An Overview of Face De-identification in Still Images and Videos

Slobodan Ribaric[1], Nikola Pavesic[2]

[1] University of Zagreb, Faculty of Electrical Engineering and Computing (FER), Zagreb, Croatia

[2] University of Ljubljana, Faculty of Electrical Engineering, Ljubljana, Slovenia

COST ACTION
IC1206

De-identification
for privacy protection
in multimedia content.

De-identification for Privacy Protection in Multimedia, Ljubljana, Slovenia, 4th May 2015

Overview

1. Introduction
2. Face de-identification in still images
3. Face de-identification in videos
4. Face de-identification systems
5. Conclusion

1. Introduction

- Face-based identification is used in various application scenarios - from identification of a person based on still images in passport or identity card, to identification based on face images captured by a surveillance system without the cooperation of the person
- In many application scenarios, especially in video surveillance, privacy can be compromised
- Preservation of privacy: face de-identification

1. Introduction

- De-identification is the process of concealing or removing personal identifiers, or replacing them with surrogate personal identifiers in personal information, in order to prevent the disclosure and use of data for purposes unrelated to the purpose for which the information was originally obtained.
- Personal information is any information relating to a person
- Personal identifiable information (or personal identifier) is the personal information, which allow his or her identification

11th IEEE International Conference on Automatic Face and Gesture Recognition
FG2015

De-identification for Privacy Protection in Multimedia, Ljubljana, Slovenia, 4th May 2015

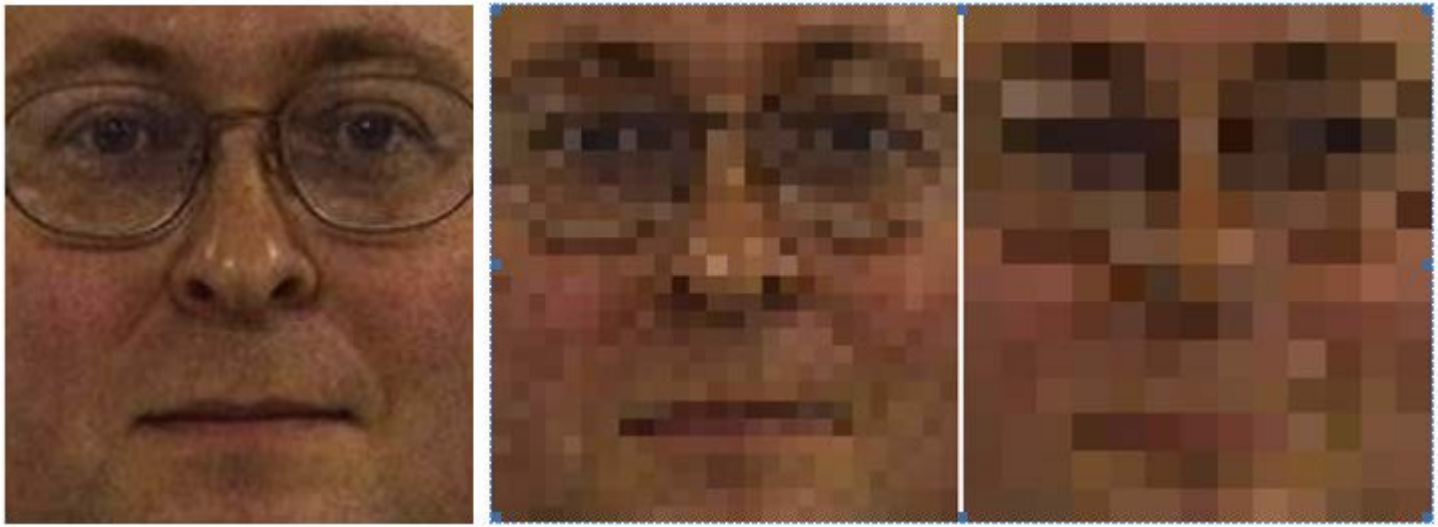
2. Face de-identification in still images

