De-identification for Privacy Protection in Multimedia Content: A Survey

Slobodan Ribarić,

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

COST ACTION
IC1206

De-identification
for privacy protection
in multimedia content.

Overview

1. Introduction
2. Privacy
3. De-identification and irreversible de-identification
4. Taxonomy of the identifiers in multimedia content
5. De-identification of non-biometric identifiers
6. De-identification of physiological biometric identifiers
7. De-identification of behavioural biometric identifiers
8. De-identification of soft biometric identifiers
9. Conclusion

1. Introduction

- Advances in audio-recording devices, multi-camera networks, wireless networks of multispectral image sensors and audio-sensor arrays, drones, web technology, signal processing, and distributed intelligence and distributed processing power have greatly facilitated the efficacy of audio and video surveillance primarily for the benefit of security and law enforcement

- This technology is now widely exploited in a variety of scenarios to capture audio-video recordings of people in public, semipublic and private environments

  - immediate inspection (e.g., abnormal behaviour recognition, identification and tracking of people in real time)

  - storage, and subsequent data analysis and sharing

1. Introduction

- (+) law enforcement, forensics, bioterrorism surveillance, disaster prediction
- (-) need to protect the privacy of innocent individuals who are captured in the recordings

- In many application scenarios, especially in video surveillance, privacy can be compromised

  - There must be a balance between privacy and security

Preservation of privacy: de-identification

1. Introduction

- In order to recognize the growing scale of this surveillance and its effects on privacy:

  - over 4 million CCTV cameras deployed in the United Kingdom

  - the average citizen in London is caught on CCTV cameras about 300 times a day

- lack of compliance with the relevant data-protection legislation (this is the case for over 80% of the CCTV systems deployed in London's business space)

1. Introduction

- 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

1. Introduction

- Julia Angwin (Dragnet Nation, 2015): "we are living in the world of indiscriminate tracking where institutions are stockpiling data about individuals at an unprecedented pace"

  This indiscriminate tracking is powered by "the technology we love so much" - powerful desktops, laptops, tablets, smartphones and web services

1. Introduction

Considerable research has now been directed towards approaches for the preservation of privacy and personal information

i) personal information is any information relating to a person

ii) personal identifiable information (or personal identifiers) is the personal information, which allow his or her identification

Preservation of the privacy of persons captured in multimedia content necessitates the de-identification of all of their personal identifiers

2. Privacy

- The term “privacy” is used frequently in ordinary language as well as in philosophical, political, legal and technical discussions, yet there is no single definition of the term

Privacy (D. J. Solove, 2008):

... "the most comprehensive of rights and the right most valued by civilized men"...

..."our ability to create and maintain different sorts of social relationships with different people"...

... "an integral part of our humanity"...

... "beginning of all freedom"...

2. Privacy

- From the legal point of view, the first definition of privacy was given by Louis D. Brandeis and Samuel D. Warren more than 120 years ago (Warren & Brandeis, 1890)

They defined privacy as the right to be let alone, and this right was specified by following types:

i) with respect to the acquisition and dissemination of information concerning the person…

ii) with respect to governmental searches and seizures that invade a sphere of individual solitude…

iii) when one individual's freedom of speech threatens to disrupt another citizen's liberty of thought and repose..

iv) with respect to fundamental (often unanticipated) decisions concerning the individual's own person…

2. Privacy

- Alan F. Westin defines privacy as the claim of an individual to determine what information about himself or herself should be known to others (Westin, 2003).

- A deep and comprehensive insight into the theory of privacy, existing attempts to conceptualize privacy and different definitions of privacy from the standpoint of jurists, philosophers and sociologists are given in the book D.J. Solove, "Understanding of Privacy", 2008.

2. Privacy

- Phases of contemporary privacy development:

i) The first era of contemporary privacy development, (period 1961–1979), which is characterized by the rise of information privacy as an explicit social, political, and legal issue of the high-technology age

ii) The second era of privacy development, (period 1980–1989). Technologically, this was a period of enhanced computer and telecommunications performance, but without fundamental changes in information-society relationships bearing on privacy

iii) The third era of privacy development, (period 1990–2002). This is the period when privacy became a first-level social and political issue in the United States, assumed global proportions, and was impacted by 9/11 and its aftermath

2. Privacy

In 1970s, European countries began to enact privacy laws applicable to the public and private sectors:

Sweden (1973)

Federal Republic of Germany (1977)

France (1978)

The main framework for privacy and personal data protection in the European Union:

The 1995 Data Protection Directive of the European Union (Directive 95/46/EC)

2. Privacy

- The directive defines the following six basic principles of Fair Information Practices:

i) the existence of personal data collections should be public knowledge;

ii) individuals have the right to review and correct their information;

iii) the minimum information necessary should be collected, and where appropriate, the consent of the included individuals should be obtained;

iv) personal data should be accurate and complete and retained only for the given time period;

v) data should only be used for the purpose originally intended;

vi) data should be protected by security safeguards against unauthorized access, modification or use.

2. Privacy

- In July 2008, the Information Commissioner's Office (ICO) commissioned a review of the 1995 EU Data Protection Directive (95/46/EC):

i) Defining privacy - when privacy is affected by personal data processing and when it is not

ii) Risk assessment – can we predict how risky it is to provide our personal data to an entity or organization?

iii) Rights of individuals in relation to the benefit of society

iv) Transparency – personal data is widely available and accessible, particularly online and through technological developments such as ambient intelligence and cloud computing

....

2. Privacy

There must be a balance between privacy and security because it guarantees foundations of our freedom and democracy

In contemporary times, the balance has shifted towards the security side of scale

2. Privacy

- COST Action IC1206 "De-identification for privacy protection in multimedia content

- *Privacy* - the ability of an individual or group to have their personal information and affairs secluded from others, and to disclose them as they choose.
- *Multimedia content* - text, still images, audio and video sequences, and their combination
- *De-identification* 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.

3. De-identification and irreversible de-identification

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

- The terms *de-identification* and *anonymization* are synonyms, but some experts make the difference between them:

- De-identification refers to the reversible process of removing or obscuring any personally identifiable information from individual records

- Anonymization refers to the process of (data) de-identification that produces data where individual records cannot be linked back to an original /a one-directional (irreversible) process/

3. De-identification and irreversible de-identification

- The de-identification process is required to be of sufficient effectiveness, regardless of whether the recognition attempts are made by humans or by machines.

- In many cases, the process of de-identification is required to preserve the data utility and naturalness

4. Taxonomy of the identifiers in multimedia content

- The Safe Harbour approach:

  18 types of identifiers that have to be de-identified in order to cover the identity of the recipients of health-care services (patients). These are names:

- all geographic subdivisions smaller than a state;
- all elements of dates (except year) for dates directly related to an individual;
- telephone and facsimile numbers;
- electronic-mail addresses;
- social security numbers;
- medical record numbers;
- health-plan beneficiary numbers;
- account numbers;

4. Taxonomy of the identifiers in multimedia content

- certificate/license numbers;
- vehicle identifiers and serial numbers including license-plate numbers;
- device identifiers and serial numbers;
- internet universal resource locators (URLs);
- internet protocol (IP) address numbers;
- biometric identifiers; including fingerprints and voiceprints; full-face photographic images and any comparable images; and
- any other unique identifying number, characteristic, or code, unless otherwise permitted by the *Privacy Rule for re-identification* (hipaa, 2014).

