MediaEval 2014 Visual Privacy Task: De-identification and Re-identification of Subjects in CCTV

Cesar Pantoja
Queen Mary University of London
Mile End Road
E1 4NS, London, UK
c.pantoja@qmul.ac.uk

Ebroul Izquierdo
Queen Mary University of London
Mile End Road
E1 4NS, London, UK
e.izquierdo@qmul.ac.uk

ABSTRACT

We present in this paper a method for de-identification of persons in a CCTV environment which uses different levels of filtering depending on the privacy sensitivity of the region of interest. The proposed method tries to tackle the problem of re-identifying (de-filtering) a person which has committed a crime. Validation of the method shows low results in privacy as a result of the identity of the subjects not being concealed at all times.

1. INTRODUCTION

Police and security forces around the world deploy great amounts of CCTV in an effort to fight crime and preserve peace. This at a cost of regular citizens' privacy, as their daily whereabouts are being recorded as well. For the MediaEval 2014 Visual Privacy task[1], we propose a method to de-identify people present in a CCTV with the option of re-identifying them in the case it is established the person is exposing a criminal behaviour. This causes that while the privacy is being maintained, the intelligibility of the scene is also preserved as the surveillance task can be carried away unfiltered when it is needed. Evaluations show acceptable intelligibility and pleasantness results of the filter, but not so good results in privacy, most likely because of the identity of the subjects not being concealed all the time. The rest of the paper is organised as follows: Section 2 presents the proposed method, the objectives and design choices behind it's development. Section 3 presents the evaluation results of the method. Finally, section 4 draws some closing remarks and states future research opportunities.

2. PROPOSED METHOD DESCRIPTION

The de-identification method applies different filters depending on the privacy sensitivity of the region of interest. All the types of regions of interest were categorised in three possible levels, each carrying more sensitive information than the previous one.

But before going into details of the de-identification method and each of the levels, it is important to note that an important feature of this filter is the ability to re-identify suspects of criminal activities. This allows CCTV operators to perform the surveillance activity in a more effective way. As soon as one actor is known to be committing a suspicious activity, the filter is switched off only for that actor performing the illicit activity but keeping the privacy of the other actors intact. The current actions for which the filter is deactivated are "fighting", "stealing", and "bad drop". This allows to effectively re-identify the criminals in the scene. This is an important feature of de-identification filters: the ability to reverse the filter if it is required by the users of the system.

As stated previously, the filter applies 3 different process depending on the privacy sensitivity of the region of interest. The sensitivity is given to the filter and it decides which process to apply.

The first level of privacy is the one with the less sensitivity and the lightest filter is applied here. In this case it was decided to use a Gaussian Blur with a kernel size of 21 pixels. The second level might carry some additional personal information which might harm the privacy of the subjects. For this level, a pixelisation filter with a new pixel size of 10 is applied.

The third and final level carries the most personal information (such as faces and skin tone) and has to be filtered the most. For this level the pixelisation filter was also selected, but with a new pixel size of 20 pixels. In addition to this, the colour of the region of interested is removed, leaving a pixelated grey-scale region.

2.1 Method Discussion

The first thing we want to achieve is to provide privacy to law-abiding citizens. The second goal of the filter is to allow the re-identification of suspects of crimes. With this in mind, and since the meta-data of the actions of the actors in the scene was available, it was decided that the filter would be deactivated to allow the surveillance task to be carried away with much more information than if it was filtered. This filter has thus two parts: the de-identification of innocent people and the re-identification of suspects of crimes.

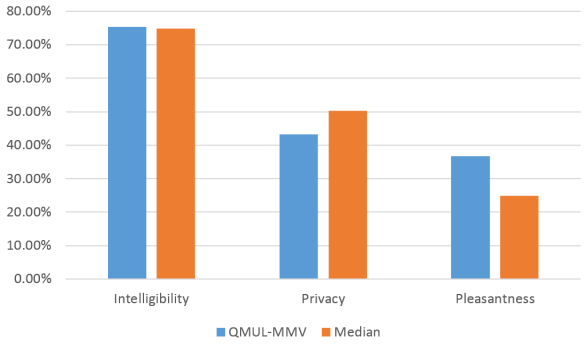
In the de-identification part of the filter, for the top levels of privacy sensitivity, the pixelisation filter has been selected because it has shown to have a very good balance of privacy and intelligibility[3]. Additionally, Skin tone is regarded as one of the most important features when identifying humans[2], which is why an additional step was added to conceal the person's real skin tone. Figure 1 shows the filter applied to a CCTV scene.

