Signal Processing: Image Communication 47 (2016) 131–151

Contents lists available at ScienceDirect

Signal Processing: *Image Communication*

journal homepage: www.elsevier.com/locate/image

De-identification for privacy protection in multimedia content: A survey

Slobodan Ribaric [a,*], Aladdin Ariyaeeinia [b], Nikola Pavesic [c]

[a] University of Zagreb, Faculty of Electrical Engineering and Computing, Zagreb, Croatia
[b] University of Hertfordshire, Hatfield, UK
[c] University of Ljubljana, Faculty of Electrical Engineering, Ljubljana, Slovenia

ARTICLE INFO

Article history:
Received 30 July 2015
Received in revised form
30 May 2016
Accepted 31 May 2016
Available online 1 June 2016

Keywords:
Privacy
Multimedia
De-identification
Biometric identifiers
Soft biometric identifiers
Non-biometric identifiers

ABSTRACT

Privacy is one of the most important social and political issues in our information society, characterized by a growing range of enabling and supporting technologies and services. Amongst these are communications, multimedia, biometrics, big data, cloud computing, data mining, internet, social networks, and audio–video surveillance. Each of these can potentially provide the means for privacy intrusion. De-identification is one of the main approaches to privacy protection in multimedia contents (text, still images, audio and video sequences and their combinations). It is a process for concealing or removing personal identifiers, or replacing them by 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. Based on the proposed taxonomy inspired by the Safe Harbour approach, the personal identifiers, i.e., the personal identifiable information, are classified as non-biometric, physiological and behavioural biometric, and soft biometric identifiers. In order to protect the privacy of an individual, all of the above identifiers will have to be de-identified in multimedia content. This paper presents a review of the concepts of privacy and the linkage among privacy, privacy protection, and the methods and technologies designed specifically for privacy protection in multimedia contents. The study provides an overview of de-identification approaches for non-biometric identifiers (text, hairstyle, dressing style, license plates), as well as for the physiological (face, fingerprint, iris, ear), behavioural (voice, gait, gesture) and soft-biometric (body silhouette, gender, age, race, tattoo) identifiers in multimedia documents.

1. Introduction

Recent advances in audio-recording devices, cameras, web technology and signal processing 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 environments, either for immediate inspection (e.g., abnormal behaviour recognition, identification and tracking of people in real time) or for storage, and subsequent data analysis and 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, drones equipped with camera, audio-sensor arrays, 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. for 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 more than forty-eight hundred government surveillance cameras in Washington, D.C. [3] and over 4 million closed-circuit television (CCTV) cameras deployed in the United Kingdom. The average citizen in London is caught on CCTV cameras about 300 times a day [4]. The problem associated with this is further exacerbated by lack of compliance with the relevant data-protection legislation. According to a study in [5], 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

* Corresponding author.
E-mail address: slobodan.ribaric@zemris.fer.hr (S. Ribaric).

http://dx.doi.org/10.1016/j.image.2016.05.020
0923-5965/

[6], Angwin analyzed relations among privacy, security and freedom in a world of relentless electronic surveillance – from Google to NSA. Angwin has concluded that 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, smart-phones and web services.

In view of the above issues, considerable research has now been directed towards approaches for the preservation of privacy and personal information. The main facet of efforts in this area, which is also the focus of this paper, is concerned with the development of methods for the de-identification of individuals captured in multimedia content (text, audio, still images, animation, video, and their combination). In order to provide an appropriate basis for the analysis presented here, the next section details the definition of privacy, and its social and legal aspects as well as its significance in today's society. The subsequent sections then present a survey of de-identification in multimedia content. The scope of the study is broad and covers methods for dealing with non-biometric, biometric physiological and behavioural identifiers, and soft biometric identifiers.

2. Privacy

There is no single definition of the term "privacy". The meaning of privacy depends on legal, political, societal, cultural and socio-technological contexts [7]. From the legal point of view, the first definition of privacy was given by Brandeis and Warren more than 120 years ago [8]. They defined privacy as "the right to be let alone", with respect to the acquisition and dissemination of information concerning the person, particularly through unauthorized publication, photography or other media. Also, according to Brandeis and Warren, the person should be protected from investigation and seizures that invade a sphere of individual solitude deemed reasonable by society. Additionally, the person has "the right to be let alone" with respect to fundamental decisions concerning his or her intimate relationships or aspects of life.

