A ROBUST FRAME-BASED TECHNIQUE FOR VIDEO WATERMARKING

R. Caldelli[a] , M. Barni[b] , F. Bartolini[a] and A. Piva[a]
[a] Department of Electronics and Telecommunications, University of Firenze
Via S. Marta 3, 50139 - Firenze, ITALY
e-mail: {caldelli, barto, piva}@lci.die.unifi.it
[b] Department of Information Engineering, University of Siena
Via Roma 56, 53100 - Siena, ITALY
e-mail: barni@dii.unisi.it

ABSTRACT

During the last few years multimedia systems success has been definitely spurred by the development of network-based on line services, like electronic commerce, teleducation, teletraining, media distribution and so on, in which multimedia systems have a major role. In this new scenario the request for privacy, security and authenticity of the documents, undergone to these transactions, is strongly upcoming.
Watermarking techniques, deriving from information hiding theory, have been suggested so far as an effective and suitable solution to satisfy this kind of requirements, and in a short time many and disparate algorithms applying different strategies to achieve the same goal have been proposed in scientific literature and by commercial entities. In this paper a watermarking algorithm, originally conceived for still images applications, has been extended to raw video, treating it as a set of single still frames. A good robustness against usual image processing and geometric manipulations has been achieved, moreover experiments with MPEG2 coding/decoding at different bit rates have been carried out giving positive results.

1 INTRODUCTION

By watching what has been happening during the last few years and what is probably going to come about in the next, it seems to be clear that a novel and powerful commercial opportunity has been provided to the multimedia market, thanks to the huge development of WWW, digital networks and multimedia. This new way of easily contacting potential worldwide spreaded purchasers has attracted either usual media distributors or new entities commonly not involved in this sort of issues. But as it happens for any marketable product, also in this case, a pressing request related to the need to safeguard goods ownership rights has been raised. Due to the ease by which digital material can be copied quickly without loss of quality, the demand for data protection has been growing unexpectedly and a way to securely defend digital documents had to be indicated.
So far digital watermarking has been suggested as an effective solution answering to this kind of requirements and much research has been made in this area. All these studies have developed into different techniques for hiding watermarks and an increasingly robustness to intentional and unintentional attacks has been shown. Attention has been dedicated to each one of the various media (audio [5], text [6], images [1, 3, 4], and video [2, 9, 10]), to succeed in embedding, separately in each kind of content, useful information regarding it.
In this paper we will focus on video watermarking and we will analyse how some specific technologies designed for a different kind of application, thanks to their versatility, can be applied to another one. In fact in Section 2 a particular raw-video oriented application, based on a watermarking algorithm [8] originally built for still images, is presented. Moreover in Subsection 2.3 some detailed considerations about robustness this approach offers are taken. In Section 3 experimental results confirming a good performance of the algorithm versus attacks like geometric transformations and MPEG2 coding/decoding are proposed and finally brief conclusions are drawn.

2 PROPOSED WATERMARKING TECHNIQUE

The proposed approach consists in applying a tested and well-performing watermarking technique [8], originally devised for still images, to non-coded video, by considering it as a collection of single frames. In the following two subsections the algorithm will be roughly described and then the main features of the approach used for video watermarking will be explained.

2.1 Watermarking of Still Images

The watermark casting is carried out, as described in [8], extracting the brightness of the to-be-marked frame, computing its full-frame DFT (Discrete Fourier Transform) and then taking the magnitude of the coefficients. The watermark is embedded by slightly modifying the magnitude of some DFT coefficients, belonging to a specific middle frequency region of the transformed domain, successively the IDFT (Inverse DFT) is performed to obtain the watermarked image. Moreover to better preserve the original quality of the single frame, a particular masking operation, exploiting knowledge of the characteristics of the HVS (Human Visual System), is accomplished. In the detection step the luminance of the image to be checked for watermark presence is extracted and the magnitude of its DFT is considered again; only who knows the private code strings, used during the coding phase, is able to generate the exact code to look for. An optimum criterion to verify if the mark is present in the image is derived, based on statistical decision theory. This kind of watermark is detectable, unperceivable and presents a good robustness to the usual image processing as linear/non-linear filtering, sharpening, JPEG compression and so on; furthermore resistance to geometric transformations as scaling, rotation, cropping, etc., is well-granted thanks to the insertion of a template during the coding step. With this method the original unmarked image is not needed to perform the detection phase, i.e. the technique can be defined as blind, besides, the algorithm permits the insertion/detection of multiple marks, to possibly manage multiple ownership situations.

