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

***Abstract*—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. One of the approaches to the preservation of privacy is de-identification, where de-identification is the process of concealing or removing personal identifiers, or replacing them with surrogate personal identifiers in personal information, captured in a multimedia content, in order to prevent the disclosure and use of data for purposes unrelated to the purpose for which the information was originally obtained. This paper presents a survey of approaches, methods and solutions for face de-identification in still images and videos.**

I. INTRODUCTION

Recent advances in cameras, web technology and signal processing have greatly facilitated the efficacy of video surveillance, primarily for the benefit of security and law enforcement. This technology is now widely exploited in a variety of scenarios to capture video recordings of people in semiprivate and public environments, either for immediate inspection (e.g., abnormal behaviour recognition, identification and tracking of people in real time) or for storage, subsequent analysis and data sharing. Capabilities in the field are further supported through continued progress in a number of relevant areas, including smart, multi-camera networks [1], wireless networks of multispectral image sensors, distributed intelligence and awareness, and distributed processing power [2].

Whilst it is clear that there are justifiable reasons for sharing multimedia data acquired in such ways (e.g., law enforcement, forensics, bioterrorism surveillance, disaster prediction), there is also a strong need to protect the privacy of innocent individuals who are inevitably "captured" in the recordings. In order to recognise the growing scale of this surveillance and its effects on privacy, it is worth noting that, for instance, there are 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 [3]. The problem associated with this is further exacerbated by a lack of compliance with the relevant data-protection legislation. According to a study in [4], this is the case for over 80% of the CCTV systems deployed in London's business space. An additional and growing feature of the privacy problem in today's networked society is the advent of technologies such as "Google Street View" and "EveryScape", social networks, biometrics, multimedia, big data, and data mining. These provide an additional framework for the invasion of an individuals' privacy.

In view of the above issues, considerable research has now been directed towards approaches to the preservation of privacy in such a way to protect personal identifiable information or personal identifiers, where personal identifier is that personal information which allow his or her identification.

Face is the main biometric personal identifier used for biometric-based identification [5]. Face-based identification is used in various application scenarios - from identification of a person based on still image in passport or identity card, through identification of the persons in the photographs of crowded scenes, to identification based on face images captured either overtly or covertly by a surveillance system without the cooperation of the person [6]. In many application scenarios, especially in video surveillance, privacy can be compromised.

De-identification [7] is one of the basic methods for protecting privacy, while permitting other uses of personal information. 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.

This paper presents a survey of approaches, methods and solutions for face de-identification in still images and videos. Besides the solutions for face de-identification, we also point to the open problems and challenges related to face de-identification, naturalness and the usability of de-identified contents.

II. FACE DE-IDENTIFICATION IN STILL IMAGES

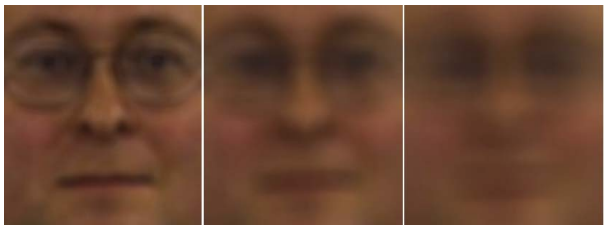
The main biometric personal identifier present in still images and videos used to identify people is the face [5], therefore it is in the focus of de-identification. The early research on face de-identification was focused on face still images, and recommended the use of ad-hoc approaches such as "black box", "pixelation" and "blurring" of the image region occupied by the face [8], [9]. 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. Pixelation consists of reducing the resolution (subsampling) of a face region (Fig.1; the experiments were performed on the cmu-pie-database [42]). Blurring is a simple method based on smoothing the face in an image with Gaussian filters using a

978-1-4799-6026-2/15/$31.00 ©2015 IEEE

variety of sufficiently large variances. By applying different variances, different levels of blurred images of the face are obtained [8] (Fig. 2.). Naive methods such as blurring and pixelation might prevent a human from recognising subjects in the image, but they cannot thwart recognition systems. An effective approach that subverts naive de-identification methods is called parrot recognition [10]. Instead of comparing the de-identified images to the original images, parrot recognition is based on comparing probe (de-identified) images with gallery images, where the same distortion is applied as in the probe images. It was shown that such an approach drastically improves the recognition rate, i.e., reduces the level of privacy protection [10].

