De-identification for Privacy Protection – COST Action IC1206 Objectives and Achievements

De-Identification for Privacy Protection in Multimedia Content

Prof. Slobodan Ribarić
University of Zagreb
Faculty of Electrical Engineering and Computing

hrzz
Croatian Science Foundation

SPLINE 2016 Aalborg

Outline

1. Action presentation
2. Main objectives of the Action
3. Privacy, multimedia, de-identification
4. Taxonomy of personal identifiers
5. De-identification of non-biometric identifiers
6. De-identification of physiological biometric identifiers
7. De-identification of behavioral biometric identifiers
8. De-identification of soft biometric identifiers
9. Conclusion

1. Action presentation

IC 1206 COST Action

De-identification for privacy protection in multimedia content

http://www.cost.eu/COST_Actions/ict/IC1206

http://costic1206.uvigo.es/

Chair: Prof. Slobodan Ribarić, University of Zagreb, Croatia

Co-chair: Prof. Carmen Garcia Mateo, Universidad de Vigo, Spain

Action Start Date: 2013-03-26

Action End Date: 2017-03-25

De-Identification for Privacy Protection in Multimedia Content

1. Action presentation

International cooperation

- 28 Cost Countries

De-Identification for Privacy Protection in Multimedia Content

1. AT 08/04/2013	11. EL 26/02/2013	21. RS 24/04/2013
2. BE 26/03/2013	12. HU 07/10/2013	22. SK 08/08/2013
3. BA 12/03/2013	13. IE 24/11/2014	23. SI 25/03/2013
4. HR 14/12/2012	14. IL 09/10/2013	24. ES 30/11/2012
5. CY 13/02/2013	15. IT 29/01/2013	25. CH 01/03/2013
6. CZ 27/02/2013	16. MT 19/12/2012	26. TR 10/04/2013
7. DK 19/12/2012	17.NL 02/07/2013	27. UK 27/11/2012
8. FI 14/01/2013	18. NO 29/05/2013	28. MK 25/12/2012
9. FR 22/01/2013	19. PL 14/12/2012	
10. DE 17/01/2013	20. PT 11/01/2013	

1. Action presentation

- 3 International Partner Countries

USA:

Carnegie Mellon University

(West Virginia University)

University of North Carolina at Charlotte

China:

Institute of Automation, Chinese Academy of Science

Argentina:

CONICET, Buenos Aires

- 1 International Partner Country

Belarus:

Yanka Kupala State University of Grodno

1. Action presentation

- **WG1:** De-identification methods for biometric identifiers (Isabel Trancoso, Portugal)
- **WG2:** De-identification methods for soft- and non-biometric identifiers (Zheng-Hua Tan, Denmark)
- **WG3:** Applications and added value of de-identified data (Jean-François Bonastre, France)
- **WG4:** Ethical, bioethical, societal and legal aspects and guidelines for de-identification and reversible de-identification (Alexin Zoltán, Hungary)

- More then 160 experts, ESRs and PhD students

1. Action presentation

- MC Committee: 45 members
- MC Core Group: 6 members (chair, vice-chair, chairs of working groups)
- STSM Committee: 3 members (Patrizio Campisi, Italy)

2. Main objectives of the Action

(i) To establish mechanisms for sharing knowledge and technology among experts in different (usually complementary) fields related to automated de-identification and reversible de-identification

(ii) To provide innovative solutions for concealing, or removal of identifiers while preserving data utility and/or naturalness

(iii) To investigate reversible de-identification and to provide a thorough analysis of security risks of reversible de-identification.

(iv) To provide a detailed analysis of legal, ethical and social repercussion of reversible/non-reversible de-identification.

3. Privacy, multimedia, de-identification

- **There is no single definition of the term “privacy”**

  - depends of legal, political, societal, cultural and socio-technological context

  - S. D. Warren and L. D. Brandeis (1890) “the right to let alone” with respect to the acquisition and dissemination of personal information

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

3.Privacy, multimedia, de-identification

- **Depending on the social contexts, real life situations and socio-technological contexts:**

1. information privacy (rules governing the collection and handling of personal data such as medical and tax records and credit information)
2. privacy of communications (security and privacy of mail, telephone, e-mail)
3. bodily privacy (protection of people's physical selves against invasive procedures such as genetic tests, drug testing and cavity searches)
4. territorial privacy (the setting of limits on intrusion into domestic and other environments, such as the workplace or public space, this includes searches, video surveillance and ID checks)

3. Privacy, multimedia, de-identification

- **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.

