# FACE DE-IDENTIFICATION FOR PRIVACY PROTECTION IN SURVEILLANCE SYSTEMS

**Darijan Marčetić, Branko Samaržija, Martin Soldić, Slobodan Ribarić**

**Laboratory for Pattern Recognition and Biometric Security Systems**
**Faculty of Electrical Engineering and Computing, University of Zagreb**
**E-pošta: slobodan.ribaric@fer.hr**
**URL: http://rubioss.zemris.fer.hr**

**ABSTRACT***: The article presents some of the intermediate results of face de-identification, after the first year of the scientific project "De-identification for Privacy Protection in Surveillance Systems - DePPSS". We present two face de-identification methods. The first face de-identification method, which improves the naturalness and utility of a de-identified video, is based on the active appearance models (AAMs) of a person-specific set of images. The second one is based on a unified model for face detection, pose and landmark estimation. The experimental results for the both methods are given.*

## 1. INTRODUCTION

Recent advances in technology and signal processing have greatly facilitated the efficacy of video surveillance [1], primarily for the benefit of security and law enforcement. Video surveillance is now widely exploited in a variety of scenarios to capture video recordings of people in public and semi-public environments [2], either for immediate recognition and tracking of people or/and abnormal behaviour recognition, or for storage, and subsequent data analysis and sharing. Whilst it is recognized that there are justified reasons for acquisition and sharing videos in manners such as security, bio-terrorism surveillance applications, low enforcement and forensics, there is also a strong need for protecting the privacy of the guiltless individuals who are inevitably captured in the recordings. There are no doubts that video surveillance is privacy intrusive because it allows the observation of certain information that is considered privacy sensitive. Face has central role in the process of human recognition and identification in videos, thus the special attention has to be devoted to the face de-identification methods for privacy protection. De-identification, in general, 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.

Project's research plan defines the following main phases and activities:

i. Review and analysis of previous approaches to the problem of face de-identification for still images and videos,

ii. Robust face localization in videos adopted to de-identification process,
iii. Novel algorithms and methods for automatic concealing of face identifiers with preserving the data utility and naturalness in videos,
iv. Set up the experimental camera surveillance system with inbuilt face de-identification,
v. Evaluation of privacy protection solutions in video surveillance.

In this paper we present the intermediate results of face de-identification, after the first year of 4-year scientific project "De-identification for Privacy Protection in Surveillance Systems - DePPSS".

## 2. FACE DE-IDENTIFICATION METHODS

The early research on face de-identification was focused on face still images, by using the ad-hoc approaches such as "black box", “pixelation” and “blurring” of the image region occupied by the face [3]. In the black-box approach, after the face detection and face localization in the image, the face region is simply substituted by a black (or white) rectangle, elliptical or circular covers. To achieve an improved level of privacy protection, more sophisticated approaches have been proposed: eigenvector-based de-identification method [4], *k*-Same, *k*-Same-Select algorithms and Model-based *k*-Same method [5], morphing- and warping-based [6] methods, cartooning [7] and scrambling-based methods [8]. The basic idea of the *k*-Same algorithms is illustrated in Figure 1.

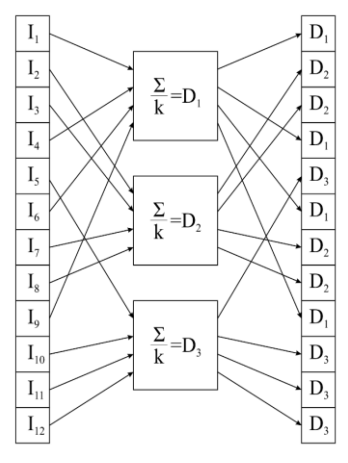


Figure. 1. The basic idea of *k*-Same algorithms

By applying the *k*-Same algorithm, to the given original person-specific set of images I, where each person is represented by no more than one image, a set of de-identified images D is computed. Each de-identified image is represented by an average face image of the *k* closest face images from the person-specific set of images. The *k* closest face images in the person specific set are replaced by the same *k* de-identified face images. The *k*-Same algorithm selects the *k* closest images based on Euclidean distances in the image space or in the Principal Component Analysis (PCA) coefficient space. The

process of de-identification is irreversible. Figure 2. illustrates the result of the *k*-Same de-identification.

a) b)

Figure 2. *k*-Same de-identification: a) Original image; b) De-identified image for $k = 6$; [9].

