Expert Systems with Applications 42 (2015) 4177–4195

Contents lists available at ScienceDirect

Expert Systems with Applications

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

Review

Visual privacy protection methods: A survey

José Ramón Padilla-López [a,*], Alexandros Andre Chaaraoui [a], Francisco Flórez-Revuelta [b]

[a] Department of Computer Technology, University of Alicante, P.O. Box 99, E-03080 Alicante, Spain
[b] Faculty of Science, Engineering and Computing, Kingston University, Penrhyn Road, KT1 2EE, Kingston upon Thames, United Kingdom

ARTICLE INFO

Article history:
Available online 31 January 2015

Keywords:
Visual privacy protection
Video surveillance
Ambient-assisted living
Computer vision
Image processing

ABSTRACT

Recent advances in computer vision technologies have made possible the development of intelligent monitoring systems for video surveillance and ambient-assisted living. By using this technology, these systems are able to automatically interpret visual data from the environment and perform tasks that would have been unthinkable years ago. These achievements represent a radical improvement but they also suppose a new threat to individual's privacy. The new capabilities of such systems give them the ability to collect and index a huge amount of private information about each individual. Next-generation systems have to solve this issue in order to obtain the users' acceptance. Therefore, there is a need for mechanisms or tools to protect and preserve people's privacy. This paper seeks to clarify how privacy can be protected in imagery data, so as a main contribution a comprehensive classification of the protection methods for visual privacy as well as an up-to-date review of them are provided. A survey of the existing privacy-aware intelligent monitoring systems and a valuable discussion of important aspects of visual privacy are also provided.

1. Introduction

It can be observed that world population is ageing. In fact, it is estimated that population over 50 will rise by 35% between 2005 and 2050, and those over 85 will triple by 2050 (EC, 2010). Furthermore, the number of people in long-term care living alone is expected to increase by 74% in Japan, 54% in France and 41% in the US (EC, 2008). Therefore, this situation will not be sustainable in the near future, unless new solutions for the support of the older people, which take into account their needs, are developed.

Ambient-assisted living (AAL) aims to provide a solution to this situation. AAL applications use information and communication technologies to provide support to people so as to increase their autonomy and well-being. Video cameras are being used more and more frequently in AAL applications because they allow to get rich visual information from the environment. The advances produced in the last decades have contributed to this. The computational power has been increased while, at the same time, costs have been reduced. Furthermore, computer vision advances have given video cameras the ability of 'seeing', becoming smart cameras (Fleck & Strasser, 2008). This has enabled the development of vision-based intelligent monitoring systems that are able to automatically extract useful information from visual data to analyse actions, activities and behaviours (Chaaraoui, Climent-Pérez, & Flórez-Revuelta, 2012b), both for individuals and crowds, monitoring, recording and indexing video bitstreams (Tian et al., 2008). By installing networks of cameras in people homes or care homes, novel vision-based telecare services are being developed in order to support the older and disabled people (Cardinaux, Bhowmik, Abhayaratne, & Hawley, 2011). But these new technologies also suppose a new threat to individual's privacy.

Traditionally, cameras are used in public spaces for surveillance services in streets, parking lots, banks, airports, train stations, shopping centres, museums, sports installations and many others. It is estimated that there is an average of one camera for every 32 citizens in the UK, one of the most camera-covered countries in the world (Gerrard & Thompson, 2011). In short, video cameras are mainly used in outdoor environments and in public places, but they are not commonly used within private environments due to people's concerns about privacy. Generally, the use of video cameras in public places has been tolerated or accepted by citizens, whereas their use in private spaces has been refused. There may be several reasons to explain this difference. On the one hand, the perceived public-safety benefits favour the usage of cameras in public places for crime prevention, fight against terrorism and others. On the other hand, there is a widespread belief that while staying in public environments, people's sensitive information will not be exposed. Finally, there are some attitudes which have also contributed to accept their use, for example, to assume that anyone demanding privacy must have something to hide (Caloyannides, 2003).

* Corresponding author.
E-mail addresses: jpadilla@dtic.ua.es (J.R. Padilla-López), alexandros@dtic.ua.es (A.A. Chaaraoui), F.Florez@kingston.ac.uk (F. Flórez-Revuelta).

http://dx.doi.org/10.1016/j.eswa.2015.01.041
0957-4174/

In traditional video surveillance systems cameras are managed by human operators that constantly monitor the screens searching for specific activities or incidents. As estimated by Dee and Velastin (2008), the ratio between human operators and screens is around 16 displays for every operator in four local authority installations within the UK. Although they can only really watch 1–4 screens at once (Wallace & Diffley, 1988), this does not prevent abuses of these systems by their operators. Furthermore, the processing capacities of next-generation video surveillance systems and the increasing number of closed-circuit television cameras installed in public places are raising concerns about individual's privacy in public spaces too.

In the near future it is expected that cameras will surround us in both public and private spaces. Intelligent monitoring systems threaten individual's right to privacy because of automatic monitoring (Adams & Ferryman, 2013). These systems can retain a variety of information about people habits, visited places, relationships, and so on (Coudert, 2010). It is known that some systems already use facial recognition technology (Goessl, 2012). This way, these systems may build a profile for each citizen in which the people identity and related sensitive information is revealed. Therefore, this evolution of intelligent monitoring systems could be seen as approaching an Orwellian Big Brother, as people may have the feeling of being constantly monitored.

