Visual Privacy by Context: A Level-Based Visualisation Scheme

José Ramón Padilla-López[1], Alexandros Andre Chaaraoui[1], and Francisco Flórez-Revuelta[2]

[1] Department of Computer Technology, University of Alicante,
P.O. Box 99, E-03080 Alicante, Spain
jpadilla@dtic.ua.es, alexandros@dtic.ua.es
[2] Faculty of Science, Engineering and Computing, Kingston University,
Penrhyn Road, KT1 2EE, Kingston upon Thames, United Kingdom
F.Florez@kingston.ac.uk

Abstract. In a near future, a greater number of individuals in long-term care will live alone. New solutions are needed in order to provide them support and increase their autonomy at home. Intelligent monitoring systems based on computer vision may provide a solution. However, privacy related issues must be solved beforehand. In this paper, we propose a level-based visualisation scheme to give users control about their privacy in those cases in which another person is watching the video. These visualisation levels are dynamically selected according to the context by displaying modified images in which sensitive areas are protected.

Keywords: privacy, context, intelligent monitoring, ambient-assisted living

1 Introduction

Video-based applications are being used more and more frequently in Ambient-Assisted Living (AAL). Computer vision techniques allow to monitor an environment and report on visual information, which is generally the most direct and natural way of describing the world. These advances have given video cameras the ability of 'seeing', thereby becoming smart cameras. They are used for several applications, from tasks such as object recognition and tracking to recognition of actions and activities of daily living, or even human behaviour analysis during a long period of time [1]. These new abilities enable the development of novel AAL services for people in need of care, *e.g.* a home accidents detection. Although video cameras allow to obtain a huge amount of environmental data in a non-intrusive and straightforward way, their usage in private spaces brings up ethical concerns related to the privacy of their inhabitants. Smart cameras in private spaces threatens privacy protection [5]. Hence, it seems unreasonable to use cameras there. Indeed, the usage of consumer electronics products like Google Glass currently raise suspicion due to people being recorded without consent. Therefore, there are some privacy issues that need to be solved in advance before using smart cameras in private spaces. In this paper, a level-based visualisation scheme that aims to solve some privacy issues is presented.

2 Privacy Protection

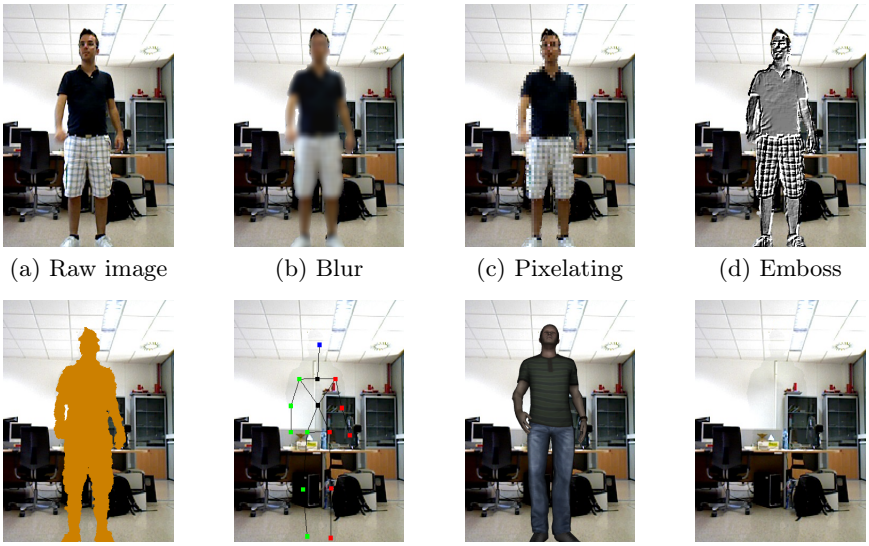
Although there are several stages in which privacy protection may be involved, this paper is focused on the visualisation stage, *i.e.* the visualisation of the video by a human viewer. This work is a continuation of another one presented in [4]. In that work, we introduced a paradigm for people monitoring that considers privacy from early stages on. In the present work, we have reviewed the privacy requirements and the privacy issue has been addressed following a privacy-by-context approach.

In contrast to works where privacy is protected by using blurring or pixelating effects to modify an image [3], this contribution is more similar to [2], where several ways of displaying an object (*i.e.* visual abstractions) are proposed according to the closeness between objects and viewers. Similarly, in our work privacy is protected by means of a set of visualisation models that provide a given level of protection. But the use of a specific model is determined by the context. In other words, visualisation models establish the way in which non-protected video images are modified before being displayed in order to conceal sensitive information of the subject. As the the correspondence between a given instance of the context and the visualisation level must be performed by the assisted person in advance, our privacy-by-context approach empowers people to adapt privacy to their preferences.

