Robust Video Watermarking for Wireless Multimedia Communications

Nicola Checcacci Mauro Barni Franco Bartolini Stefano Basagni*

E-mail: nicola.checcacci@netit.alcatel.it,barni@dii.unisi.it
barto@lci.det.unifi.it,basagni@utdallas.edu

Abstract- ***Digital watermarking*** **involves embedding copyright marks (*watermarks*), often imperceptibly, in multimedia objects to enhance or protect their value. In this paper we describe a novel watermarking algorithm suitable for *video coding techniques* such as MPEG-4 and H.263/.324 and we test it in a wireless environment. The proposed algorithm satisfies critical properties not all of which are available in previous solutions. These properties include: Resistance (robustness) of the embedded watermark to the error-prone nature of wireless channels as well as to video frame loss or misplacement, negligible probability of reading a non embedded watermark, non-degradation of the marked video sequence and the possibility to mark video objects (e.g., MPEG-4 objects) in a single frame separately. Experimental results are given that show how these and other properties are achieved when video sequences are corrupted with errors that are typical of a wireless channel.**

I. INTRODUCTION

In the past few years, no communication technologies have experienced the incredible growth and commercial success of *mobile wireless communications* and *multimedia communications*. Naturally, the great interest and recent technical advances in both areas has led to the possibility of having mobile and multimedia communications together (see, e.g., [1] and [2] for recent advances in low-bit-rate coding standards for real-time audio-video conversational services over radio networks, and the error resilience aspects of the video coding techniques standardized in the MPEG-4 standard, respectively) and a host of applications is currently underway [3].

One of the major problems connected with the successful, secure use of wireless multimedia is related to the *ownership assertion* and *copyright protection* of the multimedia data. The ease with which, particularly in a wireless environment, digital data can be copied and redistributed makes it possible for any digital work (music, video, as well as generic data such a medical history, shopping patterns, etc.) to be copied illicitly and, basically, without loss of fidelity. Of course, data encryption and scrambling technology offer security for content delivery, as well as the means for controlling data access and related billing. However, there is little, if any, protection for decrypted or descrambled content, whose perfect copy can be easily redistributed.

A solution to the problem of providing value-added data protection, possibly on top of data encryption and scrambling, is introduced through the technique of *digital watermarking*. Informally, digital watermarking is the embedding of bits that represent marks or labels in digital data. The embedded marks are generally "invisible" (or, as more commonly and precisely said, *imperceptible*) but they can be detected or extracted through computing operations, whence the name *digital watermarks*.[1] Digital watermarks are bound to and hidden in the source data, inseparable from the data itself to the extent that they can survive operations that do not degrade the data beyond its utility and intended applications. Therefore, it is clear that watermarks can be used to communicate copyright, ownership, and usage-control information. As expected, digital watermarking has already received great interest and special issues of several communication magazines have been devoted to this subject. A general description of this technology that range from its technical merits to the commercial possibilities can be found in [4]. Historical and technical contributions, as well as a basic taxonomy of watermarking techniques, can be found in [5].

Several algorithms have been proposed for digital watermarking of text and audio data and of fixed images (the reader is referred again to the papers in [4] and [5] where further references can also be found). Recently, the increasing interest on multimedia communications has introduced the need to apply watermarking techniques also to video sequences, so that in the last few years solutions have been proposed for digital video watermarking.

Since video transmission is bound to the compression of the video sequence, techniques for video watermarking may take compression into account. It is actually common to partition the algorithms for video watermarking into two

* Stefano Basagni was supported in part by the Army Research Office (DARPA) under contract No. DAAG55-97-1-0312.

[1] In the case of images and video data, watermarks can also be explicitly visible. In this case they are used to carry a visual message or a company logo. In this paper we are not concerned with this kind of watermarks.

0-7803-6596-8/00/$10.00 © 2000 IEEE

main categories, according to whether the watermarking is performed *before* the video compression (*raw-video watermarking*), or *after* (*bit-stream watermarking*). Among the algorithms in the first category, we mention the work by Su, Hartung and Girod [6] (see also [7] and [8]), the algorithm by Hsu and Wu [9], Swanson et al. [10], Kalker et al. [11] and Deguillame et al. [12]. In the domain of bit-stream watermarking, the main algorithms were presented in [13] and [14] where the watermark is inserted after the video sequence has been encoded according to the MPEG-2 standard.