Early research on face de-identification was focused on face still images, and recommended the use of ad-hoc (naive) approaches such as "black box", “pixelation” and “blurring”:

- Face region is simply substituted by a black (or white) rectangle, elliptical, circular or T-form covers

2. Face de-identification in still images

- Pixelation: reducing the resolution (subsampling) of a face region



11th IEEE International Conference on Automatic Face and Gesture Recognition
FG2015

De-identification for Privacy Protection in Multimedia, Ljubljana, Slovenia, 4th May 2015

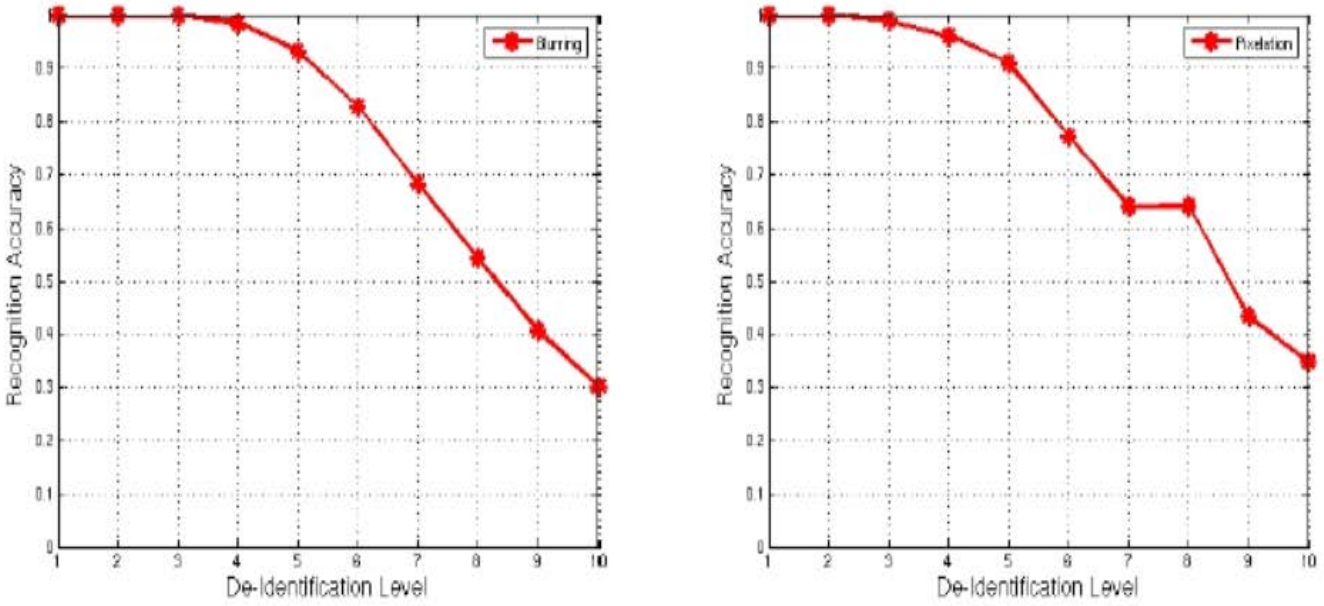
2. Face de-identification in still images

- Blurring: smoothing a face in an image with Gaussian filters using a variety of sufficiently large variances.