3. Privacy, multimedia, de-identification

- **Technologies and services which can potentially provide the means for privacy intrusion:**

  - Communications, multimedia, biometrics, big data , cloud computing, data mining, internet, social networks, audio-video surveillance, drones equipped with camera

  - Over 4 million CCTV cameras in the UK

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

  - Over 80% of the CCTV systems deployed in London's business space do not work according to relevant data-protecton legislation

3. Privacy, multimedia, de-identification

- Technologies like “Google Street View” and “EveryScape” provide an additional framework for the invasion of the individuals’ privacy

- Special attention needs to be given to develop de-identification technologies for Internet sites, and predominately social networks (Facebook, YouTube, Twitter)

3. Privacy, multimedia, de-identification

- **Multimedia contents** - text, still images, audio and video sequences and their combinations.

- **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. Privacy, multimedia, de-identification

- **De-identification and irreversible de-identification**
- De-identification – the reversible process of removing or obscuring any personally identifiable information (additional information enables the extraction of the original identifiers)
- Irreversible de-identification (anonymization) – one directional process
- Multimodal de-identification

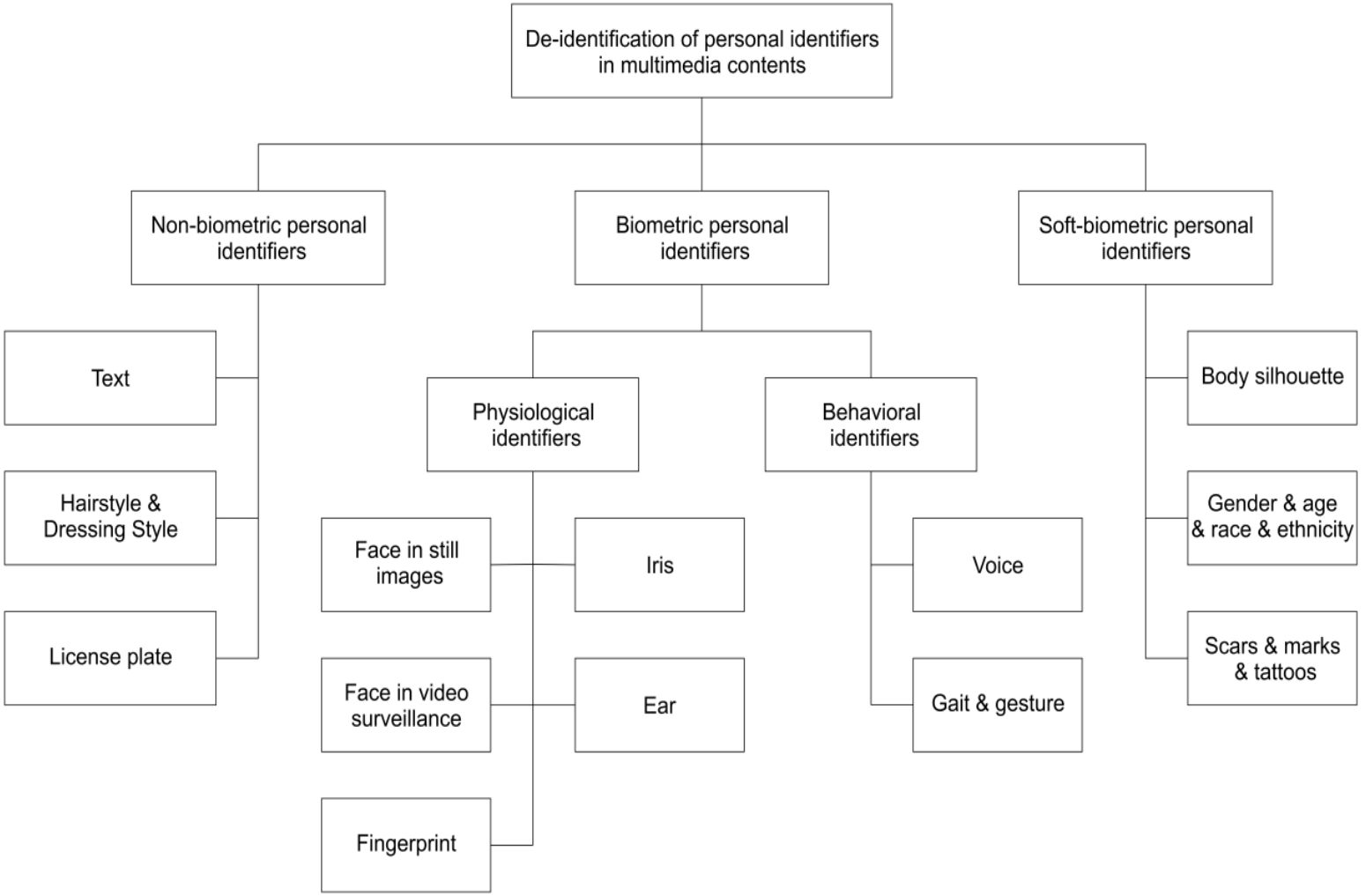
4. Taxonomy of personal identifiers

- **Personal identifiers – personal information, which allow his or her identification**

Safe Harbour approach:

18 types of identifiers (names - all geographical subdivisions smallerthan state, 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; 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.

4. Taxonomy of personal identifiers



5. De-identification of non-biometric identifiers

5.1 Text de-identification

- De-identification was initiated with text-based personal healthcare records (PHRs)
- Automated de-identification of text-based PHRs is focused on:
  i) highly-structured type-specific records and/or
  ii) free-text medical records with a highly variable structure

Reversible de-identification is commonly used in PHRs (Fraser, D. Willison, 2009), (Garfinkel, 2015).