Special attention in the field of privacy protection is now being devoted to automatic face de-identification in video surveillance systems because of their privacy-intrusive characteristics [10]. The process of automatic face de-identification in videos includes:
i) face detection; ii) face tracking; and iii) face masking by concealing or removing personal identifiers, or replacing them with surrogate personal identifiers.

i) There are face-detector candidates for use in videos as follows: neural network based detector [11], Schneiderman-Kanade detector [12], Viola-Jones detector [13], local edge orientation histograms based (EOH) [14], and histograms of oriented gradients [15]. Recently, new methods have been proposed for face detection, pose estimation and landmark localization in the wild [16]. It is worth noting that privacy might be compromised in video sequences if the face detection algorithm fails in a single frame, so one of the directions of research is the development of robust and effective algorithms for privacy protection that can efficiently cope with situations when computer vision algorithms fail.

ii) Face tracking is the process of locating a moving human faces in a sequence of frames. Tracking is based on features such as segmented regions, skin-colour models [17], local binary patterns (LBP) [18], a combination of LBP and skin-colour information [19], a combination of shape and texture information [20], and histogram-based Mean-Shift features [21]. The combination of face detection and tracking, i.e. the combination of the spatial and temporal correspondence between frames, can improve the effectiveness of the localization of faces.

iii) Each localized and traced face region in each frame has to be de-identified by some effective means. Approaches to face masking for privacy protection in video-surveillance systems follow techniques that are used in still-face images, such as: ad-hock methods, *k*-Same-based methods, morphing, warping, cartooning and scrambling. These methods are tested and level of privacy protection was evaluated by PCA-, LDA-, LBP-based face recognition algorithms [22] and crowdsourcing approach [23].

## 3. TWO FACE DE-IDENTIFICATION METHODS AND RESULTS

In order to improve the naturalness and utility of a de-identified video, we adapted the de-identification methods for still images [24]. Normally, the faces captured in a video

sequence are of varied poses. Such variations may range from a full left profile to a full right profile (yaw angle from $-90^0$ to $+90^0$) and a pitch from $-90^0$ to $+90^0$, while the roll is usually more restricted. Following the idea from *k*-Same-Select [5], where images are grouped before de-identification to preserve the facial expression and the gender, the proposed approach groups the face images into a person-specific set of images according to their poses. Each person-specific set is represented by an active appearance model (AAM); Figure 3. A raw face image is matched with each of the active appearance models of a person-specific set of images. The model with the best matching based on shape and texture is chosen to represent the pose of the raw face image. Then, from the images in the selected person-specific set of images, one image is chosen to replace the texture of the raw image. The shape of the de-identified face image remains the same as that detected during the model fitting, but the texture is changed. Note that in order to enhance the privacy protection, instead of using the most similar appearance for the raw image, the appearance of an image that is far enough (q-far based on the Euclidean distance) is used [24]. The proposed de-identification method is irreversible. Figure 4. illustrates the above-described approach.

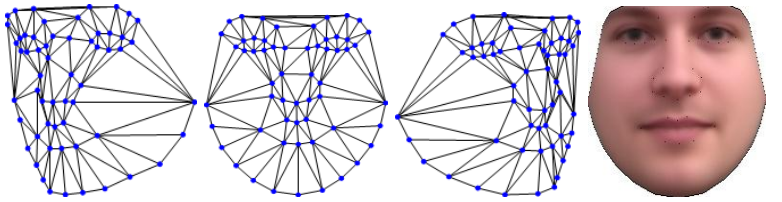

Figure 3: Model shapes (for 3 different poses) that are used for fitting to the raw image; Besides the shape, AAMs use the appearance. The appearance corresponding to the shape on far right.

The second method is based on a unified model for face detection, pose estimation, and landmark estimation described in [16]. This model is based on mixtures of trees with a shared pool of parts; facial landmarks are modelled as parts and global mixtures are used to capture topological changes due to viewpoint. This tree-structured can robustly handle global elastic deformation, and can be optimized with linear programming. This method is suitable for "in the wild" datasets. Figure 5. illustrates results of the second de-identification method.