4. Taxonomy of the identifiers in multimedia content

- The identity information extracted from multimedia content can be classified as follows:

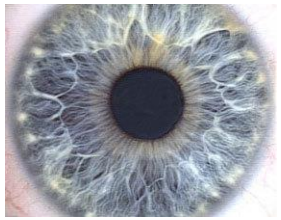
Non-biometric identifiers including text context, speech context, specific socio-political and environmental context, dressing style, and hairstyle;

Biometric identifiers: physiological (face, iris, ear, fingerprint, …), *behavioural* (voice, gait, gesture, lip-motion, stile of typing),

Soft biometric identifiers- characteristic that is not necessarily permanent or distinctive (height, weight, eye colour, silhouette, age, gender, race, moles, tattoos, birthmarks, scars)

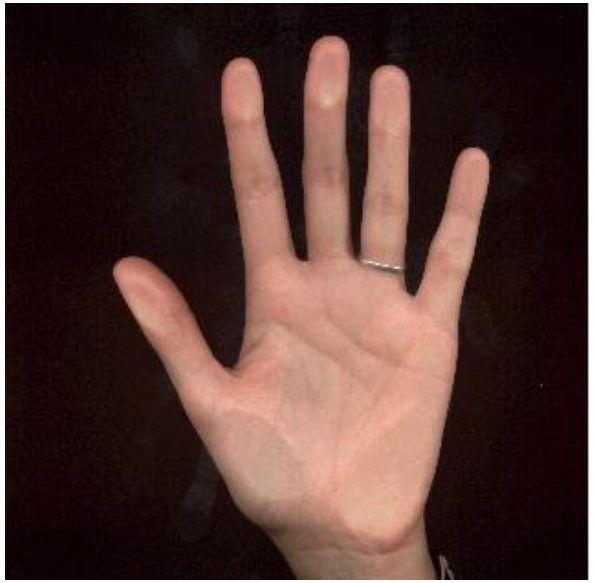
4. Taxonomy of the identifiers in multimedia content

Fingerprint



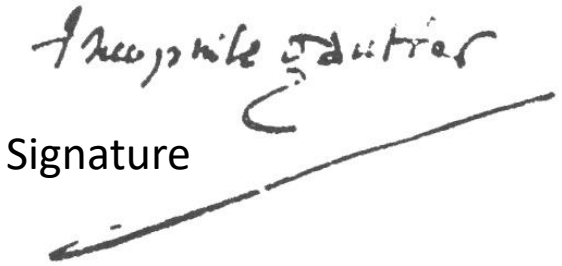
Iris

Face



Hand

Voice



Signature

4. Taxonomy of the identifiers in multimedia content

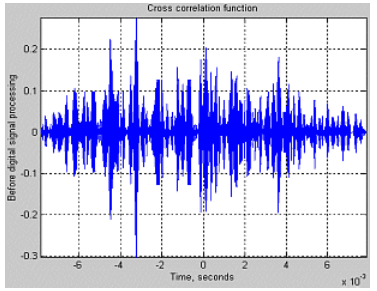
- *Multimodal de-identification*:

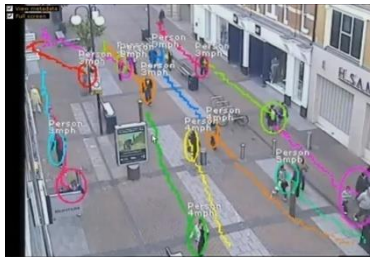
  - in multimedia content there are simultaneously present biometric, soft-biometric and non-biometric identifiers, which all have to be de-identified in order to protect the privacy of individuals.

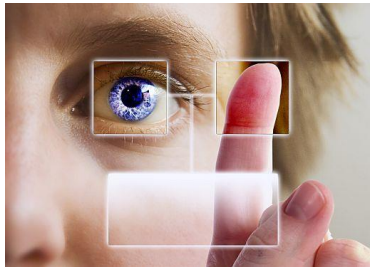
4. Taxonomy of the identifiers in multimedia content

Detecting and concealing or removing or replacing personal identifiers in multimedia content is an interdisciplinary challenge that incorporates such scientific areas as

- natural-language processing,
- text processing,
- image processing,
- pattern recognition,
- machine learning,
- speech analysis,
- video tracking and
- biometrics
- social sciences







5. De-identification of non-biometric identifiers

5.1. Text de-identification

- Research on de-identification was initiated with text-based personal health care records (PHRs)
- The approach in this application area involves the removal of a number of specific categories of information from the text file, and replacing them with realistic surrogate information
- The de-identification methods are based on templates and specialized knowledge of the context for replacing personal health information (PHI) in medical records, or on a complex combination of dictionaries and text-analysis algorithms

5. De-identification of non-biometric identifiers

5.1. Text de-identification (cont.)

- Recently, approaches based on a combination of machine learning, heuristics and statistical methods, as well as pattern-matching are used
- Reversible de-identification is commonly used in the protection of personal data in health-care and biomedical research

5. De-identification of non-biometric identifiers

5.2. Hairstyle and dressing style de-identification

- Hairstyle and dressing style carry identity-revealing information and they can be used to classify people into different categories
- Problem called "a pair-wise constraint":

  - people can determine that two de-identified face portraits in a video belong to the same person by using clothing, dress style or other cues as alternative information, and so there is a risk of exposing a person's identity.

5. De-identification of non-biometric identifiers

5.2. Hairstyle and dressing style de-identification (cont.)

- Alternative information that can be useful for identity revealing includes speech context, specific social and political context, and the environment.

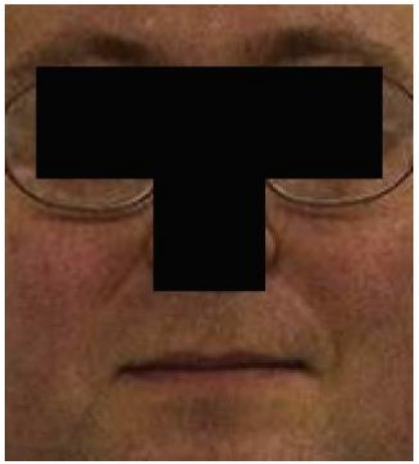
  Relatively little work has been done in the area of removing or hiding such contexts for de-identification purposes

6. De-identification of physiological biometric identifiers

6.1. 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”:

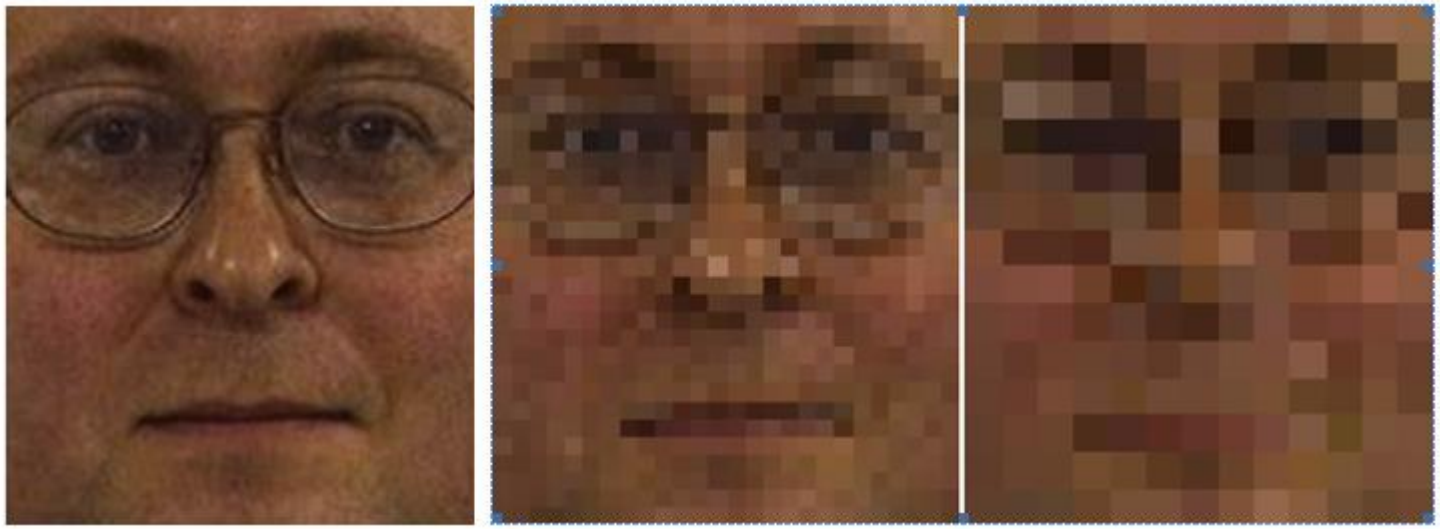
Face region is simply substituted by a black (or white) rectangle, elliptical, circular or T-form covers



