Privacy Protection Filter Using *StegoScrambling* in Video Surveillance

Natacha Ruchaud
Eurecom
450 Route des Chappes
Biot Sophia antipolis, France
ruchaud@eurecom.fr

Jean Luc Dugelay
Eurecom
450 Route des Chappes
Biot Sophia antipolis, France
dugelay@eurecom.fr

ABSTRACT

This paper introduces a new privacy filter adopted in the context of the *DPT (Drone Protect Task)* at MediaEval Benchmark 2015. Our proposed filter protects privacy by visually replacing sensitive RofI (Regions of Interest) by its shapes. A combination of steganography and scrambling is used in order to make this filter. Once the scrambling is applied on the pixels of the RofI, its MSB (Most Significant Bit) are hidden in the LSB (Least Significant Bit) of a cover image. Our filter fulfils four criteria defined by DPT: near-lossless reversibility, intelligibility, appropriateness and anonymization. We benchmarked the filter on the last three criteria and we get good results: 40 % for intelligibility and appropriateness, and 60 % for anonymization.

1. INTRODUCTION

Due to the growing of video surveillance systems and the significant improvement of automatic recognition tools, privacy protection techniques became a necessity. Moreover, these systems benefit from image sensors progress (e.g. people are recognized far away from the camera).

Here examples of already existing systems protecting privacy: pixelization, blurring or black masking with FacePixelizer [1] on Google plus, ObscuraCam [2] on Android, and also scrambling in JPEG compression with Scrambling JPEG tool [3]. Besides, people are working on methods to hide identity such as morphing [5], warping [5] and scrambling [6], but they are complex and the degradation they apply on the images prevent any usage for security purpose (lack of intelligibility).

The use-case scenario designed for the challenge was Car Park Security. The goal was the creation of privacy filtering solutions for drone videos related to public safety. They are evaluated by following four criteria:

i) protection of privacy,

ii) intelligibility for the visual quality in order to recognize events on the result (i.e. people walking, running, fighting, stealing...),

iii) appropriateness to see if the result is good looking,

iv) possibility to reverse to come back to the original image.

Privacy filter presented in [2] fails to be near-lossless reversible unlike scrambling [4]. Nevertheless, scrambling fails to recognize events easily because of the amount of noise.

Our proposed filter conceals privacy information and keep the comprehensibility of the video in order to detect events.

2. STEGOSCRAMBLING FILTER

RofI (e.g. people, vehicles or accessories bounding boxes) are previously annotated in the database [2] used for *DPT* [1].

To hide information, an XOR is computed between the six MSBs of the RofI and the random numbers generated with a PRG (pseudorandom generator) controlled by a seed, as expressed in the equation 1.

$$XORImg(i) = RofI(i) \oplus RandNums(i), \forall i \qquad (1)$$

with i the bit position and each bit $\in \{0, 1\}$.

In parallel, cover images are computed to replace RofI and keep the possibility to recognize events. An edge detector and a Kmeans clustering [3] (limited to two clusters, similar to a binarization) are applied in the RGB space of the RofI containing people. An AND is computed between the edges of the RofI and the resulting clusters of the images on each pixel, by multiplying them as shown in the equation 2.

$$CoverImg = EdgeImg. * KmeansClustering, \qquad (2)$$

with .* the Element-by-element multiplication.

The convex hull image from the binary cover image for people is generated in order to become the RofI containing people. RofI containing car or accessories use(s) only K-means clustering as cover image.

Next, the 2 MSBs of the cover image, where the pixels intensity is either 192 or 0, are inserted in the 2 MSBs of the resulting image. Finally, the 6-bit of the XOR image, where pixels intensity is between 0 and 63, are integrated in the LSB of the resulting image as shown in the equation 3. Therefore, only cover images are visible by viewers in order to recognize events.

$$ProtectedImg = \sum_{i=0}^{5} XORImg(i) * 2^i + \sum_{i=6}^{7} CoverImg(i) * 2^i, \qquad (3)$$

Figure 1 illustrates the workflow of the proposed method and Figure 2 shows an example of an entire privacy image.

[1] http://www.facepixelizer.com/
[2] https://guardianproject.info/apps/obscuracam/
[3] http://ltslinux18.epfl.ch/scramble/