For both methods the face region (ROI) detected in the original image is replaced with selected swapping face by performing following procedure. By using Delaunay triangulation, each part of the face region detected in the original image bounded by the triangles (Figure 3.) is taken into account (it is a convex region), while the rest of the ROI is neglected. Then affine warps from each triangle of ROI to the corresponding triangle of selected swapping face, are computed. The appearance of this triangle is copied into corresponding ROI triangle of the original image. To avoid possible gaps in the appearance (due to the differences in the triangle area sizes), backward warps are performed by appearance normalisation to the mean shape.

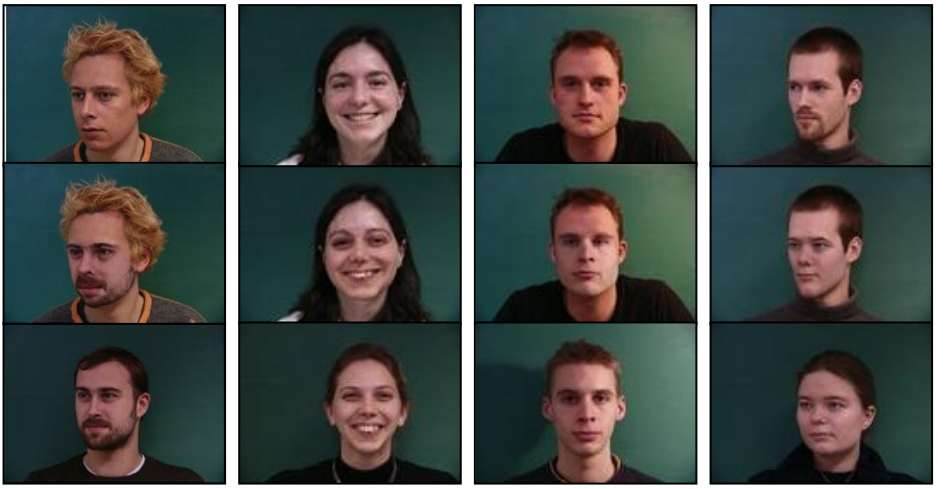

Figure 4. Illustration of the q-far de-identification method [24]: first original image; second row de-identified image q-far = 35; third row image used for the face swapping.


Figure 5. Illustration of the de-identification method: first original image; second row de-identified image; third row image used for the face swapping.

## 3. CONCLUSION

De-identification of the face in video surveillance systems is far from a complete solution. The problem lies not in the de-identification of ROIs, but in computer vision algorithms for the detection and localization of face(s) in video sequences. Despite recently intensive research in computer vision, numerous problems still remain to be solved in automatic face detection and consequently of face de-identification. These include issues such as the detection of the face under different illumination conditions, bad lighting conditions, different head positions, the presence of structural components (e.g., glasses, sunglasses, beards, moustaches), and occlusions. The unsolved problems are the detection of faces in crowd scenes and real-time de-identification.

## ACKNOWLEDGEMENT

This work has been fully supported by Croatian Science Foundation under the project 6733 De-identification for Privacy Protection in Surveillance Systems (DePPSS), Grant no:6733.

## LITERATURE

1. D. T. Raty, Survey on Contemporary Remote Surveillance Systems for Public Safety, IEEE Transactions on Systems, Man, and Cybernetics - Part C, vol. 40, no. 5, (2010) 493 - 515.
2. P. Agrawal, P. J. Narayanan, Person De-Identification in Videos, IEEE Transactions on Circuits and Systems for Video Technology, vol. 21, no. 3, (2011) 299 - 310.
3. M. Boyle, C. Edwards, S. Greenberg, The Effects of Filtered Video on Awareness and Privacy, ACM Conference on Computer Supported Cooperative Work, Philadelphia, December 2000, pp. 1-10
4. P. J. Phillips, Privacy operating characteristic for privacy protection in surveillance applications, in: T. Kanade, A. Jain, and N. Ratha (Eds.), Audio- and Video-Based Biometric Person Authentication, Lecture Notes in Computer Science, Springer, 2005, pp. 869 - 878.
5. R. Gross, L. Sweeney, J. Cohn, F. de la Torre, S. Baker, Face De-Identification, in: A. Senior (Ed.), Protecting Privacy in Video Surveillance, Springer, 2009, pp. 129 - 146.
6. P. Korshunov, T. Ebrahimi, Using Face Morphing to Protect Privacy, IEEE Int. Conference on Advanced Video and Signal-based Surveillance, (2013) 208 - 213.
7. A. Erdely, T. Barat, P. Valet, T. Winkler, B. Rinner, Adaptive Cartooning for Privacy Protection in Camera Networks, 11th IEEE Int. Conference on Advanced Video and Signal Based Surveillance (AVSS), (2014) 26 - 29.
8. F. Dufaux, T. Ebrahimi, Scrambling for Privacy Protection in Video Surveillance Systems, IEEE Trans. on Circuits and Systems for Video Technology, vol. 18, no. 8, (2008) 1168 - 1174.