Westin defines privacy as the claim of an individual to determine what information about himself or herself should be known to others [9]. Based on the various usages of the word "privacy", there are many different conceptions of privacy and they can be classified into six general types [10]: (i) the right to be let alone; (ii) limited access to the self – the ability to protect oneself from unwanted access by others; (iii) secrecy – the concealment of certain matters from others; (iv) control over personal information; (v) personhood – the protection of one's personality, individuality and dignity; (vi) intimacy – control over, or limited access to, one's intimate aspects of life.

Depending on the social contexts and/or real life situations, privacy, in general, can be divided into a number of separate, but related, concepts [11]: (i) informational privacy – the right of the individual to limit access to personal information which could be used in any way to identify an individual; (ii) intentional privacy – the right of the individual to prevent or forbid further communication of observed events or exposed features (e.g., publishing photos or video footage); (iii) decisional privacy – the right of the individual to make decisions regarding his life without any undue interference; (iv) spatial privacy – the right of the individual to have his own personal spaces which cannot be violated without his explicit consent. If we include some physical and socio-technological contexts in the above classification, we can talk about: (i) information privacy, which involves the establishment of rules governing the collection and handling of personal data such as medical and tax records and credit information; (ii) the privacy of communications, which covers the security and privacy of mail, telephone, e-mail and other forms of communication; (iii) bodily privacy, which concerns the protection of people's physical selves against invasive procedures such as genetic tests, drug testing and cavity searches; (iv) territorial privacy, which concerns 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.

An in-depth 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 [10].

Let us illustrate the need for privacy and personal data protection with three examples of privacy violation. Case 1 describes a situation in which privacy is violated due to the inadequate protection of the face as a biometric identifier. Case 2 describes a situation in which privacy is violated and abused due to the low level of protection of stored personal documents with biometric identifiers and other personal identifiable information. Case 3 deals with the potential abuse of a facial recognition system used in public places.

Case 1: A person attempted suicide by slitting his wrists with a knife in a street. A CCTV surveillance camera was recording him, and the person monitoring the camera notified the police. The person was saved and transported to hospital. Some months later, the Council issued two photographs of the person taken from the CCTV footage for publication in an article about the preventative benefits of CCTV. The person's face was not specifically masked and he could be identified by people who knew him. Extracts from the CCTV footage were also shown on regional television in which the person's face had been masked at the Council's request.

Epilogue: The person sought judicial review of the Council's decision to release the CCTV footage without his consent. His application was rejected and this decision was upheld by the Court of Appeal with the explanation that there was no violation of privacy because "actions were already in the public domain" and revealing the footage "simply distributed a public event to a wider public." The applicant applied to the European Court of Human Rights and it concluded that "the disclosure by the Council therefore constituted a serious interference with his right to respect for private life. There were no relevant or sufficient reasons to justify the disclosure by the Council without obtaining the applicant's consent or ensuring as far as possible that his identity was masked." The Court therefore awarded him damages for his distress due to violation of his privacy [12].

Case 2: An identity thief using a stolen photocopy of an ID card and VAT number signed two contracts in a web shop with a mobile service provider and picked up two smart-phones. The person whose identity was stolen reported the case to the police and the Personal Data Protection Agency (PDPA).

Epilogue: PDPA made an inspection and requested contracts, delivery reports and a copy of the submitted ID. After discrepancies were found in the contracts (a fake signature) and negligence in the delivery procedures (the ID was not checked), the mobile service provider admitted its mistakes and cancelled the contracts. Police caught the gang with this *modus operandi*. One of the gang members was an insider in the mobile service provider company.

Case 3: In 2001, the police in Tampa, USA, used face scanning and facial recognition software to scan and capture images of football fans at the Super Bowl, without the knowledge of the people involved [13].

Epilogue: The use of facial recognition systems in public places was banned. Why? Different organizations could use faces captured by a facial recognition system to discover places that a person had visited or to scan different large databases in order to profile and/or socially control a person.