Privacy Protection Filter Using StegoScrambling in Video Surveillance
Natacha Ruchaud

To cite this version:
Natacha Ruchaud. Privacy Protection Filter Using StegoScrambling in Video Surveillance. MediaEval, Sep 2015, Wurzen, Germany. hal-01367560

HAL Id: hal-01367560
https://hal.archives-ouvertes.fr/hal-01367560
Submitted on 16 Sep 2016

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
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 RoI (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 RoI, its MSB (Most Significant Bit) are hidden in the LSB (Least Significant Bit) of a cover image. Our filter fulfills 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 of 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

RoI (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 RoI and the random numbers generated with a PRG (pseudorandom generator) controlled by a seed, as expressed in the equation 1.

\[
XORImg(i) = RoI(i) \oplus RandNums(i), \forall i
\]  

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

In parallel, cover images are computed to replace RoI 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 RoI containing people. An AND is computed between the edges of the RoI and the resulting clusters of the images on each pixel, by multiplying them as shown in the equation 2.

\[
CoverImg = EdgeImg.*KmeansClustering,
\]  

with * the Element-by-element multiplication.

The convex hull image from the binary cover image for people is generated in order to become the RoI containing people. RoI containing car or accessories use(s) only Kmeans 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.

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

Figure 1 illustrates the workflow of the proposed method and Figure 2 shows an example of an entire privacy image.
To recover the original pixel, the inverse process is applied as shown in the equation 4. Two LSBs are removed from the original pixel and a recovered pixel. This error implies no impact for human vision and is negligible for machines.

\[ Recovered = \sum_{i=2}^{e}(ProtectedImg(i-2) \oplus RandNoms(i)) \times 2^2 \]  

\[ (4) \]

### 2.1 Pixel example

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

<table>
<thead>
<tr>
<th>Original pixel</th>
<th>67</th>
<th>66</th>
<th>65</th>
<th>64</th>
<th>63</th>
<th>62</th>
<th>61</th>
<th>60</th>
</tr>
</thead>
</table>

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 \( b' \).

<table>
<thead>
<tr>
<th>XORpixel, ( b' )</th>
<th>67</th>
<th>66</th>
<th>65</th>
<th>64</th>
<th>63</th>
<th>62</th>
<th>61</th>
<th>60</th>
</tr>
</thead>
</table>

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

<table>
<thead>
<tr>
<th>XORpixel, ( b' )</th>
<th>67</th>
<th>66</th>
<th>65</th>
<th>64</th>
<th>63</th>
<th>62</th>
<th>61</th>
<th>60</th>
</tr>
</thead>
</table>

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.

### 3. EVALUATION RESULTS

We tested our proposed filter on different video sequences from DronesProtect dataset [2]. The guidelines of the MediaEval 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.

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>
<thead>
<tr>
<th>Evaluation</th>
<th>Privacy</th>
<th>Intelligibility</th>
<th>Pleasantness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category 1 (R&amp;D)</td>
<td>0.63</td>
<td>0.37</td>
<td>0.36</td>
</tr>
<tr>
<td>Category 2 (Naive)</td>
<td>0.57</td>
<td>0.43</td>
<td>0.48</td>
</tr>
<tr>
<td>Average (%)</td>
<td>0.6</td>
<td>0.4</td>
<td>0.4</td>
</tr>
</tbody>
</table>

### 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 scrambled RofI in a cover image represented by its edges.

### 5. REFERENCES