9. S. Ribaric, N. Pavesic, An Overview of Face De-identification in Still Images and Videos, Workshop on De-identification for Privacy Protection in Multimedia, IEEE FG 2015 Ljubljana, (2015) 1 - 6.
10. A. Senior, Privacy Protection in a Video Surveillance System, in: A. Senior (Ed.), Protecting Privacy in Video Surveillance, Springer, Dordrecht, 2009, pp. 35 - 47.
11. H. A. Rowley, S. Baluja, T. Kanade, Neural Network-Based Face Detection, IEEE Trans. on Pattern Analysis and Machine Intelligence, vol. 20, no. 1, (1998) 23-38.
12. H. Schneiderman, T. Kanade, A Statistical Method for 3D Object Detection Applied to Faces and Cars, Proceedings on Conference Computer Vision and Pattern Recognition, vol. I, (2001) 746 - 751.
13. P. Viola, M. J. Jones, Robust Real-Time Face Detection, International Journal of Computer Vision 57(2), (2004) 137 - 154.
14. K. Levi, Y. Weiss, Learning Object Detection from a Small Number of Examples: the Importance of Good Features, Proceedings of the 2004 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'04), vol. 2, (2004) II - 53 - II - 60.
15. N. Dalal, B. Triggs, Histograms of Oriented Gradients for Human Detection, IEEE Conference on Computer Vision and Pattern Recognition, 2005, vol. 1, 886 - 893.
16. X. Zhu, D. Ramanan, Face Detection, Pose Estimation, and Landmark Localization in the Wild, Proceedings on Conference Computer Vision and Pattern Recognition, (2012) 2879 - 2886.
17. J. Yang, A. Waibel, A Real-Time Face Tracker, Proceedings 3rd IEEE Workshop on Applications of Computer Vision WACV '96, (1996) 142 - 147.
18. L. Xu, J. Li, K. Wang, Real-time and Multi-View Face Tracking on Mobile Platform, IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), (2011) 1485 - 1488.
19. W. Chuan-xu, L. Zuo-yong, A New Face Tracking Algorithm Based on Local Binary Pattern and Skin Color Information, 2008 International Symposium on Computer Science and Computational Technology, (2008) 657 - 660.
20. W-P. Choi, K-M. Lam, An Effective Shape-Texture Weighted Algorithm for Multi-view Face Tracking in Videos, 2008 Congress on Image and Signal Processing, (2008) 156 - 160.
21. D. Comaniciu, V. Ramesh, P. Meer, Real-Time Tracking of Non-Rigid Objects using Mean Shift, Proceedings on IEEE Conference on Computer Vision and Pattern Recognition, vol. 2, (2000) 142 - 149.
22. R. Gross, E. Airoldi, B. Malin, L. Sweeney, Integrating Utility into Face De-identification, in: G. Danezis and D. Martin (Eds.): PET- Privacy Enhancing Technologies 2005, LNCS 3856, 2006, pp. 227 - 242.
23. P. Korshunov, S. Cai, and T. Ebrahimi, Crowdsourcing approach for evaluation of privacy filters in video surveillance, Proceedings of the ACM Multimedia 2012 Workshop on Crowdsourcing for Multimedia, Japan, CrowdMM'12, (2012) 35 - 40.
24. B. Samarzija, S. Ribaric, An Approach to the De-Identification of Faces in Different Poses, Proceedings of Special Session on Biometrics, Forensics, De-identification and Privacy Protection BiForD 2014, (2014) 21 - 26.