MediaEval 2015 Drone Protect Task: Privacy Protection in Surveillance Systems Using False Coloring

Serdar Çiftçi[1], Pavel Korshunov[2]*, Ahmet Oğuz Akyüz[1], Touradj Ebrahimi[2]

1. Department of Computer Engineering, Middle East Technical University, Ankara, Turkey
{sciftci, akyuz@ceng.metu.edu.tr}

2. Multimedia Signal Processing Group, Ecole Polytechnique Fedéralé de Lausanne, Switzerland
{pavel.korshunov, touradj.ebrahimi@epfl.ch}

ABSTRACT

This paper describes privacy protection method based on a false coloring approach for Drone Protect Task of MediaEval 2015. The aim is to obscure regions of a video that are privacy sensitive without sacrificing intelligibility and pleasantness. False coloring transforms the original colors of pixels using a color palette into a different set of colors in which private information is harder to recognize. The method can be applied globally to an entire frame of the video or to a specific region of interest (ROI). The privacy protected output is expected to remain pleasant, and when needed, a close approximation of the original input can be recovered. Benchmarking evaluations on the mini-drone dataset show promising results, especially, for intelligibility and pleasantness criteria.

1. INTRODUCTION

Video surveillance systems are being widely used to protect the safety of public and private perimeters. An ideal surveillance system should balance well between two objectives: efficiently execute a security task (*intelligibility*) and carefully preserve subjects' privacy (*privacy*). The most commonly used methods to protect privacy such as blurring, masking, and pixelization do not achieve a good balance. For this reason, second generation solutions such as scrambling [5], warping [6], and in-painting [3] are proposed. However, these solutions have their own weaknesses such as dependency on compression and format, visually disturbing results, negative impact on intelligibility, and irreversibility.

Furthermore, most methods strongly rely on efficient computer vision algorithms for instance when regions that require privacy protection must be automatically detected (e.g., faces, license plates, etc.). However, computer vision algorithms are known to fail at times. If a sensitive region is missed, even in a single frame, it will severely compromise privacy. Therefore, there is a need to develop robust and effective algorithms for privacy protection that can efficiently cope with situations when computer vision algorithms fail.

We propose to protect privacy via false coloring, which does not rely on computer vision and can be applied either on an entire frame or a region of interest. It is simple to implement and has little computational overhead, thus, is applicable for real-time system [4]. False coloring preserves privacy without compromising pleasantness and intelligibility. Furthermore, its output can be reversed to obtain a close approximation of the unprotected information.

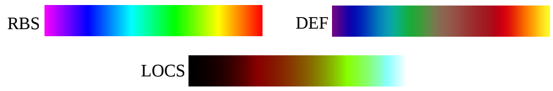

Figure 1: Color scales used in this study.

The proposed method was applied to mini-drone video dataset [2] provided by the organizers of MediaEval 2015 Drone Protect Task [1]. The dataset contains short clips captured by a surveillance mini-drone. Each clip is annotated by human observers to mark the sensitive ROIs and the privacy level for each ROI.

2. FALSE COLOR BASED PRIVACY PROTECTION

The main idea in false color based privacy protection is in transforming colors of pixels in a frame such that the private information becomes unrecognizable while the impact on intelligibility is kept as small as possible. Previous work on false coloring has demonstrated the applicability of such an approach for privacy protection against both human observers and automatic face recognition algorithms [4].

This algorithm first converts a color frame into grayscale. The pixel intensities of the grayscaled frame are then used as keys to a look-up a table that represents a color palette. Optionally, the grayscale frame can be compressed or quantized to further distort the visual information prior to table look-up. The pixel values of the original frame are then replaced by the values from the table. This algorithm can be applied on an entire frame or on one or more ROIs. The strength of the protection is controlled by the color distribution of the selected color palette (Figure 1).

The protected frames can be reversed to obtain a close approximation of the originals by performing an inverse table look-up. However, due to the initial grayscale conversion, the recovered frames will be in grayscale. Also, if the look-up table contains duplicate values, full recovery may not be possible due to the initial many-to-one mapping. Finally, the reversion is only possible if one knows the properties of the color map used during protection. Thus, security can be enhanced by utilizing a custom color palette.

*Currently with Idiap research institute (Switzerland)