3. EVALUATION RESULTS

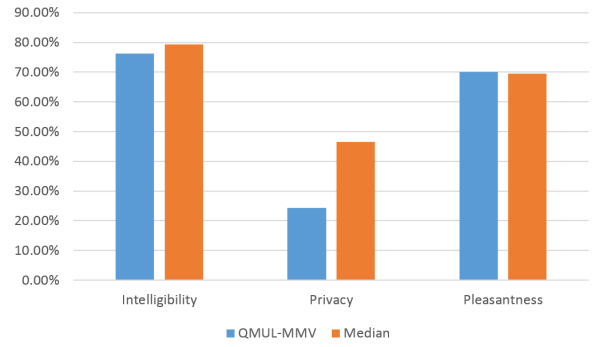
Evaluation was performed in with the DataSet and methodology presented in [4] and [1] respectively. Figure 2 presents

MediaEval 2014 Workshop, October 16-17, 2014, Barcelona, Spain

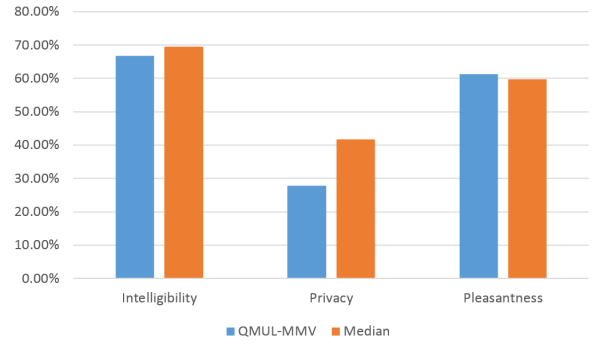
Figure 1: Output produced by the filter.



(a) Stream 1



(b) Stream 2



(c) Stream 3

Figure 2: Evaluation Results

the results. It includes the results for Stream 1 (naïve subjects - subfigure 2a), Stream 2 (video surveillance staff - subfigure 2b), and Stream 3 (online subjective evaluations - subfigure 2c).

It can be seen that the results in Intelligibility and Pleasantness are right around the median of the other results (except for pleasantness in Stream 1, where it is actually higher). But in all of the Streams, it is evident that the privacy score is significantly lower than the other approaches. This is a result of the filter not concealing the identity of the subjects (thus, NOT protecting their privacy) in the case where they are engaging in potentially illicit activity as specified by the meta-data.

4. CONCLUSIONS AND FUTURE WORK

We have developed a de-identification method for the MediaEval 2014 Visual Privacy Task, which applies different filters to different regions of interest according to it's privacy sensitivity. Most importantly, the filter allows the re-identification of a suspect by removing all relevant filters when a crime is detected. This allows us to keep the privacy of innocent citizens' intact, while exposing the full identity of crime suspects, facilitating the labour of law enforcement to the authorities.

Because of the nature of this filter, a low privacy score was actually achieved. We hope that this development leads to a wider discussion about the adequate way to address citizens' privacy concerns while still generating useful data for law enforcement. We think the best solution is a multi-tiered approach where there are different levels of de-identification depending on the relevance of the person. This discussion must include the fact that it would be a machine determining the "guilt" of a subject and thus revealing it's identity. Among other ethical issues, what would happen for example with false negatives or false positives?

In the future we expect to adjust the de-identification filter to get better results in Intelligibility and Pleasantness. The usefulness of removing the filter in case of suspicious activities has to be further evaluated as well.

5. ACKNOWLEDGMENTS

The research presented in this paper was supported by the European Commission under contract FP7-SEC 261743 VideoSense and FP7-SEC 285024 Advise.

6. REFERENCES

[1] A. Badii, T. Ebrahimi, C. Fedorczak, P. Korshunov, T. Piatrik, V. Eiselein, and A. Al-Obaidi. Overview of the mediaeval 2014 visual privacy task. In *MediaEval 2014 Workshop*, Barcelona, Spain, October 16-17 2014.

[2] M. Demirkus, K. Garg, and S. Guler. Automated person categorization for video surveillance using soft biometrics. *Proc. SPIE*, 7667:76670P–76670P–12, 2010.

[3] P. Korshunov, C. Araimo, F. De Simone, C. Velardo, J. Dugelay, and T. Ebrahimi. Subjective study of privacy filters in video surveillance. In *Multimedia Signal Processing (MMSP), 2012 IEEE 14th International Workshop on*, pages 378–382, 2012.

[4] P. Korshunov and T. Ebrahimi. PEViD: privacy evaluation video dataset. In *SPIE Applications of Digital Image Processing XXXVI*, volume 8856, San Diego, California, USA, Aug. 2013.