MediaEval 2013 Visual Privacy Task: Warping-based Privacy Protection Tool

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

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

ABSTRACT

In this paper, we describe EPFL privacy protection tool submitted to the MediaEval 2013 Visual Privacy task. The goal of the task is to obscure faces and other personal items of people in the provided surveillance clips to preserve their personal privacy. In the privacy protection tool, we used a combination of reversible privacy protection filter based on geometric warping transformation, randomized saturation filter, masking with partial opacity, and pixelization. The aim of the implementation was to achieve an acceptable balance between privacy and intelligibility, as well as, privacy and appropriateness. The results of both objective and subjective evaluations provided by the organizers of the task demonstrated that our privacy protection tool leads to high appropriateness and intelligibility (the surveillance task can be performed with high accuracy) while keeping strong privacy protection.

1. INTRODUCTION

The problem of privacy protection in video surveillance systems gaining more and more attention from research and industry. Many privacy protection tools were proposed to mitigate privacy intrusiveness of modern surveillance systems. These protection techniques vary from such simple approaches like 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 [8], scrambling-based [1], anonymization [7], and geometrical-based [5, 4] methods.

Despite wide availability of visual privacy protection tools, with an exception of a few works [2, 6], little is known about which tools are suitable for practical applications. To close this gap, MediaEval 2013 Visual Privacy task was designed to facilitate submissions of different protection tools and to evaluate them on practical privacy video dataset [3] via objective and subjective tests. 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-appropriateness tradeoff, which is about how socially acceptable is a given privacy protection tool for a human observer.

In our submission to MediaEval 2013 Visual Privacy task, we aimed to address both tradeoffs. We have built a privacy protection tool based on reversible and secure warping filter [5] and a combination of basic filters such as masking, saturation, and pixelization. Warping filter distorts the details of a visual object (e.g., a face) but keeps its general shape and appearance visible. Since warping filter does not change intensities of the pixels and, hence, does not affect image colors (and skin or hair color is personal information), we added a randomized reversible secure saturation filter and masking with low opacity to distort color information as well. For color and skin regions, as these carry relatively little intelligible information, we used strong irreversible pixelization filter to distort the visual details. Our privacy protection tool is implemented using Python and OpenCV[1].

Organizers of the task provided video dataset [3] with annotations of privacy sensitive regions including faces, hair, skin, accessories, and body regions. We, therefore, assumed these regions known (in practical scenario, they can be detected by video analytics) and focused on developing the privacy protection tool that achieves an acceptable balance between privacy and intelligibility, as well as, privacy and appropriateness. To keep as much intelligible information in the video as possible, as per the guidelines from [3], we did not use our tool on the whole body regions (though, they were provided) but only on the key privacy sensitive regions.

2. PRIVACY PROTECTION TOOL

The proposed privacy protection tool adopted a two-stage approach (see Figure 1 for an illustration): (i) warping [5] and pixelization filters were applied on primary (face and accessories) and secondary (skin regions and hair) regions respectively to hide visual details and (ii) reversible randomized saturation filter and reversible low opacity masking was applied to remove color information.

Warping filter makes the details of the visible object unrecognizable (i.e., privacy is increased), but, by controlling its strength, we can keep its overall general shape preserved, so we can still understand what is going on in the surveillance scene (i.e., intelligibility is not decreased). Higher intelligibility is also insured by not distorting the whole body regions keeping intact the less privacy sensitive visual information. Randomized saturation and opacity masking allow us to decrease the color level of skin, hair, or accessories, so they are not recognizable (i.e., privacy is increased), yet the original colors can be recovered if needed.

2.1 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 appropriateness.

Copyright is held by the author/owner(s).
MediaEval 2013 Workshop, October 18-19, 2013, Barcelona, Spain

[1] http://opencv.org/

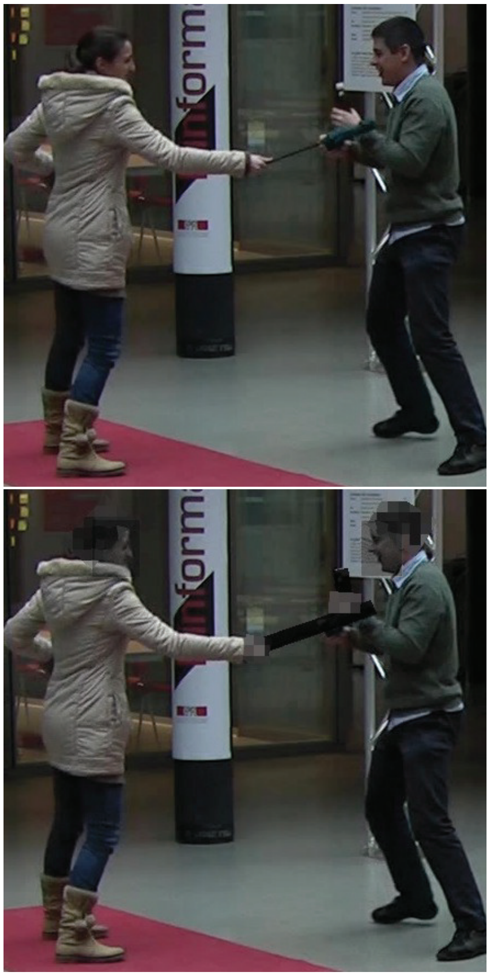

Figure 1: Original (above) and privacy protected (below) snapshots (cropped for clearer visibility) of fighting scene video.

Aiming to balance between these tradeoffs, we made the following implementation decisions:

- Warping is applied to faces and accessories. The aim is to distort facial features and details of accessories, preserving, in the same time, a general appearance of people to keep understanding of the scene and actions clear.
- Strong pixelization is applied to hair and skin regions. Since these regions are not as important for surveillance purposes as, for example, faces, but still carry information about gender and race, higher degree of protection is required.
- Randomized saturation is applied to faces, skin, and hair and opacity masking is applied to face (opacity value 0.3) and accessories (opacity value 0.8) to hide color and detailed information about these regions.
- No filter is applied to body regions to keep visible as much intelligibility information as possible.

3. EVALUATION RESULTS

The evaluation results provided by the organizers of the task are summarized in Table 1, where our objective and subjective evaluation results are compared with the average result of the total 9 submissions. The results are favorable and demonstrate that our privacy protection tool achieves a reasonable balance between privacy, intelligibility, and appropriateness, with all scores except for privacy being well above the average.

4. CONCLUSION

The proposed privacy protection tool combined several privacy protection filters achieving a balance between privacy, intelligibility, and appropriateness. For the future work, the strength of adopted filters in the tool should be adjusted, so the privacy increased while intelligibility stays at the same level.

Table 1: Results of objective and subjective evaluations for our tool

	Obj.	Av. obj.	Subj.	Av. subj.
Intelligibility	0.68	0.50	0.84	0.66
Privacy	0.51	0.67	0.60	0.68
Appropriateness	0.93	0.56	0.63	0.49

Acknowledgments

This work was conducted in the framework of the EC funded Network of Excellence VideoSense. Special thanks to Andrea Melle (Eurecom) for providing parts of the code for our implementation.

5. REFERENCES

[1] 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.

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

[3] 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.

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

[5] P. Korshunov and T. Ebrahimi. Using warping for privacy protection in video surveillance. In *18th International Conference on Digital Signal Processing (DSP)*, DSP'13, Santorini, Greece, June 2013.

[6] P. Korshunov, A. Melle, J.-L. Dugelay, and T. Ebrahimi. A framework for objective evaluation of privacy filters in video surveillance. In *SPIE Applications of Digital Image Processing XXXVI*, volume 8856, San Diego, California, USA, Aug. 2013.

[7] J. Wickramasuriya, M. Datt, S. Mehrotra, and N. Venkatasubramanian. Privacy protecting data collection in media spaces. In *Proceedings of the 12th annual ACM international conference on Multimedia*, pages 48–55, New York, NY, USA, Oct. 2004.

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