MediaEval 2015 Workshop, Sept. 14-15, 2015, Wurzen, Germany

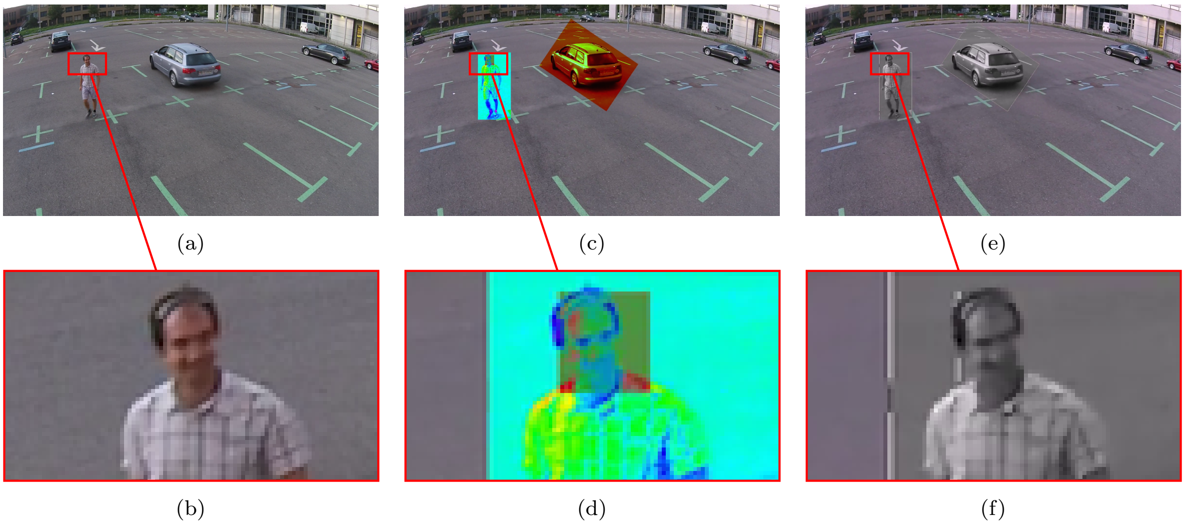

Figure 2: False color results, *a*) original frame, *c*) protected frame, *e*) recovered frame.

3. EVALUATION RESULTS

We applied false coloring to the annotated ROIs of the provided mini-drone dataset [2] using the following color maps: Radiance default (DEF) for high, rainbow color scale (RBS) for medium, and linearized optimal color scale (LOCS) for low privacy regions. This selection was motivated by the effectiveness of each color map for privacy protection as determined by earlier work [4].

A sample result is shown in Figure 2, where (a) represents an original video frame, (c) its privacy protected version, and (e) its recovered version. The close-up views can be observed in the bottom row. It can be noted in (c) and (d) that the face of the individual is represented in the DEF color scale, whereas his body is represented in the RBS color scale. The vehicle, on the other hand, is represented in the LOCS color scale based on expert annotations.

The recovered ROIs shown in (e) and (f) do not contain color information and have some artifacts near the ROI boundaries. This is due to the compression of the protected frames. As the compression works at block rather than pixel level, the false colored pixels affect the colors of the neighboring pixels and are not corrected during the inverse look-up.

The MediaEval benchmarking results reported in Table 1 show that our intelligibility and pleasantness scores are above the average of all submissions whereas the privacy level score is below the average. This can be explained by the fact that false coloring is a point operation and, unlike most other methods, it does not introduce structural distortions. Nevertheless, privacy level could be improved by using custom color palettes that are better tailored to privacy protection.

Table 1: Evaluation results where FC and AVG respectively stand for false color results and the average of all submissions. Expert and Naïve's are participant groups which represent the people conducting research on visual privacy protection and naïve observers.

	Privacy		**Intelligibility**		**Pleasantness**	
	FC	AVG	FC	AVG	FC	AVG
Expert	0.39	0.49	0.76	0.59	0.73	0.60
Naïve	0.34	0.48	0.75	0.58	0.75	0.61
Average	0.365	0.49	0.755	0.59	0.74	0.60

4. CONCLUSION

In this paper, we described a simple and effective method for protecting privacy using false coloring. Benchmarking evaluations indicated high preference for the pleasantness and intelligibility of this method, whereas it was found to be less effective for preserving privacy. Future work will investigate designing custom color scales to improve privacy protection and the quality of reversibility while enhancing security.

5. ACKNOWLEDGEMENTS

The work was conducted in the framework of FP7 NoE VideoSense and TUBITAK project number 114E445.

6. REFERENCES

[1] A. Badii, P. Korshunov, H. Oudi, T. Ebrahimi, T. Piatrik, V. Eiselein, N. Ruchaud, C. Fedorczak, J.-L. Dugelay, and D. F. Vazquez. Overview of the MediaEval 2015 drone protect task. In *MediaEval 2015 Workshop*, Wurzen, Germany, Sept. 2015.

[2] M. Bonetto, P. Korshunov, G. Ramponi, and T. Ebrahimi. Privacy in Mini-drone Based Video Surveillance. In *Workshop on De-identification for privacy protection in multimedia*, 2015.

[3] S.-C. Cheung, M. Venkatesh, J. Paruchuri, J. Zhao, and T. Nguyen. Protecting and managing privacy information in video surveillance systems. In *Protecting Privacy in Video Surveillance*, pages 11–33. 2009.

[4] S. Çiftçi, P. Korshunov, A. O. Akyüz, and T. Ebrahimi. Using false colors to protect visual privacy of sensitive content. In *SPIE Human Vision and Electronic Imaging XX*, pages 93941L–93941L–13, 2015.

[5] F. Dufaux and T. Ebrahimi. Scrambling for Privacy Protection in Video Surveillance Systems. *IEEE Trans. on Circuits and Systems for Video Technology*, vol. 18(no. 8):1168–1174, 2008.

[6] P. Korshunov and T. Ebrahimi. Using Warping for Privacy Protection in Video Surveillance. In *18th International Conference on Digital Signal Processing (DSP)*, 2013.