6. De-identification of physiological biometric identifiers

6.1. Face de-identification in still images (cont.)

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



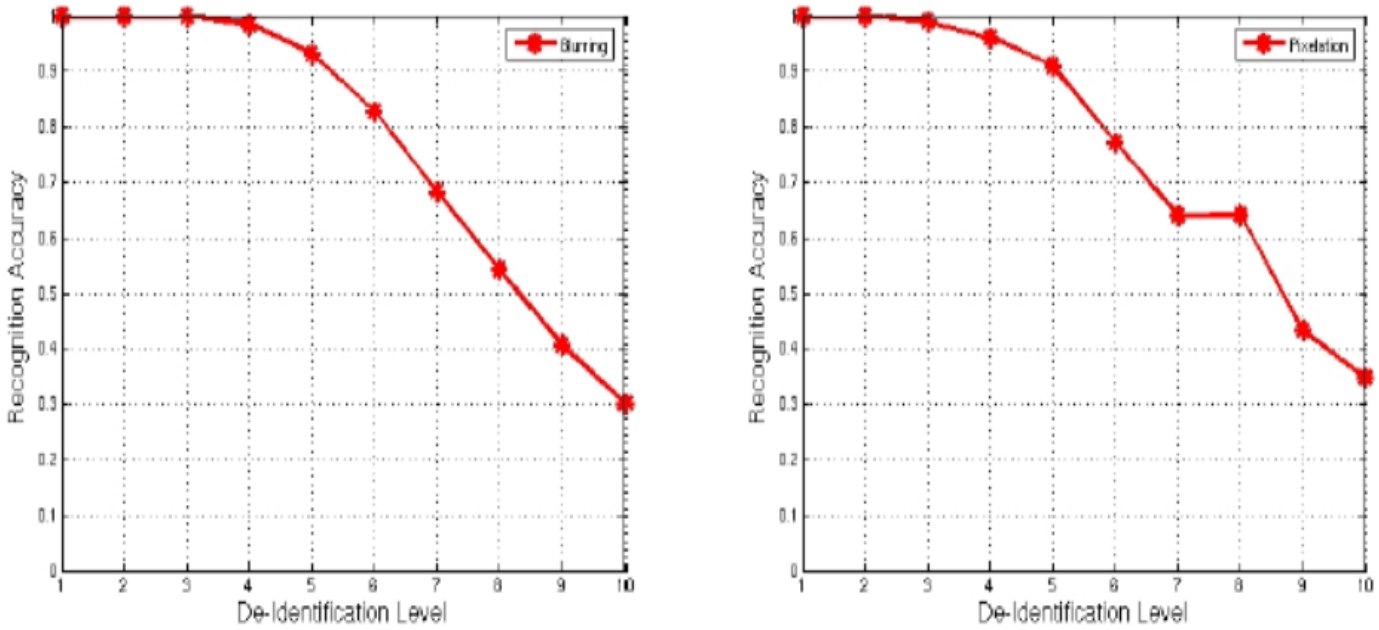
6. De-identification of physiological biometric identifiers

6.1. Face de-identification in still images (cont.)

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

6. De-identification of physiological biometric identifiers

6.1. Face de-identification in still images (cont.)



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

6. De-identification of physiological biometric identifiers

6.1. Face de-identification in still images (cont.)

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

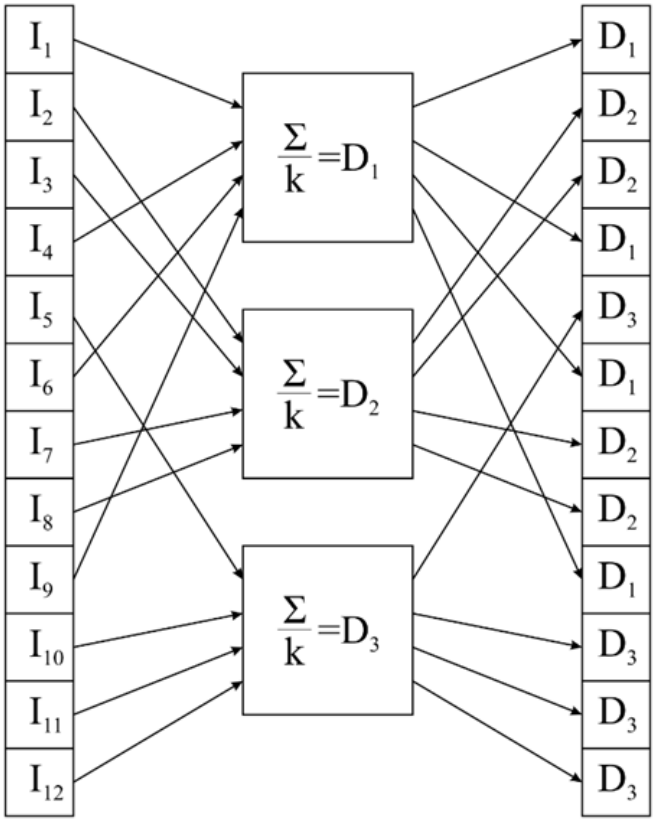
k-Same, k-Same-Select and Model-based k-Same algorithms for face de-identification

6. De-identification of physiological biometric identifiers

6.1. Face de-identification in still images (cont.)

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



6. De-identification of physiological biometric identifiers

6.1. Face de-identification in still images (cont.)

- k-Same algorithm

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

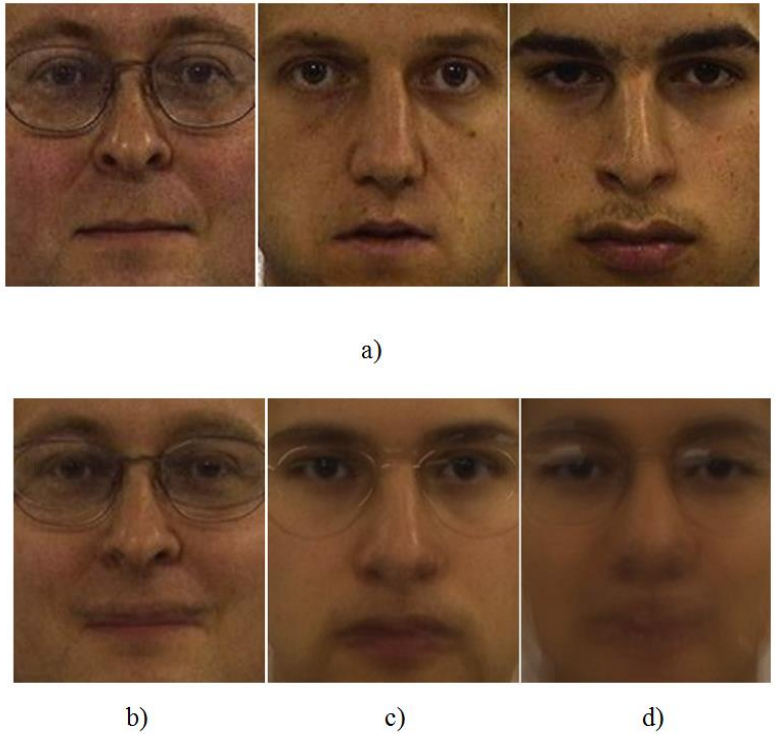
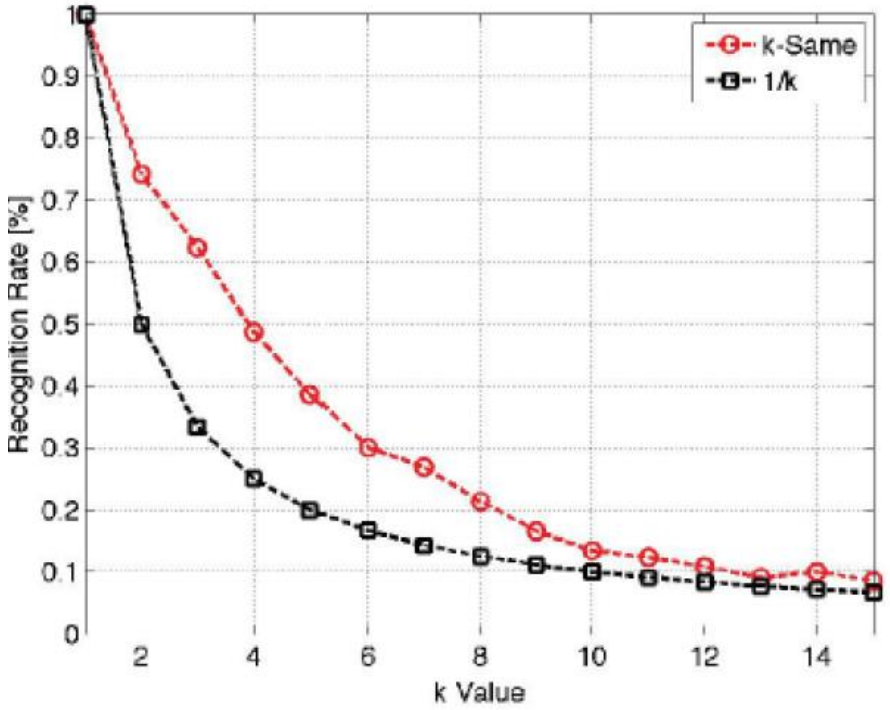