a) b) c)

Fig. 1. Pixelation (adopted from [41]): a) Original image; b) Pixelation parameter $p = 6$; Pixelation parameter $p = 12$;



a) b) c)

Fig. 2. Blurring (adopted from [41]): a) $\sigma^2 = 9$; b) $\sigma^2 = 18$; c) $\sigma^2 = 30$;

To improve the level of privacy protection, more sophisticated approaches have been proposed. In [11] an eigenvector-based de-identification method is described. The original face is substituted by a reconstructed face that is obtained by applying a smaller number of eigenfaces, so the face details are lost and the de-identified image becomes harder to recognise. In the same paper, the privacy-operating characteristic (POC) is introduced and used to show, quantitatively, the trade-off between privacy and security. The eigenvector-based method easily produces very unnatural images, but still keeps some of the facial characteristics that can be used for automatic recognition.

In recent years, advances in biometric identification have inspired researchers in the field of de-identification. Examples are the methods referred to as k-Same, k-Same-Select algorithms [12] and Model-based k-Same for face de-identification [13]. By applying the k-Same algorithm, for the given person-specific set of images, where each person is represented by no more than one image, a set of de-identified images is computed. The de-identified image is represented by an average face image of the k closest face images from a 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.

Figure 3. illustrates the k-Same algorithm (k = 4) where for a person-specific set of face images I, which consists of 12 original images, the set of de-identified face images D is computed. The set D consists of 12/k identical face images, where each image is represented as an average of the k = 4 closest original images.

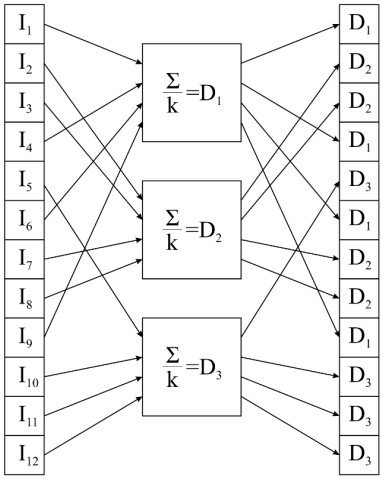
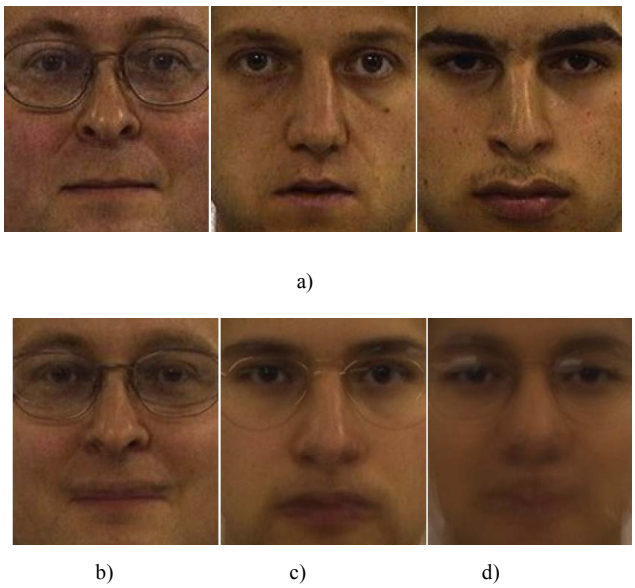


Fig. 3. An illustration of k-Same algorithm; adopted from [16]. For example, the original images I1, I4, I6 and I9 are represented with the same de-identified face image D1; I - a person-specific set of face images; D - a set of de-identified face images; $\sum$ - a sum of the k closest face images from a person-specific set of images I;

Figure 4. ilustrates the k-Same de-identification for different values of k [41].