5. De-identification of non-biometric identifiers

5.1 Text de-identification (cont.)

Approaches based on a combination of machine learning, heuristics and statistical methods, and pattern-matching

- De-identification of medical databases (Alexin, 2014)

- Text mining of patient records preserving patient anonymity (Dalianis, 2015)
/Presentation on COST IC1206 Autumn School, October 7-11, 2015, Limassol, Cyprus/

5. De-identification of non-biometric identifiers

5.2 Hairstyle and dressing style de-identification

• Hairstyle and dressing style carry identity-revealing information

- problem "a pair-wise constraint" identification

Relatively little research work has been done in the area of removing or hiding hairstyle and dressing style, and contexts for de-identification purposes

- pioneering efforts have been made only to conceal hairstyles and hair colour (Prinosil et al., 2015)

5. De-identification of non-biometric identifiers

5.3 License plate de-identification

• Web services (Google Street View ,EveryScape) systematically gather and share large-scale images of public places
• Privacy sensitive information: faces of individuals and car license numbers on license plates

• Detection of faces and license plates in Google Street View and blurring the detected locations (Frome et al. 2009)

• Method named inhomogeneous principal component blur (IPCB) - adaptively blurs different pixels of a license plate (Du, Ling, 2011)

6. De-identification of physiological biometric identifiers

6.1 Face de-identification in still images

Face - the main physiological biometric identifier in multimedia content

- Ad-hoc (naive) approaches such as "black box", “blurring” and “pixelation”


original

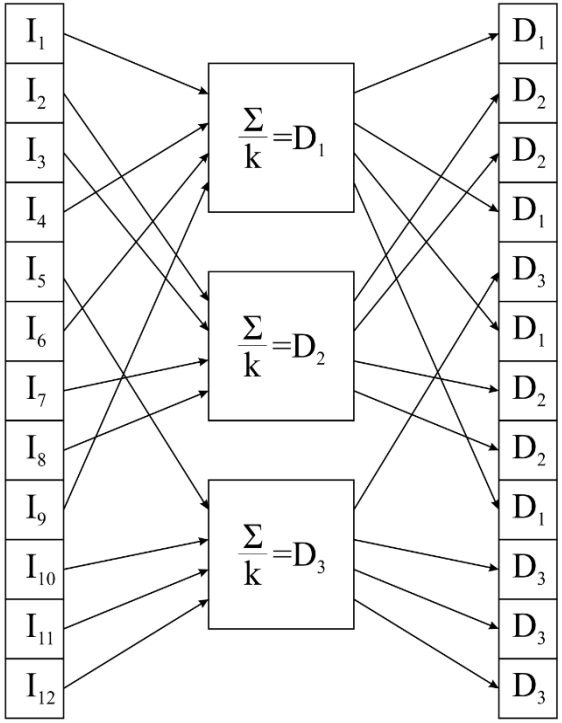

blurring


pixelation

- An effective approach that subverts naive de-identification methods is called *parrot recognition (*Gross, et al.,2006)

6. De-identification of physiological biometric identifiers

- **More sophisticated approaches have been proposed:**
  - eigenvector-based de-identification method
  - *k-Same*, *k-Same-Select* and *Model-based k-Same* (Gross et al. 2009)



I - a person-specific set of face images
D - a set of de-identified face images
∑ - 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.)