11th IEEE International Conference on Automatic Face and Gesture Recognition
FG2015

De-identification for Privacy Protection in Multimedia, Ljubljana, Slovenia, 4th May 2015

2. Face de-identification in still images



R. Gross, E. Airoldi, B. Mali,L. Sweeney, Integrating Utility into Face De-identification, PET 2005, LNCS 3856, pp. 227–242, 2006

11th IEEE International Conference on Automatic Face and Gesture Recognition
FG2015

De-identification for Privacy Protection in Multimedia, Ljubljana, Slovenia, 4th May 2015

2. Face de-identification in still images

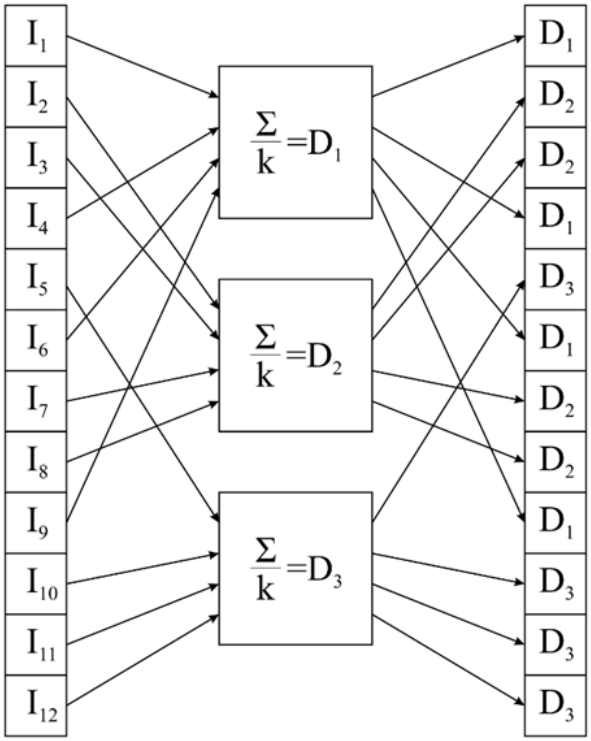
To improve the level of privacy protection, more sophisticated approaches have been proposed:

- Eigenvector-based de-identification: original face is substituted by a reconstructed face that is obtained by applying a smaller number of eigenfaces

- k-Same, k-Same-Select and Model-based k-Same algorithms for face de-identification

2. Face de-identification in still images

- k-Same algorithm (k = 4)



- A person-specific set of face images I
- A set of de-identified face images D
- ∑ - a sum of the k closest face images from a person-specific set of images I

2. Face de-identification in still images

- k-Same algorithm

- k-Same algorithm is irreversible, guarantees probable privacy (1/k), but very often results in "ghosting"