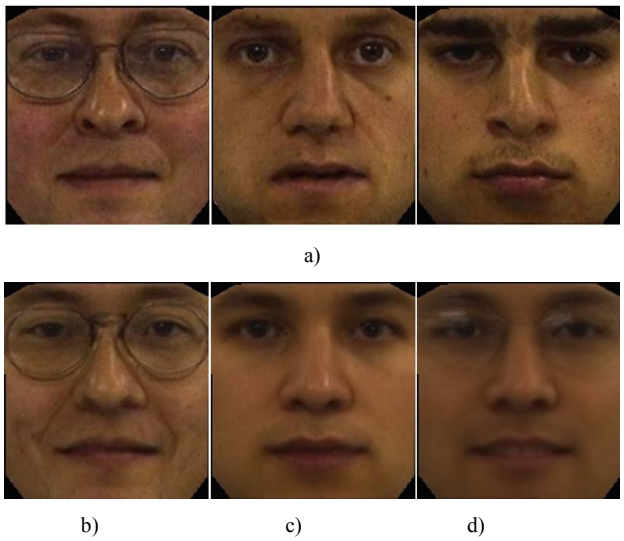


a) b) c) d)

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;

It was shown that the best-possible success rate for a face-recognition algorithm linking a de-identified face image to the correct face image in the set I is 1/k [14]. The procedure based on the k-Same algorithm is irreversible, guarantees probable privacy (1/k), but very often results in "ghosting" artefacts in de-identified images due to image misalignment or an expression variant of the faces present in the k images from set I.

In order to improve the data utility and the naturalness of the de-identified face images, the k-Same-Select is proposed [13]. 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. Due to use of the k-Same algorithm, k-Same-Select guarantees that the resulting face set is k-anonymized [14]. For both algorithms there are two main problems: they operate on a closed face set I, and the determination of the proper privacy constraint k. In order to produce de-identified images of much better quality and preserve the data utility, the model-based k-Same algorithms are proposed – one of which is based on Active Appearance Models (AAMs) [15] and another based on the model that is the result of mixtures of identity and non-identity components obtained by factorizing the input images [16]. Figure 5. illustrates the results of the model based k-Same de-identification [41].



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;

Modifications to the k-Same Select algorithm, in order to improve the naturalness of the de-identified face images (by retaining face expression) and privacy protection, are proposed in [17], [18].

Most of the above-described methods are applicable for the de-identification of still frontal facial images or facial images in a television broadcast, while they are unsuitable for use in video-surveillance systems, for the following reasons: such privacy-protection schemes degrade the visual quality needed for security, they do not preserve the naturalness of the de-identified moving images, and they modify the surveillance videos in an irreversible fashion.

III. FACE DE-IDENTIFICATION IN VIDEOS

Special attention in the field of privacy protection is devoted to face de-identification in video surveillance systems because of their privacy-intrusive character [19]. The traditional approach to privacy protection in video is face obfuscation or masking that is performed manually. The main drawback of this method is that the face region needs to be manually marked and replaced by an elliptical or rectangular overlay, or by pixelation of the area in each video frame. This process is time consuming because there are 30 frames per second, which means that for a few minutes of video more than ten thousand images have to be inspected. 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), and real-time processing is required [20]. The solution is the automatic face de-identification in videos.

The process of automatic face de-identification in videos combines face detection, face tracking and face masking. The first step in face de-identification for video is face detection. Due to the large variances in poses of the face, sizes, bad lighting conditions, the face affected by partial occlusion, the presence of structural components (e.g., glasses, sunglasses, beards, moustaches) and cluttered scenes, the face detection has to be robust. There are two main approaches to face detection [21]: the feature-based approach and the image-based approach. The feature-based approach uses low-level analyses (based on edges, colour, grey-level, motion), feature analyses (facial feature extraction, face detection based on anthropometric measures, statistical-based grouping of facial features in face-like constellations) and active shape models (snakes, deformable templates, point distributed models). The image-based approach detects faces via a learning procedure that classifies examples into face and non-face prototype classes. The main methods are linear subspace methods, neural networks, and statistical methods. An excellent overview of the face-detecting methods in images and videos is given in [22].