- Retaining expressions on de-identified faces (Meng et al. 2014)

- A reversible privacy-preserving photo sharing architecture which ensures privacy and preserves the usability and convenience of online photo sharing (Yuan, Korshunov, Ebrahimi, 2015):
  - Visual privacy in a JPEG can be protected by using:
    (i) naive de-identification
    (ii) scrambling
- A morphing-based and warping visual privacy protection methods (Korshunov, Ebrahimi, 2013)

6. De-identification of physiological biometric identifiers

6.2 Face de-identification in video surveillance systems

- De-identification of the face in video surveillance systems is far from a complete solution
- Problem in computer vision algorithms for the robust detection and localization of face(s) in video sequences

Face de-identification based on:

- privacy filters based on simple approaches such as masking, blurring, pixelation, warping and morphing

- a cartooning privacy filter - which converts raw images into abstracted frames (Erdely, et al., 2014)

- scrambling methods for video coding standard H.264/AVC (Dufaux, Ebrahimi, 2008)

6. De-identification of physiological biometric identifiers

6.2 Face de-identification in video surveillance systems (cont.)

- q-far de-identification method (Samarzija, Ribaric, 2014)

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

Original | De-identified face | Image used for the face swapping

6. De-identification of physiological biometric identifiers

6.3 De-identification in drone-based surveillance systems

- Little has been done on the technical aspects of privacy protection for mini drone-based surveillance scenarios
- Open problems in the detection of several ROIs (face, body silhouette, accessories, different positions and sizes) in dynamic scenes – MCMO
- Problem of drone-based surveillance and its effects on privacy, from the ethical and legal aspects (Wilson, 2014), (Cavoukian, 2012)
- Application of the privacy filters (blurring, pixelation, masking, morphing and warping) (Bonetto et al., 2015)

  - For an assessment of the trade-off between privacy protection and the intelligibility of the de-identified videos - crowdsourcing approach

6. De-identification of physiological biometric identifiers

6.4 Fingerprint de-identification

- Fingerprints, besides identification information, carry additional private, sensitive information (gender, ethnicity,) diseases
- De-identification with the usual de-identification procedures such as black box, blurring, pixelation, replacement by a synthetic fingerprint or by applying privacy filters
- Privacy protection by using a binary thinned fingerprint image (Sheng, Kot, 2010) or mixing two fingerprint images in order to generate a new cancellable fingerprint image (Ross, 2014)

Original

Transformation function

A new mixed fingerprint image

6. De-identification of physiological biometric identifiers

6. 4 Fingerprint de-identification (cont.)

- Fingerprint de-identification for gender estimation based on image filtering in the frequency domain (Lugini, Marasco, Cukic, Dawson, 2014)

Experiments have shown that the gender estimation accuracy in 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

6.5 Iris de-identification

- Iris at a Distance (IAD) systems - capable of acquiring an iris image at 30 metres (!!) standoff and perform iris recognition

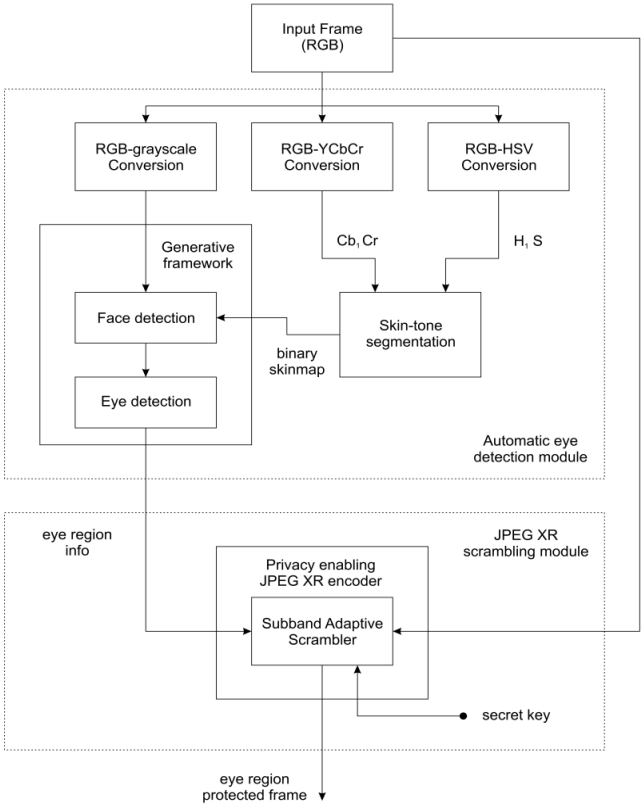
- There is no activity regarding the iris de-identification in COST Action IC1206