In this paper we are interested in introducing and testing an efficient algorithm for robust digital watermarking of video sequences transmitted over a wireless channel. The proposed algorithm inserts a watermark in a coded video sequence (bit-stream watermarking) by modifying opportunely selected quantized DCT (Discrete Cosine Transform) coefficients, similarly to methods used for watermarking of (fixed) images as introduced, e.g., in [9] and [15]. The proposed watermarking technique allows us to obtain the following characteristics, not all of which are available in previous solutions:

1. Our watermarking is not only resistant (*robust*) to processing that does not seriously degrade the quality of the video (such as the high-rate data compression imposed by the latest coding standards—e.g., MPEG-4 [16]) but also to errors that can degrade the decoded sequence (e.g., the high bit error rates typical of a wireless channel).

2. Retrieving the watermark does not require knowledge of the original video sequence.

3. The embedded watermark is imperceptible, i.e., the quality of the original video is not sensibly degraded.

4. The *false positive rate* is extremely low, i.e., the probability of reading a watermark that is not actually embedded in the video sequence is negligible.

5. The watermarking method is robust with respect to video frame loss or misplacement.

6. Single video *objects* can be watermarked separately, thus guaranteeing the protection of each single video object. This is made possible due to the orthogonality of our algorithm to the new content based functionalities of standards such as MPEG-4.

The proposed algorithm is completely general and works with any video coding standards based on Differential Pulse Code Modulation (DPCM)/DCT. It may thus be applied to video sequences coded with MPEG-1, MPEG-2 and MPEG-4 as well as H.263 and H.234 [1]. (For the sake of description, the overview of the algorithm given in the following refers explicitly to its application to video sequences coded according to the MPEG-4 standard.)

Being interested in multimedia communications over wireless channels, we test the robustness of the watermark with respect to the most common error conditions which are typical of wireless channels. Specifically, we have embedded a 15 bit watermark in the standard video sequences "Stefan," "News" and "Singer" which are typical examples of three different video typologies (fast motion, quasi-static video, natural/synthetic combination). We show that, by using common wireless transmission rates and simulating typical wireless perturbations (packet loss and burst errors), it is possible to retrieve the watermark even when the video sequence is highly degraded.

The rest of the paper is organized as follows. In Section II we give an outline of the proposed algorithm as applied to MPEG-4 video sequences. In the following Section III we demonstrate the robustness of the proposed watermarking method with respect to video transmission over a wireless channel. Section IV concludes the paper.

II. The Digital Watermarking Algorithm

In this section we outline the two main phases of our watermarking algorithm, namely the *embedding* of the watermark in the coded sequence and the watermark *recovery*. (Lack of space prevents us to describe the algorithms in full detail. The interested reader is referred to [17].) For ease of description, the two phases are described as performed on an MPEG-4 video sequence.

Watermark Embedding

Our algorithm hides a bit of the watermark in each luminance block of some macroblocks (MBs) which have been selected on a pseudo-random basis among all the MBs of an MPEG-4 Video Object Plane (VOP). Once the last bit of the watermark has been inserted, its first bit is considered again until all the selected MBs of the current VOP have been marked. The whole process is initialized again for every VOP of the MPEG-4 sequence (Video Object Layer, VOL). Figure 1 illustrates the steps for the embedding of a watermark in an MPEG-4 VOP.

More precisely, for each VOP the algorithm executes the following steps:

1. Generate a pseudo-random binary sequence based on a secret key and on the characteristics of the VOP. This binary sequence is used to choose the MBs where the watermarking code will be inserted and, at the same time, to choose some quantized DCT coefficient pairs. These pairs are selected among the mid frequency quantized DCT coefficients of each block and will be used to actually embed a bit of the watermark in the corresponding block.

2. For each luminance block in a selected MB:

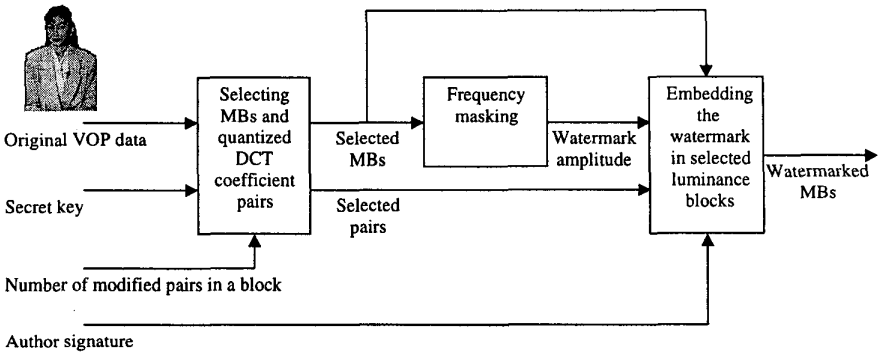


Figure 1: Watermark embedding phase.

(a) