MediaEval 2014 Visual Privacy Task: Geometrical Privacy Protection Tool

Pavel Korshunov
MMSPG, EPFL
pavel.korshunov@epfl.ch

Touradj Ebrahimi
MMSPG, EPFL
touradj.ebrahimi@epfl.ch

ABSTRACT

This paper describes EPFL privacy protection tool for the MediaEval 2014 Visual Privacy task. The goal of the task is to obscure faces, body silhouettes, and personal items of people in the provided surveillance clips to preserve their personal privacy. The EPFL privacy protection tool mainly relies on two privacy protection filters: a warping-based reversible filter to obscure features with low visual details (body silhouettes) by distorting them with randomized warping and morphing-based reversible filter to obscure features with high visual details (faces and personal items) by 'replacing' them with a graphical representation. The aim of this tool is to achieve an acceptable balance between privacy (how well the privacy is protected) and intelligibility (how well the surveillance task can still be performed), as well as, privacy and pleasantness (how pleasant is the protection). The results of three types of subjective evaluations, via crowdsourcing, practitioners, and stakeholders, provided by the organizers of the task demonstrates that EPFL privacy protection tool achieves a great overall balance between privacy, intelligibility, and pleasantness, while being secure and reversible in the same time.

1. INTRODUCTION

Recent adoption of digital video surveillance systems, especially in public spaces and communities, has significantly increased the concern for intrusion into individual privacy. New sensing technologies, such as ultra high definition, high dynamic range, or video capturing with mini-drones, threaten to eradicate boundaries of private space even more. As a possible solution, many privacy protection tools have been proposed for preserving privacy, ranging from simple methods such as masking blurring, pixelization, or masking to more advanced methods satisfying the following desirable practical properties: reversibility, robustness, and security. The advanced methods can be divided into several categories: encryption-based [7], scrambling-based [2], and geometrical-based [6, 5] methods.

Despite wide availability of visual privacy protection tools, with an exception of some work [3], little is known about which tools are suitable for practical applications. To close this gap, MediaEval 2014 Visual Privacy task was designed to facilitate submissions of different protection tools and to benchmark them on practical privacy video dataset [4] via several types of subjective evaluations. Moreover, the focus of this task is twofold: one explores the privacy-intelligibility tradeoff, which is between how well surveillance can be performed while privacy is being preserved, and another explores the privacy-pleasantness tradeoff, which is about how socially acceptable is a given privacy protection tool for a human observer. This year, the task is also separates visual privacy features into two types: low detailed features, such as body silhouettes, and features with high details, such as faces or personal items [1].

In the submission to MediaEval 2014 Privacy task, EPFL aimed to address both tradeoffs and separately obscure two types of visual features. Therefore, the proposed privacy protection tool consists of two privacy protection filters: a warping-based filter [6] that obscures features with low visual details by distorting them with randomized warping and morphing-based filter [5] to obscure features with high visual details by 'replacing' them with a graphical representation. The privacy protection tool is implemented using Python, OpenCV[1], and Matlab.

Organizers of the task provided video dataset [4] with annotations of privacy sensitive regions including faces, hair, skin, accessories, and body regions, as well as classification of these regions into low, medium, oh high detailed features. The tool, therefore, assumed the privacy regions known (in a practical scenario, they can be detected by video analytics) and focused on developing the privacy protection tool that achieves an acceptable balance between privacy (how well the privacy is protected) and intelligibility (how well the surveillance task can still be performed), as well as, privacy and pleasantness (how pleasant is the protection).

2. KEY DECISIONS AND CHALLENGES

The best privacy preserving filter would be a blacked out camera with no video feed, but, in such case, there would be no surveillance possible and intelligibility would be zero. Therefore, a usable privacy protection filter should have a balance between privacy and intelligibility. Similarly, an encryption or scrambling based privacy filters could lead to high privacy but can be annoying or even scary, resulting in very low pleasantness. Another important practical requirement is the secure reversibility of the privacy protection tool, so that the protection can be undone in secure way (only if one has a secret key) to restore the original video in case police or court would require it.

To achieve the balance between privacy, intelligibility, and pleasantness, as well as to provide reversible protection, the proposed privacy protection tool adopted a two-stage approach: (i) reversible warping filter [6] is applied on body silhouettes as a low detailed visual feature to distort general personal appearance and (ii) reversible morphing filter [5] on faces and personal items as high detailed visual features to remove all the identifiable details. Figure 1 illustrates how the proposed tool protects privacy of people.

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

[1] http://opencv.org/

Table 1: Results of three different subjective evaluations for EPFL privacy protection tool compared to average.

	Crowdsourcing		Stakeholders		Practitioners	
	EPFL	Average	EPFL	Average	EPFL	Average
Intelligibility	73.2	74.8	67.7	79.3	59.5	69.5
Privacy	51.0	50.2	61.6	46.5	57.3	41.6
Pleasantness	23.6	24.8	40.7	69.5	46.3	59.7

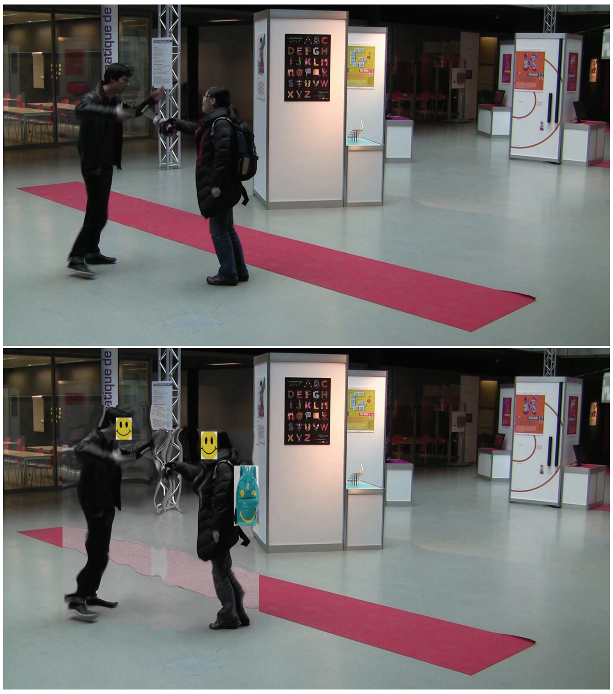

Figure 1: Original (above) and privacy protected (below) snapshots of fighting scene video.

Warping filter makes the details of the visible object unrecognizable (i.e., privacy is increased), but, by controlling the strength of the filter, the overall general shape of the object can be preserved, so it would still be possible to understand what is going on in the surveillance scene (i.e., intelligibility is not decreased). Morphing filter replaces faces and personal items with the graphical representation, e.g., 'smiley face' instead of the original face, which effectively removes all personal details, i.e., privacy is increased, with the aim to keep both intelligibility and pleasantness/appropriateness high.

3. EVALUATION RESULTS

The organizers provided the results from three subjective evaluations: crowdsourcing-based evaluation in Stream 1, evaluation by stakeholders and surveillance experts in Stream 2, and evaluation by practitioners and data protection experts in Stream 3. The corresponding results of the EPFL privacy protection tool are summarized in the Table 1 and compared against the average of the total 8 submissions to the Privacy Task of MediaEval 2014.

From the table, it can be noted that across all evaluations, the tool demonstrates higher than average level of privacy but underperforms in terms of intelligibility and pleasantness. In crowdsourcing evaluation, the performance of the tool is nearer to average compared to other two evaluations. It means that the tool would be more suitable for the scenarios where the observers are naïve subjects as it is in the case of crowdsourcing. The low intelligibility score can be compensated by the fact that the tool is reversible and original video can be securely restored, which would allow the detailed examination of the video data if necessary. Low pleasantness value is probably due to the choice of graphical representations for faces and personal items (see Figure 1), which subjects did not like. A more appropriate and use case oriented choice of such representation may improve the pleasantness of the visual protection.

4. CONCLUSION

EPFL privacy protection tool combines warping and morphing privacy protection filters and achieves an acceptable balance between privacy, intelligibility, and pleasantness, providing, in the same time, ability to securely restore the original content if necessary. In a practical scenario, a better fitting graphical representations of the faces and personal items can be selected.

Acknowledgments

This work was conducted in the framework of the EC funded Network of Excellence VideoSense.

5. 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] F. Dufaux and T. Ebrahimi. Scrambling for privacy protection in video surveillance systems. *IEEE Trans. on Circuits and Systems for Video Technology*, 18(8):1168–1174, Aug. 2008.

[3] P. Korshunov, C. Araimo, F. De Simone, C. Velardo, J. Dugelay, and T. Ebrahimi. Evaluation of visual privacy filters impact on video surveillance intelligibility. In *International Workshop on Quality of Multimedia Experience (QoMEX)*, pages 150–151, July 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.

[5] P. Korshunov and T. Ebrahimi. Using face morphing to protect privacy. In *IEEE International Conference on Advanced Video and Signal-Based Surveillance (AVSS)*, pages 208–213, Krakow, Poland, Aug. 2013.

[6] P. Korshunov and T. Ebrahimi. Using warping for privacy protection in video surveillance. In *18th International Conference on Digital Signal Processing (DSP)*, pages 1–6, Santorini, Greece, July 2013.

[7] T. Winkler and B. Rinner. TrustCAM: Security and privacy-protection for an embedded smart camera based on trusted computing. In *IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)*, pages 593–600, Sept. 2010.