The context has to provide enough information so as people can decide by whom, how and when they are watched. Different privacy protection needs of an individual have been considered (identity, appearance, location, and ongoing activity or event) in order to decide which variables are part of the context. This leads us to propose a context made up of the following variables: i) the observer, ii) identity of the person (to retrieve the privacy profile), iii) closeness between person and observer (*e.g.* relative, doctor or acquaintance), iv) appearance (dressed?), v) location (*e.g.* kitchen), and vi) ongoing activity or detected event (*e.g.* cooking, watching TV, fall). By using these variables, an individual can describe a situation and choose the corresponding visualisation level for this situation (see Table 1).

Table 1. An example of the privacy levels (see Sect. 3) selected by John according to the context.

#	**Observer**	**Rest of the context**	**Visualisation Level**
1	My daughter Mary (caregiver, relative)	dressed, living room, watching TV	Raw Image
2	My daughter Mary (caregiver, relative)	undressed, shower, fall	Highly protected (Silhouette)
3	Alice (my doctor, friend)	dressed, living room, watching TV	No image



(a) Raw image (b) Blur (c) Pixelating (d) Emboss

(e) Solid silhouette (f) Skeleton (g) 3D avatar (h) Invisibility

Fig. 1. Visualisation models included in our implementation.

3 Implementation

A software prototype for our visualisation scheme has been developed considering eight visualisation models (see Fig. 1). The silhouette of the person is considered as the sensitive area, thereby these models focus on protecting identity and appearance. The implemented visualisation models use some visual effects to conceal the person, replace the individual with something different, or even make the person disappear completely. Next, we describe each model:

(a) **Raw image**. It does not modify the raw image, so no protection is provided. In some cases, it could be useful to assess the gravity of a detected event.
(b) **Blur**. The silhouete is smoothed. Although a balance between privacy and awareness is not provided, it can partially protect the appearance.
(c) **Pixelating**. It reduces the image resolution. As in blur, it can partially protect the appearance.
(d) **Emboss**. This model removes colour information of the image (corresponding to skin, hair, etc.) but it preserves the structure of the textures.
(e) **Solid silhouette**. Information about colour and structure of textures is removed. Height and shape allow identification. Nudity is partially protected.
(f) **Skeleton**. A virtual skeleton that mimics the movements is used. Colour and shape are fully removed (nudity protection), but posture is preserved.
(g) **3D avatar**. A 3D avatar that mimics the movements is used. Appearance information is completely removed, preventing direct identification.
(h) **Invisibility**. The person is completely removed from the image. Interaction with the environment can be seen (e.g. objects) but not the person.

4 Conclusion

In this paper, we have presented a privacy scheme that uses visualisation levels for privacy preserving. The selection of the appropriate level is handled by the assisted person according to the context made up of six variables. By using this, the individual can decide how to be visualised in any situation. We have also developed a prototype that has eight visualisation models. These are focused on the protection of the identity and the appearance of the person, and they work in real time.

As future work, it would be interesting to compare the different visualisation models as well as develop new ones. Also, other image regions should be considered as sensitive areas so as to prevent indirect identification. Further research will be carried out in order to recognise identity and appearance to enhance the context.

Acknowledgements

This work has been partially supported by the Spanish Ministry of Science and Innovation under project 'Detección temprana de síndromes de fragilidad y demencia mediante análisis visual de la marcha' (TIN2013-47152-C3-2-R). José Ramón Padilla-López and Alexandros Andre Chaaraoui acknowledge financial support by the Conselleria d'Educació, Formació i Ocupació of the Generalitat Valenciana (fellowships ACIF/2012/064 and ACIF/2011/160 respectively). The funders had no role in study design, data collection and analysis, decision to publish, or preparation of the manuscript.

References

1. Chaaraoui, A.A., Climent-Pérez, P., Flórez-Revuelta, F.: A review on vision techniques applied to human behaviour analysis for ambient-assisted living. Expert Systems with Applications 39(12), 10873–10888 (2012)
2. Chinomi, K., Nitta, N., Ito, Y., Babaguchi, N.: PriSurv: Privacy Protected Video Surveillance System Using Adaptive Visual Abstraction. In: Proceedings of the 14th International Conference on Advances in Multimedia Modeling. pp. 144–154. MMM'08, Springer-Verlag, Berlin, Heidelberg (2008)
3. Frome, A., Cheung, G., Abdulkader, A., Zennaro, M., Bo, W., Bissacco, A., Adam, H., Neven, H., Vincent, L.: Large-scale privacy protection in google street view. In: Computer Vision, 2009 IEEE 12th International Conference on. pp. 2373–2380 (Sept 2009)
4. Padilla-López, J.R., Flórez-Revuelta, F., Monekosso, D.N., Remagnino, P.: The 'Good' Brother: Monitoring People Activity in Private Spaces. In: Distributed Computing and Artificial Intelligence, Advances in Intelligent and Soft Computing, vol. 151, pp. 49–56. Springer Berlin Heidelberg (2012)
5. Senior, A., Pankanti, S.: Privacy protection and face recognition. In: Li, S.Z., Jain, A.K. (eds.) Handbook of Face Recognition, pp. 671–691. Springer London (2011)