A Novel Video Watermarking Approach Based on Implicit Distortions

Hannes Mareen, Johan De Praeter, Glenn Van Wallendael and Peter Lambert
Ghent University – imec, IDLab, Department of Electronics and Information Systems, Ghent, Belgium
Email: {hannes.mareen, johan.depraeter, glenn.vanwallendael, peter.lambert}@ugent.be

***Abstract*—In order to protect videos from copyright infringement, a watermarking approach is proposed based on implicit distortions generated by a video encoder, rather than artificial distortions used in the state-of-the-art. These distortions are imperceptible and robust against video manipulations.**

I. Introduction

Copyright-sensitive videos are commonly leaked or illegally distributed by so-called digital pirates. Typical security measures involving the encryption and decryption of multimedia are not sufficient to protect video owners from copyright infringement [1], since pirates might legally acquire those videos before illegally leaking or distributing them. For example, trusted critics and award voters regularly receive screeners of a film or TV series before they are officially released. However, some critics with malicious intentions may upload the videos to torrent sites.

In order to protect video copyrights, watermarking techniques have been developed that consist of hiding a unique watermark in every video that contains information of the receiver. If the video is then illegally distributed, the copyright owner can extract the watermark and identify the malicious receiver. However, pirates may manipulate the video in the hope of destroying the embedded watermark. Therefore, it is important for the watermark to be robust, i.e. it should survive common video manipulations such as a re-encoding with lower quality. Additionally, the watermark should be hidden imperceptibly, such that honest users are not bothered by the security measure.

Several watermarking techniques exist, although only few are both imperceptible and provide a high level of robustness [2]. Watermarking methods can be classified as either correlation-based or noncorrelation-based [3]. Correlation-based methods rely on certain distortions introduced during the embedding phase. These distortions can be correlated to the observed distortions in the pirated video. If the resulting correlation value is high, the watermark is detected. Usually, the embedded watermark is represented as noise [4]. On the other hand, noncorrelation-based techniques embed and extract the watermark in a different way, often based on a variation of least-significant-bit modification in selected transform coefficients or based on an artificially-created relationship between certain bitstream components [3], [5].

The above existing robust techniques explicitly add many distortions to the video. Even though these distortions are usually imperceptible, it is questionable whether adding such artificial, unnatural distortions is desirable. Therefore, new approaches should be investigated.

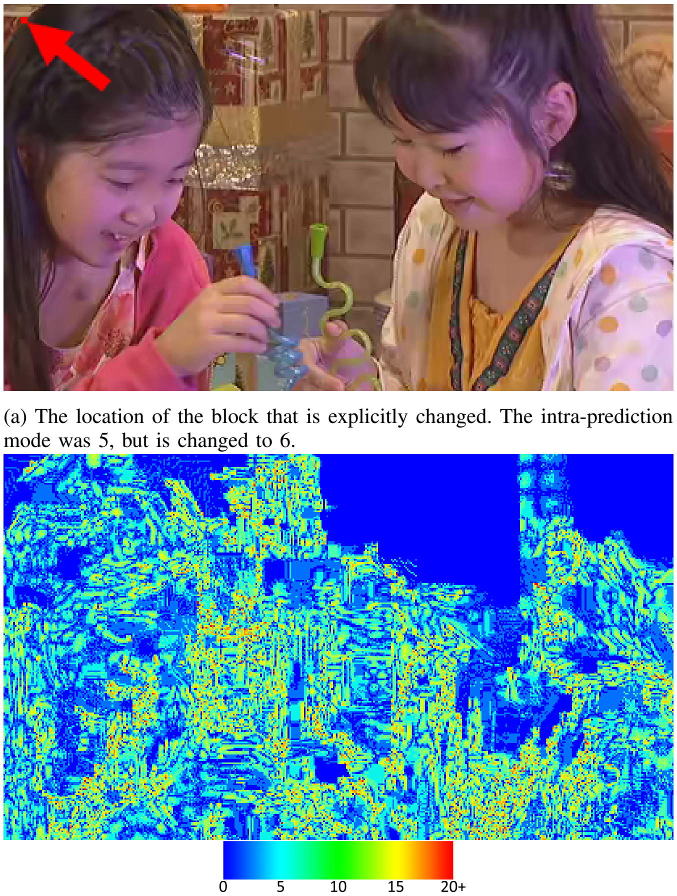
As its main novelty, this paper proposes a watermarking scheme for videos that uses implicit distortions generated by a video encoder, contrary to the artificial distortions used in the state-of-the-art. The scheme aims to be both robust and imperceptible, thus being applicable to the distribution of copyright-sensitive multimedia. Moreover, although the proposed scheme is implemented using the reference software (HM 16.5) of the H.265/High Efficiency Video Coding (HEVC) standard, the underlying ideas are applicable to other standards as well.

II. Proposed watermarking scheme

Most existing techniques explicitly make many artificial changes in a video in order to hide a watermark. The embedding scheme proposed here, on the other hand, explicitly modifies only a few coding decisions when a video is encoded with a watermark, while preserving all other coding decisions as when encoding the video without a watermark. By explicitly changing a coding decision in a certain region, some pixels in that region will be slightly different than when the optimal coding decision is used. Then, due to intra- and inter-frame prediction, these small differences will propagate into many so-called implicit distortions.

Note that, since the explicit changes are made during the encoding process and hence the encoding loop is always closed, no drift-error propagation occurs. Instead, the implicit distortions are assumed to be imperceptible because the encoder still tries to resemble the original video as closely as possible. As a result, they are ordinary encoder-created distortions, similar to distortions that are also present in unwatermarked videos. Fig. 1 illustrates the creation of implicit distortions by showing the first frame of the video *BlowingBubbles*, the location of a block in that frame of which the intra-prediction mode was explicitly changed, and the resulting distortion map.

Every watermark can be represented by a unique, small collection of explicit changes and, as a result, by a unique, large collection of implicit distortions. Then, in order to detect the watermark, correlation-based techniques can be used to correlate the implicit distortions of a watermark with the ones observed in a pirated video. Several correlation measures exist, such as the correlation coefficient (z_{cc}), which is an extension of the normalized correlation (z_{nc}) [6]. These measures are defined as in equation 1, in which o and w are vectors of pixels, representing the observed and watermarked video,



(a) The location of the block that is explicitly changed. The intra-prediction mode was 5, but is changed to 6.

(b) A visualization of the resulting implicit distortions. Blue means that the corresponding pixel is not changed in Y value, whereas red means a change of 20 or higher in Y value. A Y value is represented by 8 bit, i.e. it can range from 0 to 255.

Fig. 1. By explicitly changing a single coding decision (a), many implicit distortions are created (b).

respectively. Additionally, $|o|$ and $|w|$ represent the Euclidean length of the vectors o and w, respectively, and $\bar{o}$ and $\bar{w}$ represent the mean pixel values of o and w, respectively.

$$\begin{aligned} z_{nc}(o,w) &= \sum_i \frac{o[i]}{|o|} \cdot \frac{w[i]}{|w|}, \\ z_{cc}(o,w) &= z_{nc}(o-\bar{o}, w-\bar{w}) \end{aligned} \tag{1}$$

Fig. 2 illustrates the robustness of the proposed watermarking technique. The video *BlowingBubbles* is watermarked 2433 times, each time changing a different intra-prediction mode in the first frame of the video. Then, watermarked video nr. 1000 is attacked by re-encoding it with a bit rate equal to 10% of the original, i.e. a bit rate reduction of 90%. The figure shows the correlation coefficients between the attacked video and all watermarked videos. A single clear outlier can be detected with the highest correlation, which corresponds to watermark nr. 1000. In other words, even after a strong re-encoding attack, the watermark is correctly detected. The sequences *RaceHorses*, *BasketballDrill*, *FourPeople*, *Johnny*, *BasketballDrive* and *Traffic* have been evaluated as well and showed similar behavior.

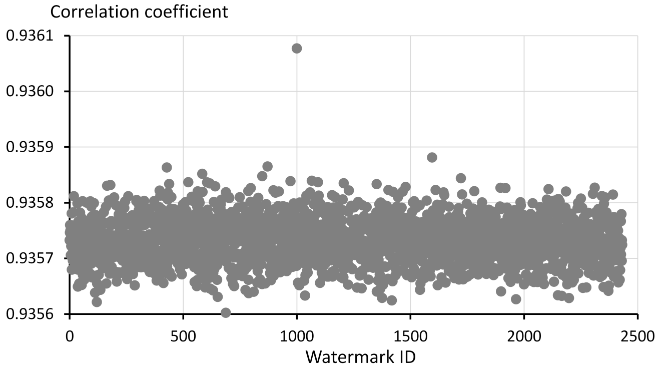


Fig. 2. The correlations between an attacked watermarked video (nr. 1000) and all watermarked videos.

III. Conclusion

In order to create a robust and imperceptible watermarking scheme, this paper proposed a novel approach in which watermarks are represented as a large collection of so-called implicit distortions, automatically generated by an encoder in which only few coding decisions are explicitly changed. Then, correlation-based detection techniques can be performed.

Consequently, the proposed scheme can be applied to help combat piracy by identifying malicious users that illegally distribute the video, even when they significantly lower the video quality. Moreover, innocent users are not bothered by unnatural distortions since the implicit distortions are ordinary encoder-created distortions and hence imperceptible.

Acknowledgment

The computational resources (STEVIN Supercomputer Infrastructure) and services used in this work were kindly provided by Ghent University, the Flemish Supercomputer Center (VSC), the Hercules Foundation and the Flemish Government department EWI.

References

[1] A. Boho, G. Van Wallendael, A. Dooms, J. De Cock, G. Braeckman, P. Schelkens, B. Preneel, and R. Van de Walle, "End-to-end security for video distribution," *IEEE Signal Processing Magazine*, vol. 30, no. 2, pp. 97–107, 2013.

[2] S. Bhattacharya, T. Chattopadhyay, and A. Pal, "A Survey on Different Video Watermarking Techniques and Comparative Analysis with Reference to H.264/AVC," in *2006 IEEE International Symposium on Consumer Electronics*, 2006, pp. 1–6.

[3] G. C. Langelaar, I. Setyawan, and R. L. Lagendijk, "Watermarking digital image and video data. A state-of-the-art overview," *IEEE Signal Processing Magazine*, vol. 17, no. 5, pp. 20–46, Sep 2000.

[4] F. Hartung and B. Girod, "Watermarking of uncompressed and compressed video," *Signal processing*, vol. 66, no. 3, pp. 283–301, 1998.

[5] K. Ogawa and G. Ohtake, "Watermarking for HEVC/H.265 stream," in *2015 IEEE International Conference on Consumer Electronics (ICCE)*, Jan 2015, pp. 102–103.

[6] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, *Digital Watermarking and Steganography*, 2nd ed. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 2008.