2.2 Watermarking of Video Sequences

Many different techniques oriented to video watermarking have been recently developed. These algorithms can be divided in two basic separate categories on the basis of which kind of video they deal with: some of them work directly in the MPEG2/MPEG4 coded domain by embedding the watermark in the bit-stream [12], on the contrary, others need a non-coded video [11] to be able to insert a mark in an appropriate way. Both seem to show advantages and drawbacks as well, either from the point of view of robustness or from the point of view of computational complexity.

Here an application of the watermarking algorithm, described in the previous subsection, to non-coded video sequences, processing each frame in a distinct and different way [7], is presented. In fact, thanks to the used watermarking technique, the inserted code is frame-dependent and though the private key is always the same, the mark really introduced in the image is diverse every time. Doing so we will embed correlated watermarks between correlated frames and uncorrelated watermarks between uncorrelated frames, allowing changes, due to code insertion, to adapt gracefully to the video content. Practically a set of still images is available and only those frames which have to be watermarked, are passed to the marker, the others are let unaltered. Obviously dealing with raw video allows to achieve video-coding format independence and moreover to be able to choose how many and which are the frames to be marked. In particular for this application it has been decided to watermark the first frame of each GOP (Group Of Pictures), which was composed of 12 frames, leaving the other ones uncorrupted. Being frame rate equal to 25 frame/sec, this approach grants that at least 2 frames per second are marked and this would seem to be a considering part with respect to video length. Anyway if a superior protection is needed a higher number of frames can be marked, at most the entire GOP. Moreover by-passing most of frames without changes (referring to this application case 11/12 that is 91.6%) results in a good preserving of the whole video quality. Other experiments have been carried out by marking one frame every six, that is two in a GOP, or frames located in intermediate positions of GOP, for example the ninth or the eleventh one; these changes have led to similar conclusions as in the above considered case.

During the detection phase all the video is checked for the mark presence, not only the first frame of each GOP, in such a way a syncronization of the stream is not required and the knowledge of the exact position within the sequence, is not needed, as it would seem to be for other algorithms [2]. When the checked code is found, that is the detector response has got a peak over the established threshold, it means that the video contains at least a watermarked frame; the process could go on with its search into the remaining part of video, but it would not be necessary if a more accurate validation is not specifically wanted. Therefore the revealing process might be stopped, after a sufficient number of positive check of watermark presence is reached, thus resulting in a saving of computational time, obviously this is true only if the watermark has been detected, in the case of no-detection the whole video has to be definitely checked.

2.3 Robustness Evaluation

The possibility to decide to watermark one or more frames in a GOP (at most all of them), together with the fact of considering each frame as a still image [10] yield some important advantages from a robustness point of view. First a trade-off between time spent for marking and the degree of robustness needed for the sequence can be achieved, in other words the lower the number of watermarked frames in the GOP, the faster the coding phase, but, conversely, just a minor part of the video stream will be watermarked, thus causing a robustness decrease; obviously if a superior security has to be obtained a higher amount of frames might be considered. Moreover, if some attacks like frames exchange or frames dropping/replacing, which do not result in a strong video quality degradation, are applied to the watermarked sequence, it will always be possible to reveal the watermark; in the first case its position will be different with respect to the code insertion phase, and in the second one the mark may be found in the remaining watermarked frames belonging to the same GOP or to the other successive ones. Experiments carried out in this direction have confirmed these assumptions. Furthermore it has been verified that MPEG2 coding/decoding operations, at various and lower bit-rates, do not harm to the correct watermark detection. Thanks to the good robustness the watermarking algorithm had already shown in the case of still images against usual image processing as linear/non-linear filtering, noise addition, JPEG compression, etc., and geometric transformations as rotation, scaling, cropping, etc., also for video applications these longed-for characteristics are held.