Fig. 4. k-Same de-identification: a) Original images; b) De-identified image for k = 2; c) De-identified image for k = 6; d) De-identified image for k = 20;

6. De-identification of physiological biometric identifiers

6.1. Face de-identification in still images (cont.)



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

6. De-identification of physiological biometric identifiers

6.1. Face de-identification in still images (cont.)

- 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.

6. De-identification of physiological biometric identifiers

6.1. Face de-identification in still images (cont.)

- 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 Active 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)

6. De-identification of physiological biometric identifiers

6.1. Face de-identification in still images (cont.)

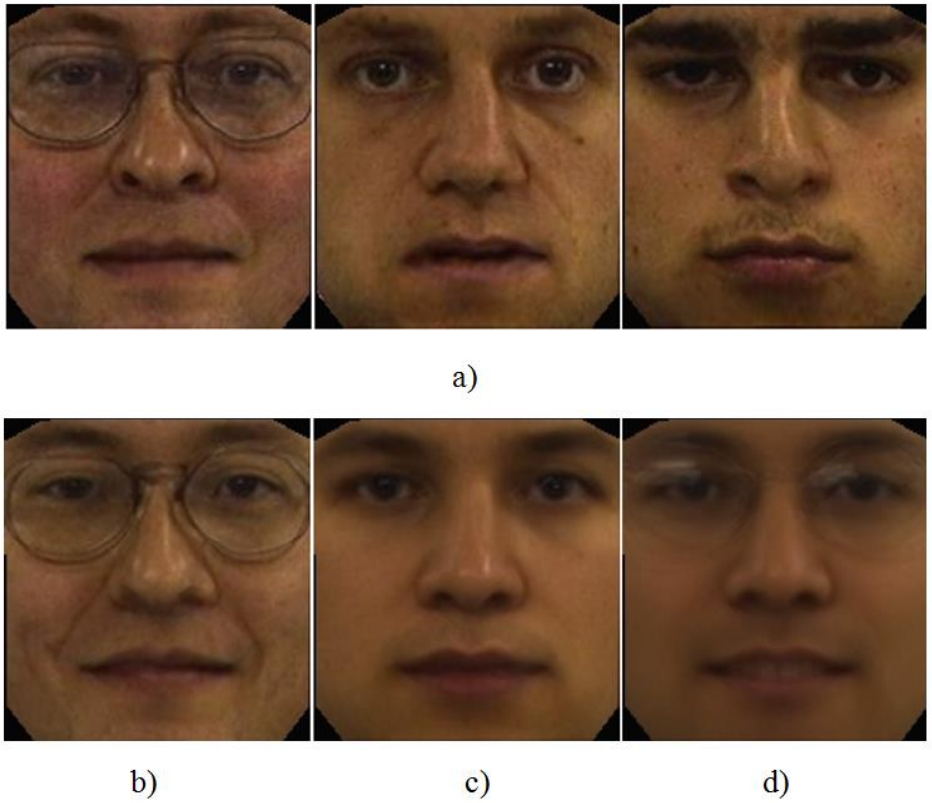


Fig. 5. Model-based k-Same de-identification: a) Original images; b) De-identified image for k = 2; c) De-identified image for k = 6; d) De-identified image for k = 20;

6. De-identification of physiological biometric identifiers

6.2. Face de-identification in videos

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.

6. De-identification of physiological biometric identifiers

6.2. 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

6. De-identification of physiological biometric identifiers

6.2. 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

6. De-identification of physiological biometric identifiers

6.2. Face de-identification in videos

- More recently, new methods have been proposed for face detection, pose estimation and landmark localization in the wild:

- a unified model for face detection, pose estimation and landmark localization using a mixture of trees with a shared pool of part templates (Zhu & Ramanan, 2012),

- the multiple registered image channels are computed using linear and non-linear transformations (e.g. gradient histograms, color (including grayscale, RGB, HSV and CIE-LUV), gradient magnitude, Gabor filters, Difference of Gaussian (DoG) filters) of the input image (Dollár et al., 2009),

- approximation of multi-resolution image features for image pyramid (Dollár et al., 2014),

6. De-identification of physiological biometric identifiers

6.2. Face de-identification in videos

- Face tracking is the process of locating a moving human face (or multiple human faces) in a sequence of frames.
- Tracking is based on :
  - segmented regions
  - skin-colour models
  - local binary patterns (LBP)
  - a combination of LBP and skin-colour information
  - a combination of shape and texture information
  - histogram-based Mean-Shift features
  - Kalman filters and particle filters

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

6. De-identification of physiological biometric identifiers

6.2. 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

6. De-identification of physiological biometric identifiers

6.2. 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):

i) face images are grouped into a person-specific set of images according to their poses

ii) each person-specific set is represented by an active appearance model

iii) raw face image is matched with each of the active appearance models of a person-specific set of images

iv) model with the best matching based on shape and texture is chosen to represent the pose of the raw face image

6. De-identification of physiological biometric identifiers

6.2. Face de-identification in videos

v) from the images in the selected person-specific set of images, one image is chosen to replace the texture of the raw image

vi) 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

6. De-identification of physiological biometric identifiers

6.2. Face de-identification in videos

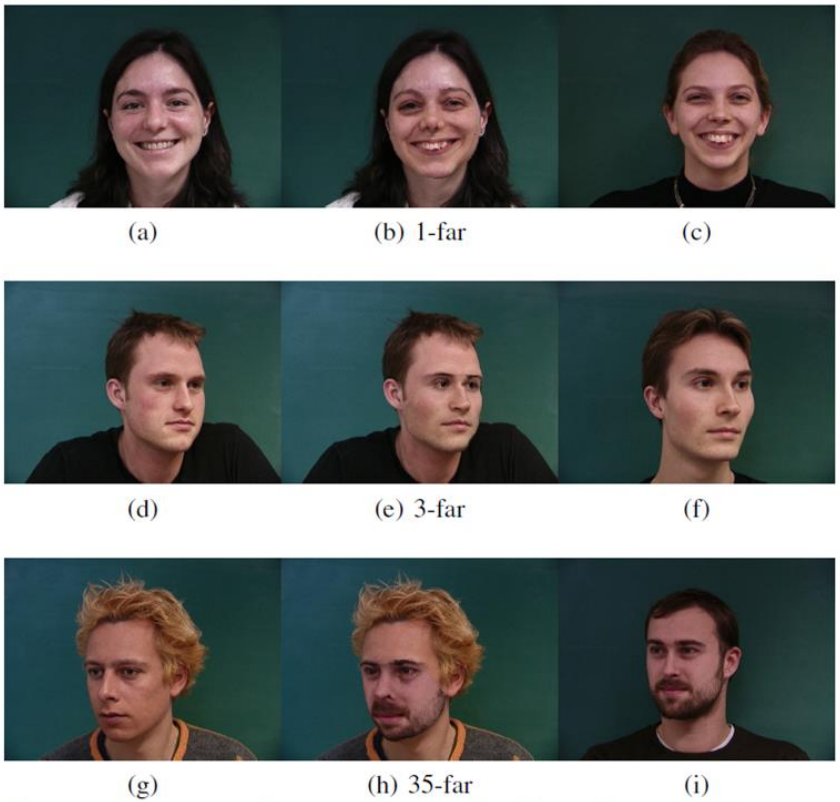


Fig.6. An illustration of the q-far de-identification method [34]. In each row the first image is a raw image (a), (d), (g); The second image is a de-identified image: (b) de-identified with q = 1 distance, (e) de-identified with q = 3, and (h) de-identified with q = 35; The third images in each row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

6. De-identification of physiological biometric identifiers

6.2. 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 ($x \times y \times t$))
- De-identification (exponential blur of pixels in the voxel or line integral convolution)

6. De-identification of physiological biometric identifiers

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

6. De-identification of physiological biometric identifiers

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

6. De-identification of physiological biometric identifiers

6.3. Fingerprint de-identification

- fingerprint recognition is categorized as an *overt biometric* application, i.e. a person is cooperative and aware that he or she is being subjected to recognition
- according the newest reports of ongoing research (technologyreview, 2015), it is possible to detect and acquire fingerprints by shining polarized light onto a person's hand at distance up to two meters

6. De-identification of physiological biometric identifiers

6.3. Fingerprint de-identification

- fingerprints, besides identification information, carry additional private, sensitive information:

- gender
- ethnicity
- diseases such as Huntington's chorea and Parkinson's , Alzheimer's, corneal dystrophy coeliac, and congenital heart disease

3D Imager (touchless)

6. De-identification of physiological biometric identifiers

6.3. Fingerprint de-identification

De-identification:

- procedures such as black box, blurring, pixelation, and replacement by a synthetic fingerprint (Maltoni et al., 2003)
- distortion transforms based on image morphing and /or block scrambling
- feature perturbation and noninvertible feature transform (Ratha et al., 2001)
- based on mixing two fingerprint images in order to generate a new cancellable fingerprint image (Ross, 2014)

6. De-identification of physiological biometric identifiers

6.3. Fingerprint de-identification

- mixing two fingerprint images

a) Original fingerprint

b) Transformation function – fingerprint from a different finger

c) A new mixed fingerprint image

6. De-identification of physiological biometric identifiers

6.3. Fingerprint de-identification

- Method of fingerprint de-identification for gender estimation (Lugini et al., 2014) is based on image filtering in the frequency domain.
- The linear filtering process applies blurring by attenuating the high-frequency content
- Experiments have shown that the gender estimation accuracy on de-identified fingerprint images for 100 users is reduced from the initial 88.7% (original fingerprints) to 50.5%.

6. De-identification of physiological biometric identifiers

6.4. Iris de-identification

- Iris represents an important biometric identifier and it enables an efficient approach to reliable, non-invasive identification of people (Daugman, 2004), (Wildes, 1997)

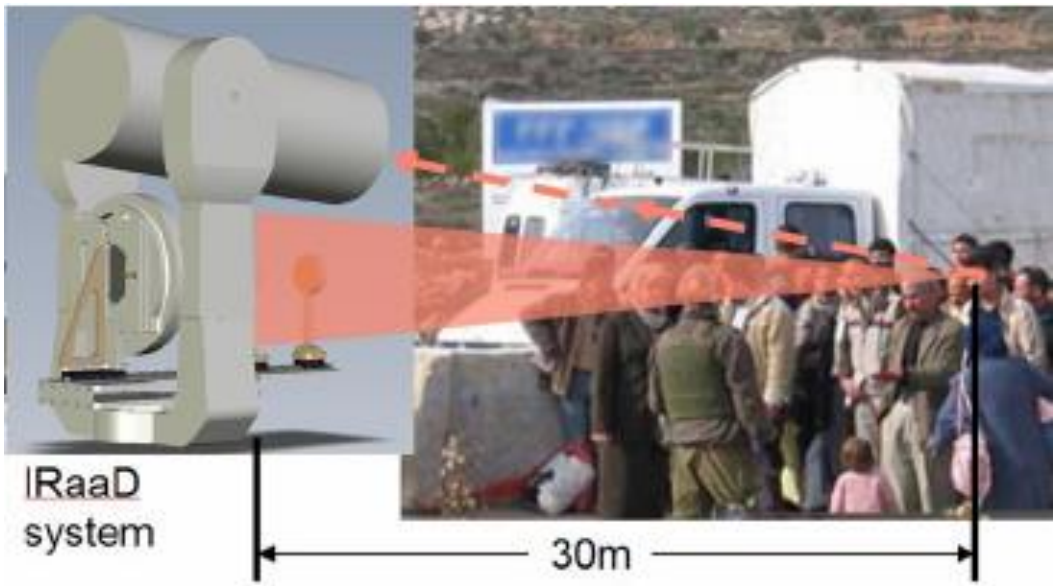
- Most commercial iris-recognition systems operate at a standoff between 0.1 and 0.45 m, with a verification time of 2 to 7 seconds (George & Durai, 2013)

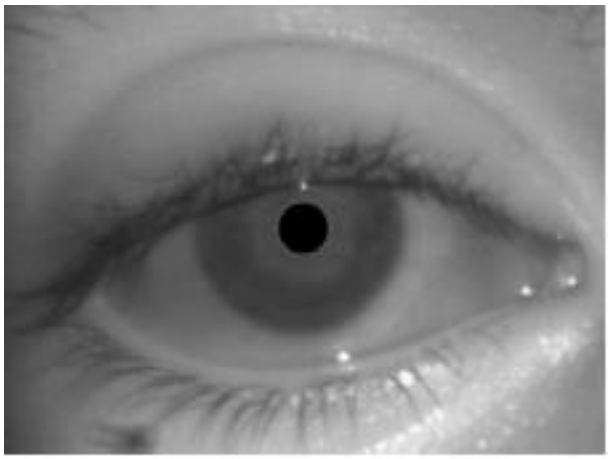
- "the Iris at a Distance (IAD) system" provides the capability to identify a person at a range of more than 1 m in less than a second (morpho, 2014)

6. De-identification of physiological biometric identifiers

6.4. Iris de-identification

- recent iris-recognition technology is capable of acquiring an iris image at 30 m standoff and perform iris recognition (De Villar et al., 2010)





30m iris image with co-located illuminator

6. De-identification of physiological biometric identifiers

6.4. Iris de-identification

- A rare study related to de-identification of the eye areas, and thus the iris, is presented in (Lee & Plataniotis, 2012).
- The proposed system for the reversible de-identification of an eye region consists of two modules:
  - an automatic eye-detection module and
  - a privacy-enabling encoder module