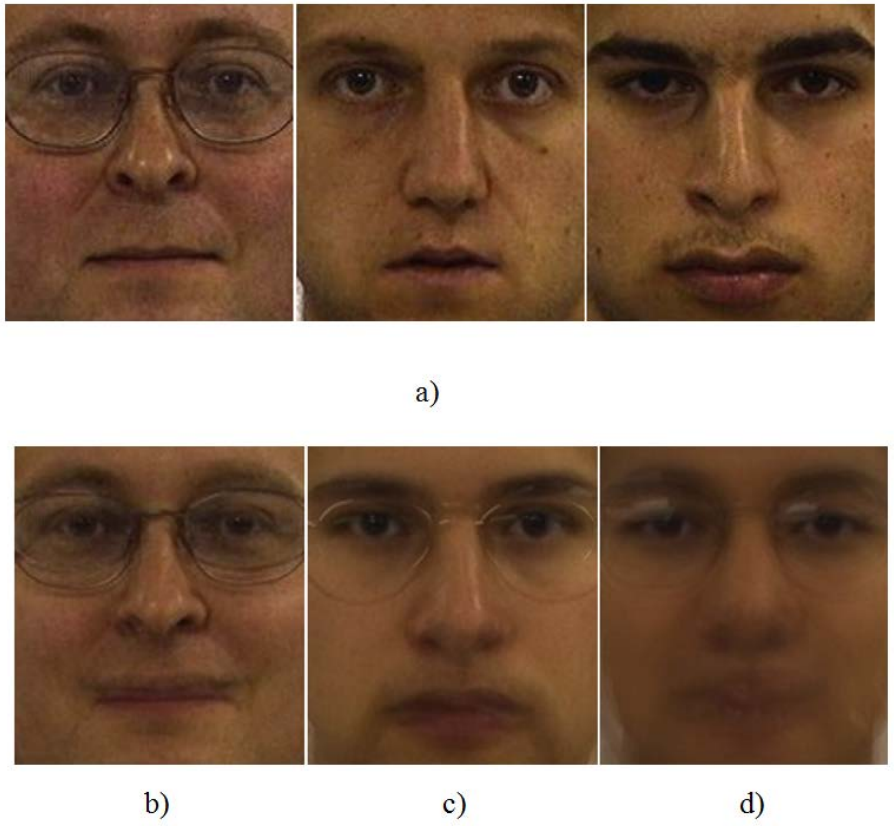
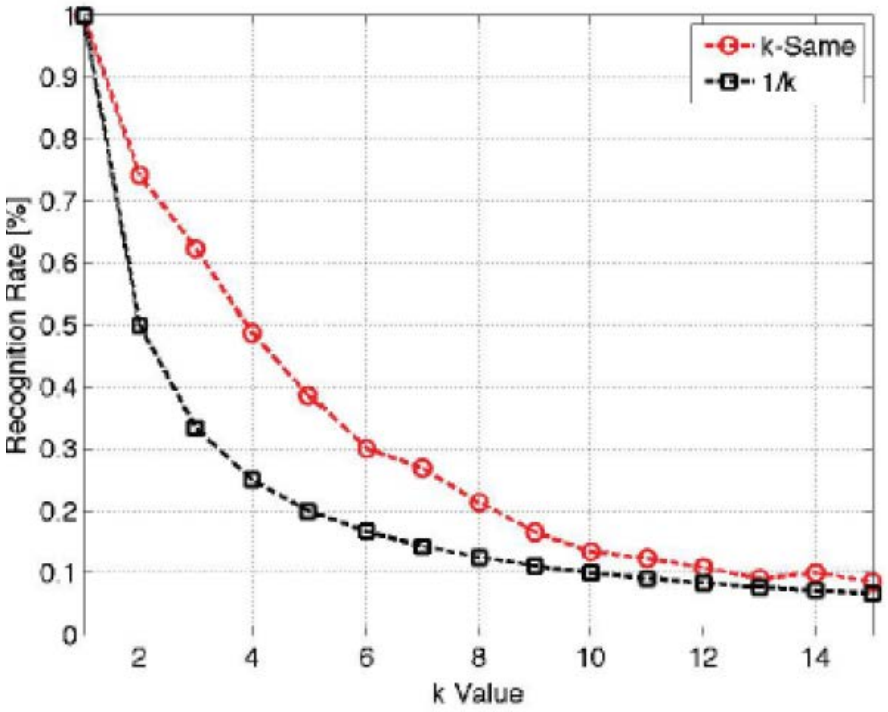


Fig. 4. k-Same de-identification: a) Original images; b) De-identified image for k = 2; c) De-identified image for k = 6; d) De-identified image for k = 20;

11th IEEE International Conference on Automatic Face and Gesture Recognition
FG2015

De-identification for Privacy Protection in Multimedia, Ljubljana, Slovenia, 4th May 2015

2. Face de-identification in still images



R. Gross, L. Sweeney, Towards Real-World Face De-Identification, First IEEE Conference on Biometrics, Theory, Applications, and Systems 2007,

11th IEEE International Conference on Automatic Face and Gesture Recognition
FG2015

De-identification for Privacy Protection in Multimedia, Ljubljana, Slovenia, 4th May 2015

2. Face de-identification in still images

- k-Same-Select algorithm

The algorithm partitions the input set of face images into mutually exclusive subsets using the data-utility function and applies the k-Same algorithm independently to the different subsets. The data utility function is usually selected to preserve the gender or a facial expression in the de-identified face images.