The IAD prototype system (De Villar, Ives, Matey, 2010)

6. De-identification of physiological biometric identifiers

6.5 Iris de-identification (cont.)

- De-identification of the eye areas by scrambling (Lee, Plataniotis, 2012)



6. De-identification of physiological biometric identifiers

6.6 Ear de-identification

- 2D ear image can be easily acquired from a distance, even without the cooperation of the subject - applications in intelligent video-surveillance systems

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

  - There is no activity regarding the ear de-identification in COST Action IC1206

  - Multimodal de-identification (ear & face)

7. De-identification of behavioural biometric identifiers

7.1 Voice de-identification

- *visual identity* vs. *audio identity*
- The speech signal carries privacy-sensitive information: gender, age, emotional state, health status, level of education, origin and the identity of the speaker
- *Voice de-identification* is based on the principles of voice transformation (VT) - modifications of the non-linguistic characteristics of a given utterance without affecting its textual content (Schultz et al., 2013)
- 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 (Pobar, Ipsic, 2014)

7. De-identification of behavioural biometric identifiers

7.1 Voice de-identification (cont.)

- Speaker De-identification using Diphone Recognition and Speech Synthesis (Justin et al., 2014)

De-identification is performed in two steps:

(i) the input speech is recognized with a diphone-based recognition system and converted into phonetic transcription

(ii) phonetic transcription is used by a speech synthesis subsystem to produce a new speech

7. De-identification of behavioural biometric identifiers

7. 2 Gait and gesture de-identification

- Very few studies have been directly geared towards gait de-identification
- Gait de-identification based on two de-identification transformations (line integral convolution (LIC) and temporal blurring of the space-time boundaries) (Agrawal, Narayanan, 2011)
- There is no activity regarding the gait and gesture de-identification in COST Action IC1206

8. De-identification of soft biometric identifiers

8.1 Body silhouette de-identification

De-identification based on the Gaussian blurring of the silhouette

- de-identification of individuals in activity videos (Ivasic-Kos, Iosifidis, Tefas, Pitas, 2014)

a) b)

De-identification of individuals in activity videos depicting:
a) walking; b) jumping in place actions after 2D Gaussian filtering

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
- Information about *gender*, *age*, *race* and *ethnicity* is obtained from facial images and/or a speaker utterance, gait and silhouette and silhouetted face profiles – multimodal de-identification
- Masking of race and gender is a difficult problem (Agrawal, Narayanan, 2011) - naturalness of the de-identified videos?

8. De-identification of soft biometric identifiers

8.3 Scars, marks and tattoos (SMTs) de-identification

- SMTs can improve automatic face recognition and retrieval performance
- There are no published papers related to de-identification of scars and marks
- Tattoo de-identification (Marčetić, Ribarić, 2014)
  - Tattoo detection and localization based on SIFT features
  - De-identification process is performed in the skin-swapping module



9. Conclusion

- Research in the field of de-identification and multimodal 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 (context-sensitive and environmental de-identification) - a knowledge-based approach for modelling a specific environment and situation?
- Problem of license plate de-identification (undetected license plates 4% - 6 %)
- Google reports – 89% of faces are blurred
- De-identification of the face in video surveillance systems is far from a complete solution - computer vision algorithms for the detection and localization of face(s)
- De-identification in drone-based surveillance systems

9. Conclusion

- Online voice or speaker de-identification, such as de-identification in an environment with background noise, voice de-identification in situations where there are multiple individuals speaking simultaneously
- 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
- Evaluation of privacy protection, intelligibility, pleasantness and the trade-off between privacy protection and utility/intelligibility
- De-identification also requires a platform for studies of the legal, ethical and social aspects of de- and re-identification in multimedia content and social network sites

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”.