6. De-identification of physiological biometric identifiers

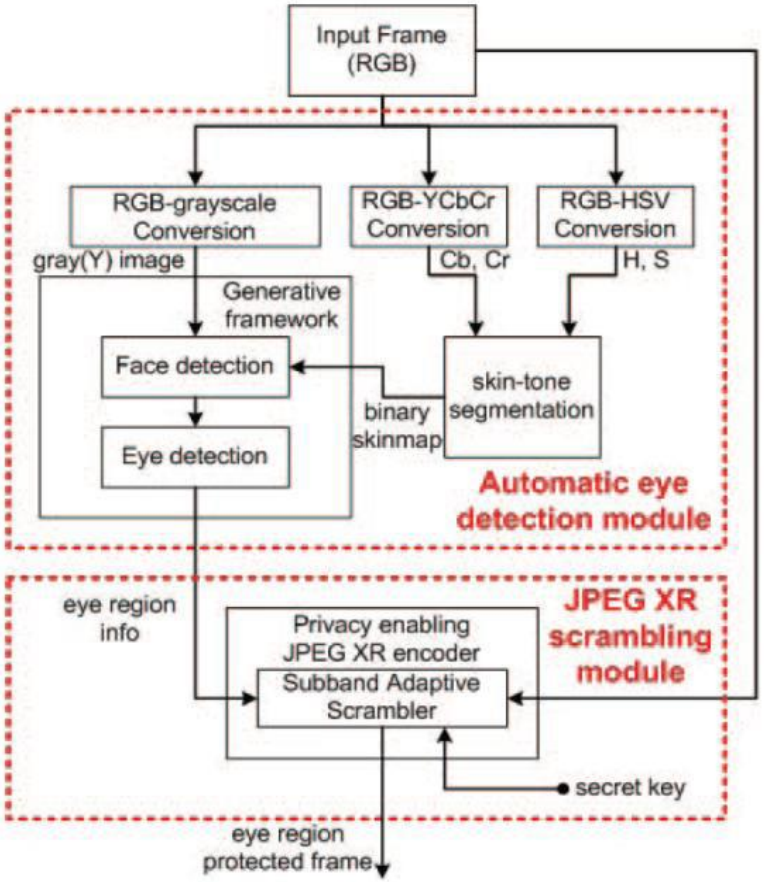
6.4. Iris de-identification

- automatic eye-detection module :

  in real time locates the human-eye region by a combination of colour-based and Haar-like/GentleBoost methods

- privacy-enabling encoder module:

  based on a JPEG XR encoder the macrobloks consisting of 16 × 16 pixels of located eye region are scrambled



6. De-identification of physiological biometric identifiers

6.4. Iris de-identification

- Based on the characteristics of the current iris-recognition systems at a distance, and expected future advances in the field, it can be concluded that iris de-identification for privacy protection is a growing problem.

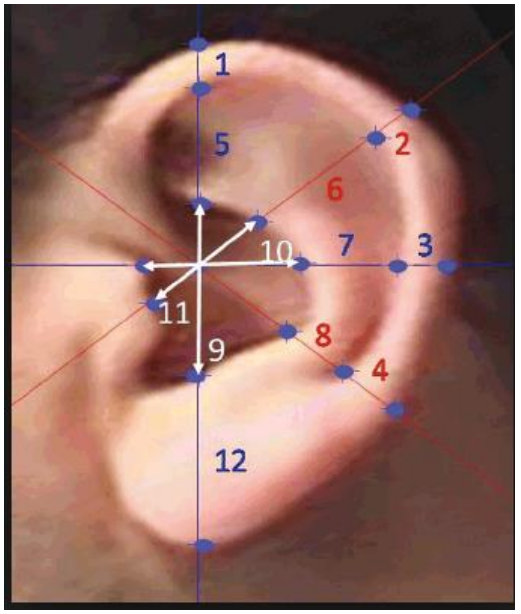
- most IAD systems combine face and iris image acquisition – *multimodal de-identification*

6. De-identification of physiological biometric identifiers

6.5. Ear de-identification

- A number of drawbacks of face and iris identification: head pose, facial expressions , aging, …, high-resolution camera, …

- A human ear is offered as an alternative physiological biometric identifier for non-invasive person identification or verification at a distance



6. De-identification of physiological biometric identifiers

6.5. Ear de-identification

- (Abaza et al., 2013) & (Pflug & Busch, 2012) comprehensive surveys on two-dimensional (2D) and three-dimensional (3D) ear recognition

- ear-based recognition systems also interesting for applications in intelligent video-surveillance systems (Yuan & Mu, 2007), (Kumar et al., 2011), (Abaza et al., 2010)

6. De-identification of physiological biometric identifiers

6.5. Ear de-identification

- there are no existing commercial 2D or 3D ear-based biometric systems for automatic person identification or verification

- it is main reason for lack of research in the field of ear de-identification for privacy protection

- In the near future, due to the development of relatively low-cost, high-resolution, video cameras and telescopic equipment, we can expect ear-based recognition and tracking in semi- or non-controlled outdoors conditions

- Most ear-recognition systems use a combination of a profile face and ear detection ---- *multimodal de-identification problem*

7. De-identification of behavioural biometric identifiers

7.1. Voice de-identification

- biometric identifiers as the face, iris and ear refer to *the visual identity of a person*

- a person has *an audio identity* - voice, speech signal

- speech signal carries privacy-sensitive information such as gender, age, emotional state and the identity of the speaker

- Applications and services such as audio-video surveillance, speech-based services, life-log systems and telephone-based services enable person identification based on voice, and therefore flag the importance of privacy protection

7. De-identification of behavioural biometric identifiers

7.1. Voice de-identification

- Voice de-identification is based on the principles of voice transformation (VT)

- Voice transformation refers to modifications of the non-linguistic characteristics of a given utterance without affecting its textual content

- The non-linguistic information of speech signals, such as voice quality and voice individuality, may be controlled by VT (Stylianou, 2009)

7. De-identification of behavioural biometric identifiers

7.1. Voice de-identification

VT is based on three types of voice modifications (Muda et al., 2010): source, filter and their combination

- Source modifications: time-scale, pitch and energy modifications

- Filter modification - a modification that changes the magnitude response of the vocal tract system

A special VT: Voice conversion (Sundermann, 2005), (Abe et al., 1988), (Upperman, 2014) - the characteristics of a source speaker's voice are mapped to those of a specific (target) speaker

7. De-identification of behavioural biometric identifiers

7.1. Voice de-identification

- Voice de-identification for the privacy protection of life-log video (Chaudhari, 2007a), (Chaudhari et al., 2007b) is based on voice distortion by altering the pitch by the Pitch-Scale Synchronous Overlap and Add (PitchScale SOLA) method

  The distortion is accomplished in two steps:

  - time stretching the audio signal

  - re-sampling it to obtain the original length

7. De-identification of behavioural biometric identifiers

7.1. Voice de-identification

- In (Jin et al., 2009a) the authors propose a transformation of the speaker's voice

  - strategy for de-identifying that results in the speech of various speakers to be transformed to the same synthetic (target) voice

  - use Gaussian Mixture Model (GMM)-mapping based VT to convert a relatively small set of source speakers (24 males) to a syntactic voice

7. De-identification of behavioural biometric identifiers

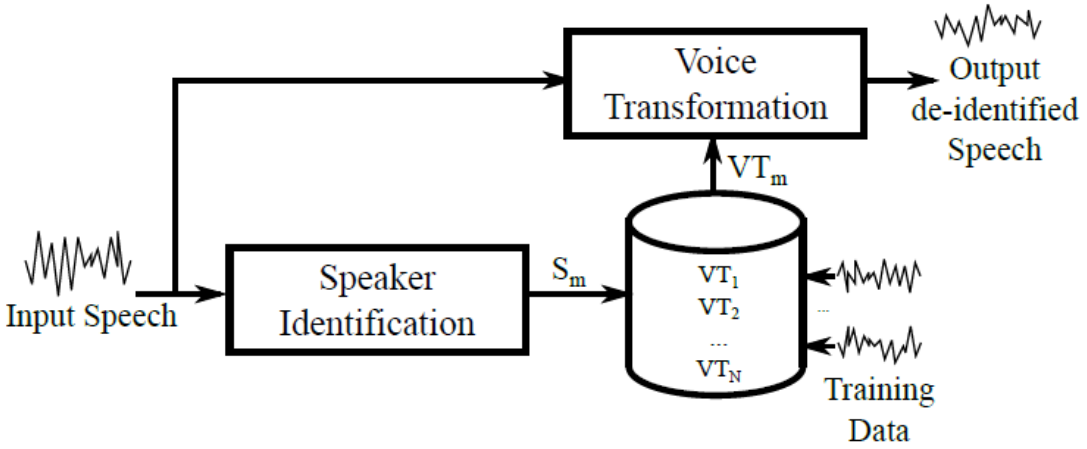
7.1. Voice de-identification

- A novel scheme for voice de-identification, where a set of pre-calculated voice transformations based on GMM mapping is used to de-identify the speech of a new speaker, is presented in (Pobar & Ipsic, 2014)