There are face-detector candidates for use in videos such as: an upright frontal face detector based on a neural network [23], the Schneiderman-Kanade frontal and profile face detector, which combines visual attributes represented by subsets of quantized wavelet coefficients and statistics expressed by the likelihood ratio between possibilities of “face class” and “non-face class” [24], the Viola-Jones face detector based on Haar-like features and the boosting technique, which achieves fast and robust frontal face detection in real-time [25], the face real-time detector using local edge orientation histograms (EOH) as features in the AdaBoost algorithm, which greatly improves the learning of frontal faces from a small database and enables an improvement in real-time systems for learning profile faces [26].

There are some approaches that combine the background subtraction and bag-of-segments feature to represent head-and-shoulder patterns, and a Support Vector Machine (SVM)

classifier to detect faces [20]. Face detection in videos under changing illumination conditions, with the face having varying poses and scales, is still a major challenge.

Face tracking is a process of locating a moving human face (or multiple human faces) in a sequence of frames. Beside this, face tracking needs to find the same face (in the case of multiple human faces) in a video. Tracking is based on features such as segmented regions, skin-colour models [27], local binary patterns (LBP) [28], a combination of LBP and skin-colour information [29], a combination of shape and texture information [30], and histogram-based Mean-Shift features [31]. Face tracking includes the prediction of a face location in the next image frame based on the motion model or the information obtained from the previous consecutive frames. Kalman filters and particle filters are normally used for predictions. On the basis of this prediction, the face tracking can be treated as a local search problem where the features are locally searched within a search window instead of the entire image. In order to increase the tracking speed an adaptive search window is used. Its size may grow with the square of the maximum velocity of the face [27].

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. An example of such an approach is applying a bi-directional tracking algorithm that combines face detection, tracking and background subtraction [20]. The effectiveness of the face detection and tracking is very important because the face has to be detected and de-identified in each frame of the videos. If the face cannot be detected in only one frame (and so is not de-identified) this means a major degradation in the privacy protection.

Each localized and traced face region in each frame has to be de-identified by masking. Some approaches to face masking for privacy protection in video-surveillance systems follow techniques that are used in still-face images using a "black-box" approach, simple blurring filters, and pixelation.

An 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. For example, in [32], [33] the authors proposed two scrambling methods for H.264/AVC – one of the most commonly used formats for the recording, compression, and distribution of video content. Both methods scramble the quantized transform coefficient of each 4 × 4 block of the region of interest by pseudo-randomly flipping their sign, or by applying a random permutation of the coefficients. These two methods are fully reversible – the authorized user, by using a secret encryption key, can reverse the scrambling process and recover the image of the face.

A more sophisticated privacy protection in videos is obtained by replacing a face with a generic face. The preliminary results of such an approach applied to video sequences are shown in [16]. Recently, in order to improve the naturalness and utility of a de-identified video, the adoption of de-identification methods for still images is proposed in [34]. In the video sequences the people's faces are captured in arbitrary poses. The face poses vary 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 [10], 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. 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. Figure 6. illustrates the above-described approach

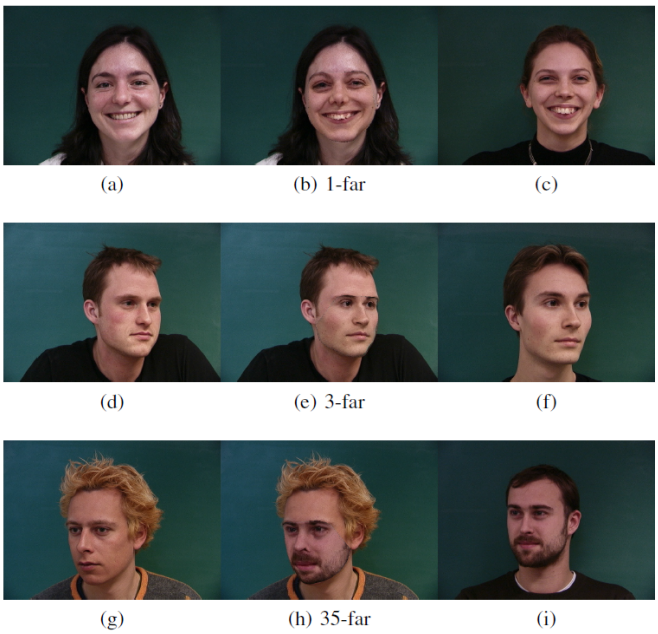


Fig.6. An illustration of the q-far de-identification method [34]. In each row the first image is a row image (a), (d), (g); The second image is a de-identified image: (b) de-identified with q = 1 distance, (e) de-identified with q = 3, and (h) de-identified with q = 35; The third images in each row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