In the light of the above, it is clear that the protection of the individual's privacy is of special interest in telecare applications as well as in video surveillance, regardless whether they operate in private or public spaces. Therefore, privacy requirements must be considered in intelligent monitoring systems by design (Langheinrich, 2001; Schaar, 2010). As aforementioned, smart cameras become essential for AAL applications. Given that security and privacy protection have become critical issues for the acceptance of video cameras, a privacy-aware smart camera would make it possible to use video cameras in realms where they have never been used before. If individual's privacy can be guaranteed through the use of this technology, public acceptance would be increased giving the opportunity of installing these cameras in private environments to replace simpler binary sensors or, most importantly, to develop new telecare services (Chen et al., 2012; Morris et al., 2013; Olivieri, Conde, & Sobrino, 2012). This breakthrough could open the door to novel privacy-aware applications for ambient intelligence (AmI) (Augusto, Nakashima, & Aghajan, 2010), and more specifically in AAL systems for ageing in place (O'Brien & Mac Ruairi, 2009), being beneficial to improve the quality of life and to maintain the independence of people in need of long-term care.

1.1. Related studies

The focus of this review is on the protection of visual privacy. There are valuable reviews about AmI and AAL that have already considered privacy in video and have also highlighted its importance for the adoption of video-based AAL applications (Cardinaux et al., 2011; Cook, Augusto, & Jakkula, 2009). But these works scarcely go into detail about how visual privacy protection can be achieved. Other works from the video surveillance field have also analysed this topic but from a different point of view (Cavoukian, 2013, Senior et al., 2003, 2005). The main threats and risks of surveillance technologies like closed-circuit television cameras, number plates recognition, geolocation and drones are discussed in depth. As a consequence, some guidelines to manage privacy are also proposed, but how to protect visual privacy is not considered. In the same line, Senior and Pankanti (2011) unify their previous works and extend the review of visual privacy not only to video surveillance but also to medical images, media spaces and institutional databases. They consider some technologies to protect visual privacy and provide a classification. As far as we know, this is the first attempt to provide such a classification of protection methods for visual privacy but it is not a comprehensive one. In a more recent work (Winkler & Rinner, 2014), security and privacy in visual sensor networks are reviewed. Although they perform a detailed analysis of the security from several points of view (data-centric, node-centric, network-centric and user-centric), they do not provide an in-depth analysis of privacy protection.

In this survey, we focus on giving an answer to the question of how the visual privacy can be protected, and how such a kind of protection is developed by some of the existing privacy-aware intelligent monitoring systems that have been found in the literature. Because of this, a comprehensive classification of visual privacy protection methods is provided as the main contribution of this work. The remainder of this paper is organised as follows: Section 2 gives an intuitive notion of what visual privacy protection is. A comprehensive review of visual privacy protection methods is presented in Section 3. In Section 4, relevant privacy-aware intelligent monitoring systems are introduced. A discussion of important privacy-related aspects is carried out in Section 5. Finally, a summary of the present work as well as future research directions are given in Section 6.

2. Visual privacy protection

Privacy protection consists in preventing that the information that an individual wants to keep private becomes available to the public domain. In the context of images and videos, we refer to it as visual privacy protection. In this paper, the terms visual privacy and privacy will be used indistinctly, except when indicated.

First of all, it is worth to clarify when individual's privacy needs to be protected. When protecting privacy, it can be differentiated between person's identity and sensitive information which has to be kept in private. Video can convey an enormous amount of information that can be qualified as sensitive. Nevertheless, if sensitive information is present in a video but person's identity is not, there is no privacy loss. The same is true whether person's identity is in a video but without any sensitive information. In both cases, privacy is protected because there does not exist any association or mapping between sensitive information and person's identity.

Another important issue related to visual privacy is which is the sensitive information or region of interest to be protected. In many works only the face is obscured but that is not enough to protect visual privacy. Even when the person's face is obscured, other elements could exist in the image through which person identification may be performed, for instance, using inference channels and previous knowledge (Saini, Atrey, Mehrotra, & Kankanhalli, 2014). Visual cues like clothes, height, gait, and the like can be used to identify the person. For instance, in a pair-wise constraints identification (Chang, Yan, Chen, & Yang, 2006; Chen, Chang, Yan, & Yang, 2009) where faces had been masked, observers were able to identify whether a person in one image was the same one than in a different image. In that test, recognition hit rate was higher than 80%. By using this information and only detecting an image where a privacy breach exists, the person may be identified and tracked in images where privacy was presumably preserved. These visual clues must be considered in order to protect privacy as they affect to the election of which regions of interest have to be protected. So, there is not actually only one region of interest but multiple. A region of interest should be extended to a wider area in some cases, while two or more regions of interest should be created in others.

3. Protection methods

There are different ways to protect and preserve the privacy of individuals appearing in videos and images (see Table 1). Two