- inspired by an approach that is used for face de-identification (e.g., *k-Same)*

7. De-identification of behavioural biometric identifiers

7.1. Voice de-identification



The scheme uses automatic voice identification within the set that is used to build pre-calculated voice transformations to select the appropriate transform, which is then used to de-identify the speech of the new user

7. De-identification of behavioural biometric identifiers

7.1. Voice de-identification

There are several challenges in the field of online voice de-identification:

- de-identification in an environment with background noise

- voice de-identification in situations where there are multiple individuals speaking at various times

7. De-identification of behavioural biometric identifiers

7.2. Gait and gesture de-identification

- Gait - a manner of walking
- Represents a behavioural biometric characteristic
- Gait, as a body gesture, which is usually a motion without meaning- information that can be used for person identification
- Gait includes information about individual appearance, such as silhouette, leg length, height, even age, and gender (Yoo et al., 2005), (Lee & Grimson, 2002)
- it is possible to recognize non-cooperating individuals at a distance based on their walking characteristics

7. De-identification of behavioural biometric identifiers

7.2. Gait and gesture de-identification

- Based on the state of the art for gait recognition systems, their characteristics and performances - gait-based technologies can be used for biometric-based person verification in controlled environments

- Very few studies have been directly geared towards gait de-identification

- The study in (Baaziz et al., 2007) presents an automated video-surveillance system designed to ensure the efficient and selective storage of data, to provide a means for enhancing privacy protection

7. De-identification of behavioural biometric identifiers

7.2. Gait and gesture de-identification

- The approach to the privacy enhancement of captured video sequences is based on two main steps:

  - salient motion detector, which finds regions of interest (corresponding mainly to moving individuals), and

  - the second step applies to those regions with a procedure of information concealment based on a scrambling technique described in (Dufaux & Ebrahimi, 2010).

7. De-identification of behavioural biometric identifiers

7.2. Gait and gesture de-identification

An illustration result of the scrambling method (Dufaux & Ebrahimi, 2008)

7. De-identification of behavioural biometric identifiers

7.2. Gait and gesture de-identification

- In (Agrawal, 2010), (Agrawal & Narayanan, 2011) gait de-identification, based on two de-identification transformations, i.e. the exponential blur of pixels of the voxel and line integral convolution (LIC) is proposed

- These two kinds of smooth temporal blurring of the space-time boundaries of an individual aim to remove any gait information

7. De-identification of behavioural biometric identifiers

7.2. Gait and gesture de-identification

A main problem with gait de-identification in a video-surveillance system:

- how to obscure the characteristics of individuals' walking patterns, and at the same time preserve the usability and naturalness of the de-identified video

7. De-identification of behavioural biometric identifiers

7.2. Gait and gesture de-identification

Gestures - the movement of a body part (fingers, hands, arms, head, or face) or a whole body that is made with or without the intension meaning something (Mitra & Acharya, 2007), (Abdallah et al., 2012)

- To date, there have only been a few attempts to develop biometric verification systems based on *hand-gesture recognition (Lentsoane et al., 2006), (Lentsoane, 2007), (Fong et al., 2013), (Osada et al., 2000), (Yang et al., 2013)*

7. De-identification of behavioural biometric identifiers

7.2. Gait and gesture de-identification

As far as we know, there has been no research into the problem of hand gesture de-identification

The problem of gesture de-identification in video surveillance is similar to the problem of gait de-identification and can be solved by approaches similar to those used for gait.

8. De-identification of soft biometric identifiers

Soft biometric identifiers (SBIs) are physical, behavioural or adhered human characteristics of the person that provide some information about the person, but lack the distinctiveness and permanence to sufficiently differentiate any two persons (Jain et al., 2004)

- two advantages of SBIs compared to the biometric identifiers:

i) SBIs bridge the semantic gap between biometric identification and human descriptions of the identifiers

ii) SBIs can be collected at a distance by low-resolution sensors and do not require cooperative individuals, so they are ideal in surveillance applications

8. De-identification of soft biometric identifiers

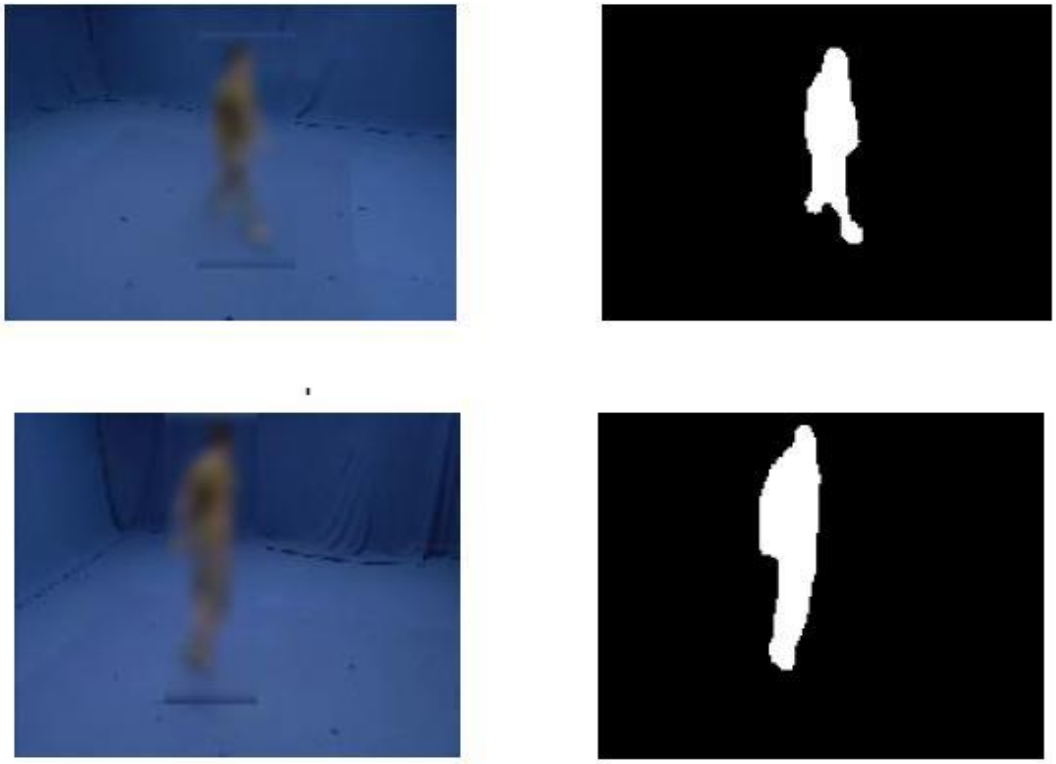
8.1. Body silhouette de-identification

- The body silhouette is an important soft biometric identifier and it can help the recognition process

- There are only a few papers on *silhouette de-identification. In (Agrawal, 2010), (Agrawal & Narayanan, 2011)* - masking of a silhouette is relatively easy, through the use of dilatation or Gaussian blurring

8. De-identification of soft biometric identifiers

8.1. Body silhouette de-identification



De-identification of individuals in activity videos (Ivasic-Kos et al., 2014)

8. De-identification of soft biometric identifiers

8.1. Body silhouette de-identification

- An interesting approach to silhouette de-identification is described in (Nodari et al., 2012); it involves replacing a person with another one from a dataset gallery