In [35] the authors give the general framework of de-identification by describing different scenarios of video capturing (casual videos, public surveillance and private surveillance videos), criteria for de-identification and methods of subverting the de-identification. They proposed a method of de-identification that consists of three modules: Detect and Track, Segmentation and De-identification. The detect-and-track module combines a HOG-based person detector and a robust tracking algorithm. The tracking algorithm uses a patch-based recognition approach: the object is divided into multiple spatial patches and each of them is tracked by a voting mechanism based on the histogram of the corresponding image patch [35]. The system uses the

bounding boxes of the person in every frame and forms a video tube across time. Each detected person in a video has his or her own video tube. The segmentation of the video tube is performed by using the so-called fixed-size voxels (x × y × t) in the spatial (x, y) and temporal (t) domains. The result of the segmentation is the classification of the voxels into two classes: foreground and background. The de-identification is performed on foreground voxels by applying the exponential blur of pixels in the voxel or line integral convolution. The implemented system was tested on standard data sets like CAVIAR and BEHAVE.

Despite the current research, numerous problems and challenges still remain to be solved in face de-identification in videos. These include issues such as occlusion, head position, presence of structural components (e.g. glasses, beard), illumination conditions, and the preservation of data utility (e.g. age, gender and facial expression) and naturalness of de-identified video.

IV. Face De-identification Systems

Examples of real-time, privacy-protection video systems are as follows: Respectful Cameras [36], PrivacyCam [37], TrustCam [38], and the De-Identification Camera [39]. In the Respectful Cameras system 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. The tracker is based on a 9-dimensional colour space and the combination of a particle filter and a probabilistic AdaBoost algorithm. Because of the type of markers used the system it is well suited to dynamic scenes. An elliptical white cover is used to hide the faces of the users.

The DSP-based PrivacyCam [37] system implements a real-time Privacy through Invertible Cryptographic Obscuration (PICO) process that consists of five basic steps: i) capture of the image with a camera, ii) detection of the region of interest (face detection, skin detection, motion detection), iii) exchanging public key, generating session key, and storing the secured key along with the protected region information, iv) selective encryption of the region (human face region) to be protected. The face is protected by scrambling the coefficients used for the JPEG image encoding.

The TrustCam prototype system [38] consists of a network of trustworthy cameras and a control station. Each camera is equipped with an individual Trusted Platform Module (TPM) that is used for the data encryption to hide the identity of individuals captured in a video.

The De-identification Camera [39] is an example of real-time privacy protection at the sensor level. The de-identification pipeline of the De-identification Camera consists of the background segmentation (motion detection), person detection based on histograms of gradients (HOG) [40], tracking based on Mean-Shift, segmentation of an image based on a bounding box that forms a video tube for each person in time, and a de-identification transform applied on the video tube. The real-time identification transform uses two types of "naive" procedures: the Gaussian blur of pixels inside a bounding box, and the binarization of the pixels inside the bounding box. Note that the De-identification Camera performs de-identification of the whole human figure.

Due to the scrambling of the coefficients, or using "naive" de-identification techniques, all the above-described systems produce de-identified videos that do not preserve the naturalness of the original videos.

V. Conclusion

Privacy is one of the most important social and political issues of any free society. In our networked society, which is characterized by technologies and services such as internet, wireless communication, social networks, biometrics, multimedia, big data, data-mining, and audio and video surveillance, the problem of the privacy protection of individuals becomes a major challenge for experts from law, political, ethical and technical domains.