3 EXPERIMENTAL RESULTS

In this section some experimental results to point out how the proposed approach really works and its robustness particularly against geometric manipulations and MPEG2 coding/decoding, at various bit-rates, are shown.

The results obtained with a video sequence, named *Quintana*, in which a medieval banquet is represented, are proposed. The sequence is composed by 250 frames ($4 : 2 : 2$ PAL format) of size 720×576 pixels and has been first watermarked and then MPEG2 coded at 6 Mbit/sec at 25 frame/sec.

In Fig.1(a) and Fig.1(b) the frame 36 of the watermarked video and the relative detector response have been depicted respectively. The whole video is checked for the mark presence; the watermarking code is revealed when the detector response is higher than the established threshold; in Fig.1(b) the difference between the response and the threshold is visualized, so when a watermarked frame is detected a positive spike is obtained. Going through the 250 frames a set of periodical peaks ($1/12$ in this test case) is displayed.

In Fig.2(a) the same frame of the test video is pictured. Now the sequence has undergone a geometrical composite attack as a 15 degrees rotation, then an asymmetric scaling to 1000×900 pixels and finally a cropping to the original size. Like the above case, the respective detector response is proposed on the right; because of the transformations occurred the spikes, though still well distinguishable, have a height lower than before and moreover two peaks in the middle of the sequence are missed, but, as explained in Section 2.3, this does not invalidate the extraction process at all.

In the end, as third robustness test, another kind of attack is considered: a MPEG2 coding where bit-rate is reduced to half, in this case from 6 Mbit/sec to 3 Mbit/sec (in Fig.3(a) frame 36 is depicted again). As it can be seen in Fig.3(b) the detector is always able to exactly reveal the mark, there are no missed frames, but the height of the peaks is lower with respect to the first case, obviously that is due to the MPEG2 coding with a decreased bit-rate.

4 CONCLUSIONS

In the present paper the attempt to apply to raw video watermarking a technique initially designed only to deal with still images has been presented. Moreover, to support the goodness of this methodology, some advantages either from the point of view of the possibility of tuning the choice of which and how many frames have to be watermarked, or from the point of view of the good robustness against different sort of attacks video can be undergone, like frames exchange or frames dropping/replacing, have been highlighted. Finally experimental results confirming the effective behaviour of this technique particularly in presence of composite geometric manipulations and MPEG2 coding/decoding operations, involving bit-rate changes, have been presented.

REFERENCES

[1] M. Barni, F. Bartolini, V. Cappellini, and A. Piva, ”Copyright protection of digital images by embedded unperceivable marks”, *Image and Vision Computing*, vol.16, pp. 897–906, August 1998.

[2] F. Hartung and B. Girod ”Digital Watermarking of Raw and Compressed Video”, N. Ohta editor, Digital Compression Technologies and Systems for Video Communications, volume 2952 of SPIE Proceedings Series, pp. 205-213, October 1996.

[3] M. D. Swanson, M. Kobayashi, A. H. Tewfik, ”Multimedia data-embedding and watermarking technologies”, *Proceedings of the IEEE*, vol. 86, pp. 1064–1087, June 1998.

[4] S. Craver, N. Memon, B. L. Yeo, M. M. Yeungraver, ”Resolving rightful ownership with invisible watermarking techniques: limitations, attacks and implications”, *IEEE Journal of Selected Areas in Communications*, vol 4, pp. 573–586, May 1998.

[5] V. Basia and I. Pitas, ”Robust Audio Watermarking in the time-domain”, Proc. of EUSIPCO’98, Rhodes, Greece, September 1998.