2. Face de-identification in still images

- In order to produce de-identified images of much better quality and preserve the data utility, the model-based k-Same algorithms are proposed

- based on Appearance Models (AAMs)

- based on the model that is the result of mixtures of identity and non-identity components obtained by factorizing the input images (R. Gross, L. Sweeney, J. Cohn, F. de la Torre, S. Baker)

2. Face de-identification in still images

a)

b) c) d)

Fig. 5. Model-based k-Same de-identification: a) Original images; b) De-identified image for k = 2; c) De-identified image for k = 6; d) De-identified image for k = 20;

11th IEEE International Conference on Automatic Face and Gesture Recognition
FG2015

De-identification for Privacy Protection in Multimedia, Ljubljana, Slovenia, 4th May 2015

3. Face de-identification in videos

- over 4 million CCTV cameras deployed in the United Kingdom, and that the average citizen in London is caught on CCTV cameras about 300 times a day (A. Cavallaro)

Solution (?)

- traditional approach to privacy protection in video is face obfuscation or masking that is performed manually

/The manual approach is unusable in applications such as 24-hour video surveillance, where the amount of data is enormous (there are 2,592,000 frames per day)/

Solution: automatic face de-identification in videos.

3. Face de-identification in videos

- Process of automatic face de-identification in videos combines face detection, face tracking and face masking
  - Face detection

    Problems:
  - large variances in poses of the face, sizes,
  - bad lighting conditions,
  - face affected by partial occlusion,
  - presence of structural components,
  - cluttered scenes

3. Face de-identification in videos

- Face detection

  - feature-based

  - image-based approach

Face-detector candidates

  - Viola-Jones face detector

  - Schneiderman-Kanade frontal and profile face detector

  - Detector(s) based on local edge orientation histograms (EOH)

  - Combination of the background subtraction, bag-of-segments feature and SVM

Combination of face detection and tracking improves the effectiveness of the localization of faces

De-identification for Privacy Protection in Multimedia, Ljubljana, Slovenia, 4th May 2015

3. Face de-identification in videos

Localized and traced face region in each frame has to be de-identified by masking - techniques that are used in still-face images

- Alternative approach to face de-identification, especially popular in the video-surveillance domain, is based on distortion applied to the face image by using transform-domain scrambling methods (F. Dufaux, T. Ebrahimi)
- A more sophisticated privacy protection in videos is obtained by replacing a face with a generic face

3. Face de-identification in videos

In order to improve the naturalness and utility of a de-identified video, the adoption of de-identification methods for still images is proposed: q-far de-identification method (B. Samarzija, S. Ribaric)

- face images are grouped into a person-specific set of images according to their poses
- each person-specific set is represented by an active appearance model
- raw face image is matched with each of the active appearance models of a person-specific set of images
- model with the best matching based on shape and texture is chosen to represent the pose of the raw face image
- from the images in the selected person-specific set of images, one image is chosen to replace the texture of the raw image
- in order to enhance the privacy protection, the appearance of an image that is far enough (q-far based on the Euclidean distance) is used

11th IEEE International Conference on Automatic Face and Gesture Recognition
FG2015

De-identification for Privacy Protection in Multimedia, Ljubljana, Slovenia, 4th May 2015