8. De-identification of soft biometric identifiers

8.2. Gender, age, race and ethnicity de-identification

- there are many papers related to the automatic recognition of *gender*, *age*, *race* and *ethnicity*
- relatively little is done on their de-identification in multimedia content

8. De-identification of soft biometric identifiers

8.3. Scars, marks and tattoos (SMT) de-identification

- Scars, marks and tattoos (SMT) are imprints on skin that provide more discriminative information than age, height, gender, and race to identify a person (Lee et al., 2008)

- In (Jain & Park, 2009) the authors have showed that facial marks, such as freckles, moles, scars and pockmarks can improve automatic face recognition and retrieval performance

8. De-identification of soft biometric identifiers

8.3. Scars, marks and tattoos (SMT) de-identification

Tattoos are not only popular in particular groups, such as motorcyclists, sailors, and members of criminal gangs, they have become very popular in the wider population

- Tattoos are primarily used for content-based image retrieval (CBIR) in law-enforcement applications (Manger, 2012), (Lee et al., 2011)

- based on the visual appearance of tattoos and their location on a body (Laumann & Derick, 2006), they can be used for person recognition, as well as for suspect and victim identification in forensics

8. De-identification of soft biometric identifiers

8.3. Scars, marks and tattoos (SMT) de-identification

Tattoos are not only popular in particular groups, such as motorcyclists, sailors, and members of criminal gangs, they have become very popular in the wider population

- Tattoos are primarily used for content-based image retrieval (CBIR) in law-enforcement applications (Manger, 2012), (Lee et al., 2011)
- based on the visual appearance of tattoos and their location on a body (Laumann & Derick, 2006), they can be used for person recognition, as well as for suspect and victim identification in forensics

8. De-identification of soft biometric identifiers

8.3. Scars, marks and tattoos (SMT) de-identification

- The main features used for tattoo recognition are Scale Invariant Feature Transform (SIFT) features (Lee et al., 2008), (Heflin et al., 2012), (Acton & Rossi, 2008), active contours and so-called glocal features – local features that contain global information regarding colour and edge orientation (Acton & Rossi, 2008).

- There are no published papers related to SMT de-identification, except (Marcetic et al., 2014).

8. De-identification of soft biometric identifiers

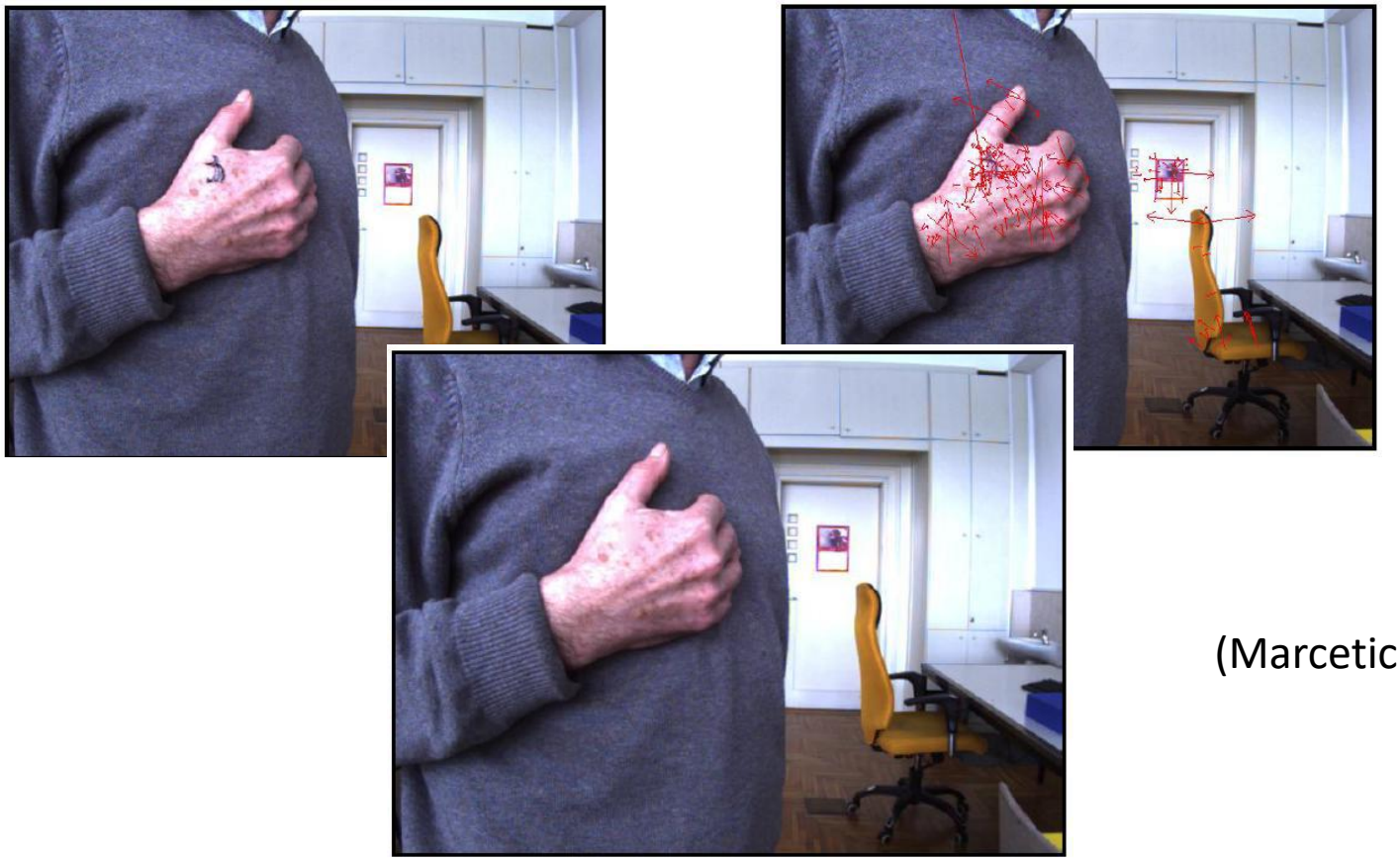
8.3. Scars, marks and tattoos (SMT) de-identification

The tattoo de-identification system consists of the following modules:

- skin and region-of-interest (ROI) detection,
- feature extraction (SIFT features are extracted from a ROI),
- tattoo database (each tattoo in the tattoo database has an average of 56 template SIFT features),
- matching (SIFT features are matched with template SIFT features) ,
- tattoo detection,
- skin swapping (the original tattoo's region is replaced by pixels from a surrounding, non-tattoo region) , and
- quality evaluation.

8. De-identification of soft biometric identifiers

8.3. Scars, marks and tattoos (SMT) de-identification



(Marcetic et al., 2014)

9. Conclusion

- Privacy is one of the most important social and political issues in any free society
- Research in the field of de-identification in multimedia content is still in its infancy
- Relatively little has been done in the field of de-identification of non-biometric identifiers, except in the field of text de-identification
- There are unsolved problems of de-identification of hairstyle and dressing style to avoid "a pair-wise constraint", as well as the de-identification of physiological and behavioural biometric identifiers in combination with the specific social, political and environmental contexts

9. Conclusion

- in the field of de-identification of biometric identifiers, there are many open problems, such as real-time detection, localization, tracking and removing or hiding of physiological biometric identifiers
- These problems are particularly emphasized for videos of crowded scenes
- there is not yet a complete solution for speaker de-identification and speaker tracking in situations where multiple individuals are speaking simultaneously or at various times

9. Conclusion

Some open questions and challenges:

- How does the combination of non-biometric, biometric and soft-biometric information, simultaneously present in data, influence de-identification methods?

- What are the metrics in measuring privacy protection in multimedia content, utility and the naturalness of de-identified data?

- Which de-identification methods are applicable in real-time?

Acknowledgment

This work has been supported by the Croatian Science Foundation under project 6733 De-identification for Privacy Protection in Surveillance Systems (DePPSS). It is also the result of activities in COST Action IC1206 “De-identification for Privacy Protection in Multimedia Content”.

Thank you for your attention