[6] A.K. Choudhury, N.F. Maxemchuk, S. Paul, and H.G. Schulzrinne, ”Copyright Protection for Electronic Publishing over Computer Networks”, IEEE Network, v. 9 no. 3, pp. 12-20, May/June 1995.

[7] M. Holliman, W. Macy and M. M. Yeung, ”Robust frame-dependent video watermarking” to appear in volume 3971 of SPIE Proceedings Series, January 2000.

[8] A. Piva, M. Barni, F. Bartolini, V. Cappellini, A. De Rosa, M. Orlandi, ”Improving DFT Watermarking robustness through optimum detection and synchronisation”, Proc. Of ACM Workshop on Multimedia and Security ’99, Orlando, Florida, October 1999.

[9] Gabriella Csurka, Frédéric Deguillaume, Joseph J. K. Ó Ruanaidh and Thierry Pun, ”A Bayesian approach to affine transformation resistant image and video watermarking”, International Workshop on Information Hiding, Dresden, Germany, September/October 1999.

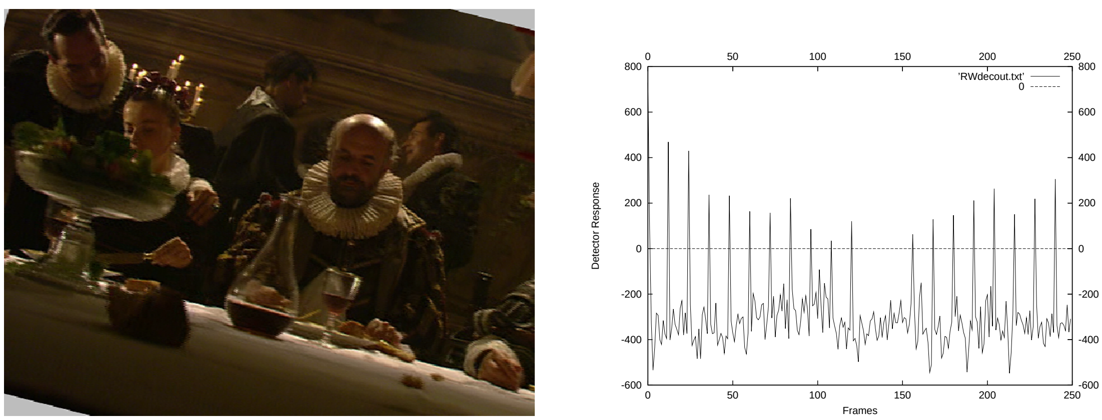
[10] T. Kalker, G. Depovere, J. Haitsma, and M. Maes, ”A Video watermarking System for Broadcasting Monitoring”, Wong, Delp editors, Security and Watermarking of Multimedia Contents, volume 3657 of SPIE Proceedings Series, pp. 103-112, January 1999.

[11] M. D. Swanson, B. Zhu, and A. H. Tewfik, ”Multiresolution Scene-Based Video Watermarking Using Perceptual Models”, IEEE Journal on Selected Areas in Communications, vol. 16, num. 4, May 1998.

[12] G. C. Langelaar, R. L. Lagendijk, and J. Biemond, ”Real-time Labeling Methods for MPEG Compressed Video”, 18th Symposium on Information Theory in the Benelux, Veldhoven, The Netherlands, May 1997.

(a) (b)

Figure 1: Test video sequence: (a) frame 36 of the watermarked sequence MPEG2 coded at 6 Mbit/sec; (b) detector response.



(a) (b)

Figure 2: Test video sequence: (a) frame 36 of the watermarked sequence undergone a 15 degrees rotation, a scaling to size 1000×900 and finally a cropping to the original size; (b) detector response.

(a) (b)

Figure 3: Test video sequence: (a) frame 36 of the watermarked sequence after a MPEG2 coding at lower bit rate (3 Mbit/sec); (b) detector response.