3. Face de-identification in videos

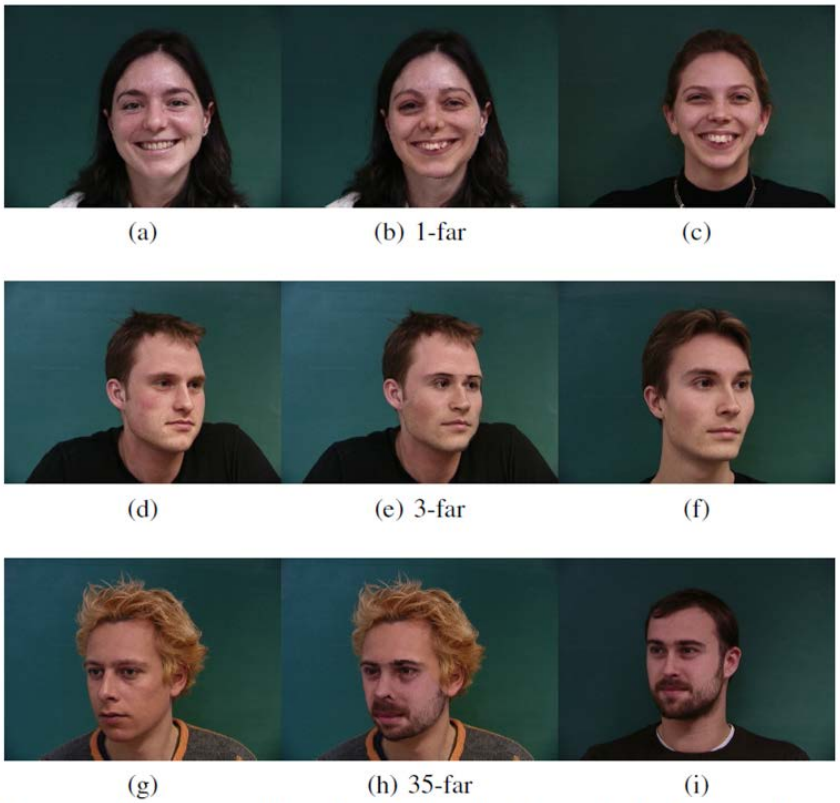


Fig.6. An illustration of the q-far de-identification method [34]. In each row the first image is a raw image (a), (d), (g); The second image is a de-identified image: (b) de-identified with q = 1 distance, (e) de-identified with q = 3, and (h) de-identified with q = 35; The third images in each row are images that were used for the face swapping.

11th IEEE International Conference on Automatic Face and Gesture Recognition
FG2015

De-identification for Privacy Protection in Multimedia, Ljubljana, Slovenia, 4th May 2015

3. Face de-identification in videos

P. Agrawal and P. J. Narayanan (2011) - general framework of de-identification by describing different scenarios of video capturing (casual videos, public surveillance and private surveillance videos)

• De-identification consists of three modules:

- Detect and Track (HOG-based person detector and a robust tracking algorithm (patch-based approach))
- Segmentation (performed by using the so-called fixed-size voxels (x × y × t))
- De-identification (exponential blur of pixels in the voxel or line integral convolution)

De-identification for Privacy Protection in Multimedia, Ljubljana, Slovenia, 4th May 2015

4. Face de-identification systems

Examples of real-time, privacy-protection video systems :

• Respectful Cameras (J. Schiff, M. Meingast, D. K. Mulligan, S. Sastry, K. Goldberg)
- users who wish to be protected wear colour markers (hats or vests) that are tracked and the faces of such users are masked in real time
• DSP-based PrivacyCam (A. Chattopadhyay, T.E. Boult)
- the face is protected by scrambling the coefficients used for the JPEG image encoding

4. Face de-identification systems

Examples of real-time, privacy-protection video systems (cont.):

• TrustCam prototype system (T. Winkler, B. Rinner)
- Trusted Platform Module (TPM) that is used for the data encryption to hide the identity of individuals captured in a video

• De-identification Camera (Mrityunjay, P. J. , Narayanan)
- Real-time privacy protection at the sensor level
- Gaussian blur or binarization

De-identification for Privacy Protection in Multimedia, Ljubljana, Slovenia, 4th May 2015

5. Conclusion

- Privacy is one of the most important social and political issues of any free society
- A human face, as the main biometric personal identifier present in still images and videos, is in the focus of de-identification research

Open problems:

- Real-time face detection, localization and tracing
- Naturalness and utility of de-identified videos
- Multimodal de-identification