MediaEval 2015 Workshop, September 14-15, 2015, Wurzen, Germany

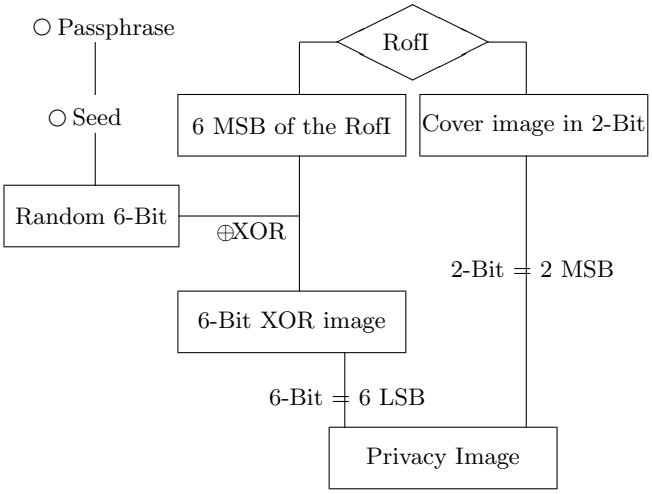

Figure 1: Workflow of the proposed process

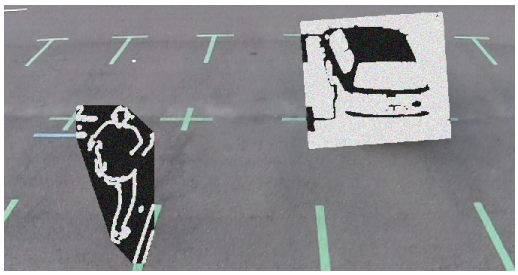

Figure 2: Illustration of the proposed filter

To recover the original RofI, the inverse process is applied as shown in the equation 4. Two LSBs are removed from the original RofI, thus, a maximum error rate of 3 may be produced between an original pixel and a recovered pixel. This error implies no impact for human vision and is negligible for machines.

$$Recovered = \sum_{i=2}^{7} (ProtectedImg(i-2) \oplus RandNums(i)) * 2^i \quad (4)$$

2.1 Pixel example

One pixel is considered with 8-bit from MSB to LSB.

Original pixel	$b7$	$b6$	$b5$	$b4$	$b3$	$b2$	$b1$	$b0$

For each pixel of the RofI, only the MSB bits between 2 and 7, are preserved. An XOR is computed between the MSB of the original pixel and a random number. The result is denoted b'.

XORpixel, b'	$b'7$	$b'6$	$b'5$	$b'4$	$b'3$	$b'2$	X	X

The bits of b' are shifted in the six LSBs.

XORpixel, b'	X	X	$b'7$	$b'6$	$b'5$	$b'4$	$b'3$	$b'2$

Two MSBs of a white and black pixel are represented by $e_6 = 1$ and $e_7 = 1$ for the former, and $e_6 = 0$ and $e_7 = 0$ for the latter. Finally, the two MSBs of e are added with the six LSBs of b'. The result is denoted, protected pixel.

Edge pixel, $b'+e$	1	1	$b'7$	$b'6$	$b'5$	$b'4$	$b'3$	$b'2$
No-edge pixel, $b'+e$	0	0	$b'7$	$b'6$	$b'5$	$b'4$	$b'3$	$b'2$

To recover the original pixel, an XOR is computed between the same random number than previously, and the six LSBs of the protected pixel.

Recovered pixel	$b7$	$b6$	$b5$	$b4$	$b3$	$b2$	X	X

The process is mostly reversible because the two LSBs, denoted $b0$ and $b1$ are lost.

3. EVALUATION RESULTS

We tested our proposed filter on different video sequences from DronesProtect dataset [2]. The guidelines of the MediaEvel 2015 DroneProtect Tasks [1] are followed to perform the evaluation. This evaluation is based on the human-perceived and interpretation of the resulting privacy filtered videos in terms of level of privacy, intelligibility and appropriateness.

The aim of the challenge is to find a trade-off between privacy and visual quality of the protected image. Indeed, the higher is the protection, the lower is the level of information (see intelligibility and appropriateness).

Two human evaluator groups are selected. In the first group, people come from surveillance security domain (R & D), and in the second group they come from any other domain (Naive).

In Table 1, we report the average results of our filter. We obtained positive feedbacks from the jury and especially for the privacy protection. Indeed, according to the results 60 % of privacy is well protected. However, we got 40 % for intelligibility and appropriateness; this shows a lack in our filter for recognizing events properly. This can be explained because the edges detector makes mistakes and also colors of RofI are turned to black and white. It is planned as future work to improve the edges detection method with a new design for the cover image, in order to be better tailored to release more information and having a better event recognition.

Table 1: Average results (%)

Evaluation	Privacy	Intelligibility	Pleasantness
`Category 1 (R&D)`	0.63	0.37	0.36
`Category 2 (Naive)`	0.57	0.43	0.48
`Average (%)`	0.6	0.4	0.4

4. CONCLUSIONS

We presented a new privacy filter applied on videos in a car park from drone. The novelty of the work is to combine a scrambling to encrypt privacy-sensitive RofI, and a steganography to hide this scambled RofI in a cover image represented by its edges.

5. REFERENCES

[1] A.Badii, P.Koshunov, H.Oudi, T.Ebrahimi, T.Piatrik, V.Eiselein, N.Ruchaud, C.Fedorczak, JL.Dugelay, and D. 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*, number EPFL-CONF-206109, 2015.

[3] H. Fradi, Y. Yan, and J.-L. Dugelay. Privacy protection filter using shape and color cues. In MediaEval 2014 Workshop, Barcelona, Spain, October, 2014.

[4] J. Hu and F. Han. A pixel-based scrambling scheme for digital medical images protection. *Journal of Network and Computer Applications*, 32(4):788–794, 2009.

[5] P. Korshunov and T. Ebrahimi. Towards optimal distortion-based visual privacy filters. In *IEEE International Conference on Image Processing*, number EPFL-CONF-197087, 2014.

[6] A. Melle and J.-L. Dugelay. Scrambling faces for privacy protection using background self-similarities. In *Image Processing (ICIP), 2014 IEEE International Conference on*, pages 6046–6050. IEEE, 2014.