A human face, as the main biometric personal identifier present in still images and videos, is in the focus of de-identification research. In spite of relatively big research efforts in the field of face de-identification and proposed solutions, there are many open problems, such as real-time detection, localization, tracing and removing, hiding or substituting the faces as physiological biometric identifiers. These problems are particularly emphasized for videos of crowded scenes. Additional problems arise when there is demand to preserve the usability and naturalness of the de-identified video at the same time.

Due to recent advances in multi-sensor acquisition and recording devices and remote surveillance systems, there is a need for the research and development of multimodal de-identification methods that simultaneously hide, remove or substitute different types of personal identifiers (face, gesture, gait) from multimedia content. The solution of the problem of multimodal de-identification is still a major challenge.

Acknowledgment

This work has been fully supported by Croatian Science Foundation under the project 6733 De-identification for Privacy Protection in Surveillance Systems (DePPSS). It is the result of the collaboration between partners in COST Action IC1206 "De-identification for Privacy Protection in Multimedia Content".

References

[1] K. Abas, C. Porto, K. Obraczka, "Wireless Smart Camera Networks for the Surveillance of Public Spaces", IEEE Computer, vol. 47, no. 5, pp. 37-44, May 2014.

[2] D. T. Raty, "Survey on Contemporary Remote Surveillance Systems for Public Safety", IEEE Transactions on Systems, Man, and Cybernetics—Part C: Applications and Reviews, vol. 40, no. 5, pp. 493-515, September 2010.

[3] A. Cavallaro, "Privacy in Video Surveillance", IEEE Signal Processing Magazine, pp. 168-169, March 2007.

[4] A. Senior, "Privacy Protection in a Video Surveillance System", in *Protecting Privacy in Video Surveillance*, (A. Senior, ed.), Springer, pp. 35-47, 2009.

[5] S. Z. Li, A. K. Jain (eds.), *Handbook of Face Recognition*, Springer, 2005.

[6] R. M. Bolle, J. H. Connell, S. Pankanti, N. K. Ratha. A. W. Senior, *Guide to Biometrics*, Springer, 2004.

[7] R. Gellman, "The Deidentification Dilemma: A Legislative and Contractual Proposal, Fordham Intellectual Property", Media and Entertainment Law Journal, vol.21, issue 1, pp. 33-61, 2011.

[8] M. Boyle, C. Edwards, S. Greenberg, "The Effects of Filtered Video on Awareness and Privacy", ACM Conference on Computer Supported Cooperative Work, Philadelphia, pp. 1-10, December 2000.

[9] C. Neustaedter, S. Greenberg, M. Boyle, "Blur Filtration Fails to Preserve Privacy for Home-Based Video Conferencing", ACM Trans. on Computer Human Interaction, vol. 13, issue 1, pp. 1-36, March 2006.

[10] E. Newton, L. Sweeney, B. Malin, "Preserving Privacy by De-identifying Facial Images", IEEE Trans. on Knowledge and Data Engineering, vol. 17, no.2, pp. 232-243, February 2005.

[11] P. J. Phillips, "Privacy operating characteristic for privacy protection in surveillance applications," Audio- and Video-Based Biometric Person Authentication (T. Kanade, A. Jain, and N. Ratha, eds.), Lecture Notes in Computer Science, Springer pp. 869-878, 2005.

[12] R. Gross, E. Airoldi, B. Malin, L. Sweeney, "Integrating Utility into Face De-identification", G. Danezis and D. Martin (eds.): PET- Privacy Enhancing Technologies 2005, LNCS 3856, pp. 227–242, 2006.

[13] R. Gross, L. Sweeney, F. de la Torre, S. Baker, "Model-Based Face De-Identification", Proceedings of the 2006 Conference on Computer Vision and Pattern Recognition Workshop (CVPRW'06), 2006. /http://repository.cmu.edu/

[14] L. Sweeney, "k-Anonymity: A Model for Protecting Privacy", International Journal on Uncertainty, Fuzziness and Knowledge-Based Systems, vol. 10, no. 5, pp. 557-570, 2002.

[15] T. Cootes, G. Edwards, C. Taylor, "Active appearance models", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 23, pp. 681–685, June 2001.

[16] R. Gross, L. Sweeney, J. Cohn, F. de la Torre, S. Baker, "Face De-Identification", in [4], pp. 129-146, 2009.

