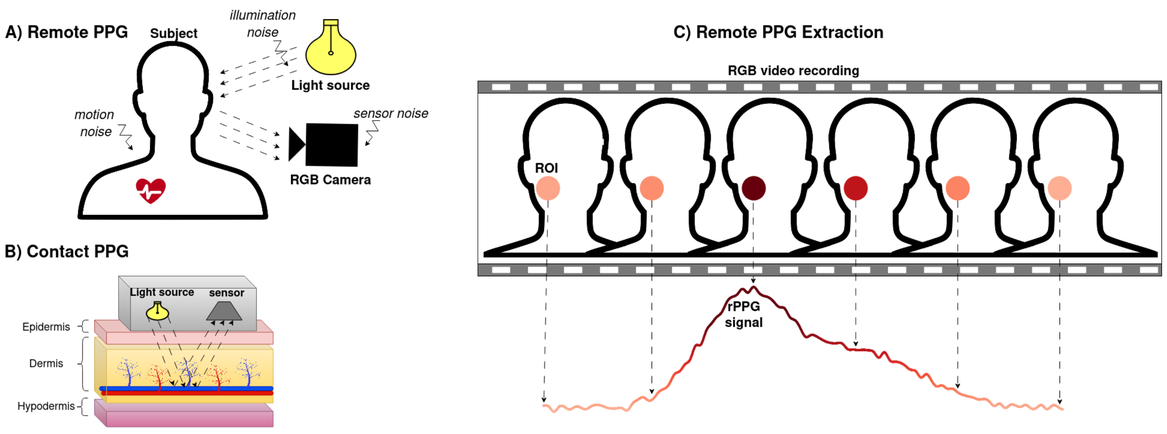
De-identification of facial videos while preserving remote physiological utility

Marko Savic and Guoying Zhao
Center for Machine Vision and Signal Analysis (CMVS)
University of Oulu, Finland

What is Remote Photoplethysmography (rPPG) ?

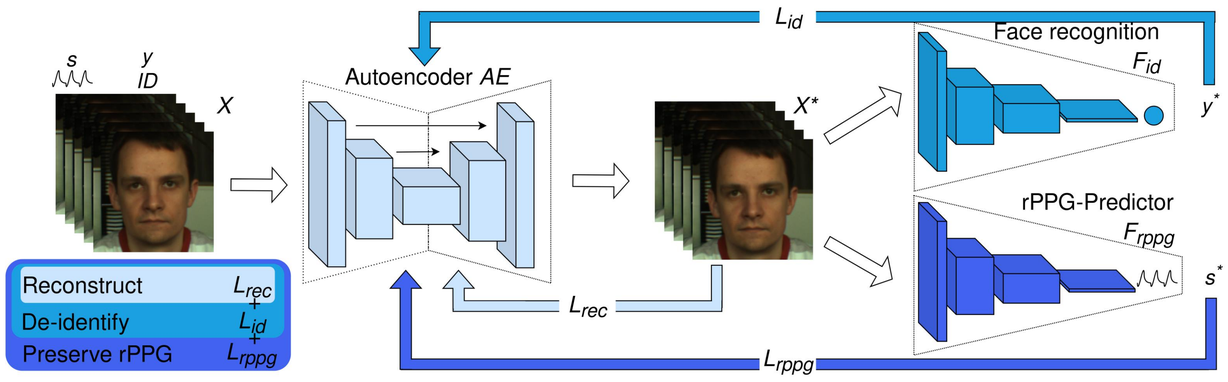
- Convenient non-contact method for cardiac signal estimation
- rPPG signals are extracted from facial videos recorded with RGB cameras
- Derived from subtle periodical variations in facial colour (sensitive to noise)



Potential Privacy issues

- Data contains both sensitive physiological signals and facial videos, which are biometric data subject to special restrictions (GDPR, EU AI Act)
- Big data and Machine Learning allow to extract sensitive data like Identity, Race, Gender, etc. → high risk of intentional or unintentional unethical practices
- De-identification from machines is crucial for future applications

Our rPPG preserving De-identification method



- Retains data utility (underlying rPPG signals and visual appearance) while removing identity related features, rendering videos un-recognisable by machines
- Unobtrusive perturbations added to input by semi-adversarial training of Autoencoder
- Learning constraints imposed by pre-trained Face recogniser and rPPG predictor
- Trained with three objectives: Reconstruct, De-identify and Preserve rPPG.

1. Reconstruct

- Reconstructs input video with visually imperceptible perturbations

$$L_{rec}(X,X^*) = |X - X^*|_2 + \frac{1}{T}\sum_{t=1}^{T}\frac{1}{W}\sum_{i=1}^{W} SSIM(w_i x_t, w_i x_t^*)$$

2. De-identify

- Deceives the identity recognizer, resulting in wrong and non-confident identity predictions

$$L_{id}(X^*,F_{id},y) = \frac{1}{K}\sum_{x_k^* \in X_K^*} l_{id}(x_k^*,F_{id},y) \quad where \quad X_K^* = \{X^*(i)\}_{i=1}^{K}$$

$$l_{id}(x_k^*,F_{id},y) = \frac{1}{N}\sum_{i=1}^{N} y_i log(F_{id}(x_k^*)) + \lambda \frac{\|F_{id}(x_k^*) - [(1/N)_{\times N}]\|_2}{\|F_{id}(x_k^*)\|_2 + \|[(1/N)_{\times N}]\|_2}$$

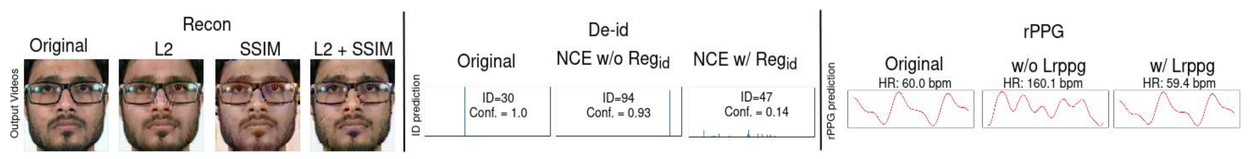
3. Preserve rPPG

- Ensure that the perturbations do not deteriorate the rPPG signal

$$L_{rppg} = \frac{\sum_i (s_i - \bar{s})(s_i^* - \bar{s}_i^*)}{\sqrt{\sum_i (s_i - \bar{s})^2 (s_i^* - \bar{s}_i^*)^2}} \quad i \in [0, T[$$

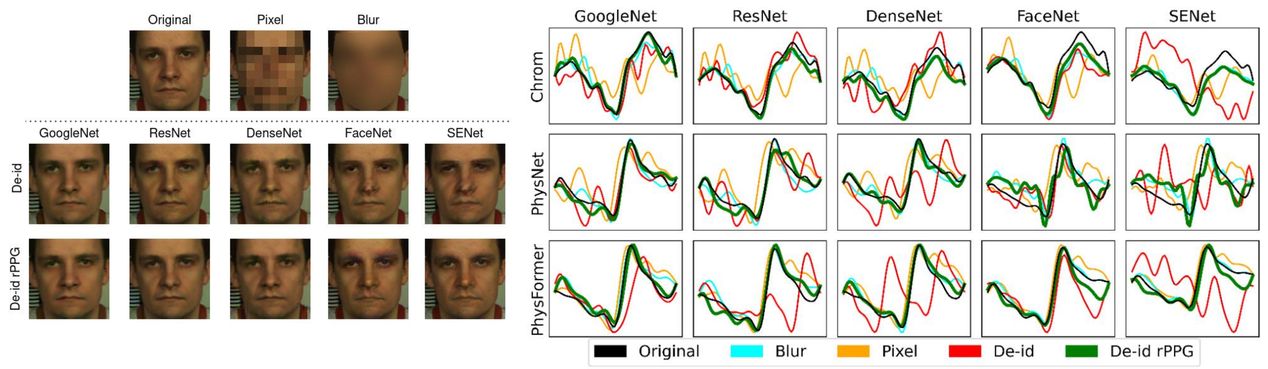
Total loss function

$$L = \alpha L_{rec} + \beta L_{id} + \gamma L_{rppg}$$

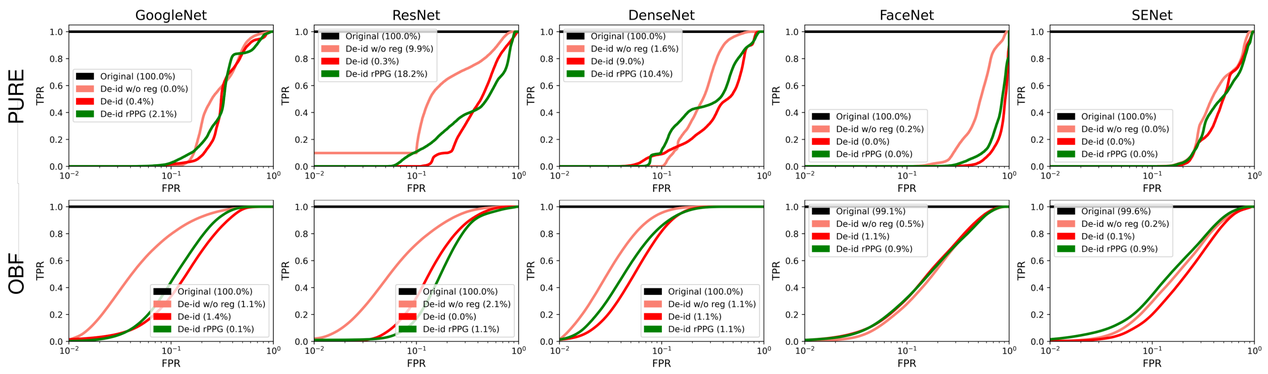


Results

- Visual acceptance PSNR>30dB and SSIM approx. 0.97
- Signals and heart rates extracted of high quality (R = 0.99, RMSE < 1)



- De-identification is successful, with accuracy below random guessing and high EER



Results

- First learning based method for facial video de-identification that preserves the physiological and visual fidelity, while protecting user's privacy from machines
- Experiments on two public datasets show effectiveness of our method in deteriorating biometric performance, while preserving visual information and rPPG signal.
- Future work will include more challenging biometric attack scenarios and removal of soft biometrics while preserving rPPG.

UNIVERSITY OF OULU

BMVC 2023