[17] L. Meng, Z. Sun, A. Ariyaeeinia, K. L. Bennett, "Retaining Expressions on De-identified Faces", Proceedings of Special Session on Biometrics, Forensics, De-identification and Privacy Protection BiForD 2014, pp. 27-32, 2014.

[18] L. Meng, Z. Sun, "Face De-identification with Perfect Privacy Protection", ibid, pp. 9-14, 2014.

[19] http://plato.stanford.edu/ (accessed June, 2014)

[20] D. Chen, Yi Chang, R. Yan, J. Yang, "Protecting Personal Identification in Video", in [4], pp. 115-128, 2009.

[21] E. Hjelmas, B. K. Low, "Face Detection: A Survey", Computer Vision and Image Understanding 83, pp. 236–274, 2001.

[22] M.-H. Yang, D. J. Kriegman, N. Ahuja, "Detecting Faces in Images: A Survey", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 24, no. 1, pp. 34-58, January 2002.

[23] H. A. Rowley, S. Baluja, T. Kanade, "Neural Network-Based Face Detection", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 20, no. 1, pp. 23-38, January 1998.

[24] 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, pp.746-751, 2000.

[25] P. Viola, M. J. Jones, "Robust Real-Time Face Detection", International Journal of Computer Vision 57(2), pp.137–154, 2004.

[26] 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, pp. II-53-II-60, 27 June-2 July, 2004.

[27] J. Yang, A. Waibel, "A Real-Time Face Tracker", Proceedings 3rd IEEE Workshop on Applications of Computer Vision, WACV '96, pp. 142 – 147, 1996.

[28] 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), pp. 1485-1488, 2011.

[29] 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, pp. 657-660, 2008.

[30] 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, pp.156-160, 2008.

[31] D. Comaniciu, V. Ramesh, P. Meer, "Real-Time Tracking of Non-Rigid Objects using Mean Shift", Proceed on. IEEE Conference on Computer Vision and Pattern Recognition, vol: 2, pp. 142 - 149, 2000.

[32] F. Dufaux, T. Ebrahimi, "A Framework for the Validation of Privacy Protection Solutions in Video Surveillance", 2010 IEEE International Conference on Multimedia and Expo (ICME), pp.66-71, 2010.

[33] F. Dufaux, T. Ebrahimi, "Scrambling for Privacy Protection in Video Surveillance Systems", IEEE Transactions on Circuits and Systems for Video Technology, vol. 18, no. 8, pp. 1168-1174, August 2008.

[34] 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, pp.21-26, 2014.

[35] P. Agrawal and P. J. Narayanan, "Person De-Identification in Videos", IEEE Transactions on Circuits and Systems for Video Technology, vol. 21, no. 3, pp. 299-310, March 2011.

[36] J. Schiff, M. Meingast, D. K. Mulligan, S. Sastry, K. Goldberg, "Respectful Cameras: Detecting Visual Markers in Real-time to Address Privacy Concerns", in [4], pp. 65-89, 2009.

[37] A. Chattopadhyay, T.E. Boult, "PrivacyCam: a Privacy Preserving Camera Using ucLinox on the Blackfin DSP", IEEE Conference on Computer Vision and Pattern Recognition, 2007. CVPR '07, pp. 1 – 8, 2007.

[38] T. Winkler, B. Rinner, "TrustCAM: Security and Privacy-Protection for an Embedded Smart Camera based on Trusted Computing", Seventh IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), pp. 593 – 600, Aug. 29 -Sept. 1 2010.

[39] Mrityunjay, P. J. , Narayanan, "The De-Identification Camera", Third National Conference on Computer Vision, Pattern Recognition, Image Processing and Graphics, pp.192 -195, 2011.

[40] N. Dalal, B. Triggs, "Histograms of Oriented Gradients for Human Detection", IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2005, vol. 1, 2005. , pp. 886 – 893, 2005.

[41] R. Benko, Face De-identification, University of Zagreb, Faculty of EE and Computing, Diploma Thesis no. 1928, September 2013.

[42] http://www.computervisiononline.com/dataset/cmu-pie-database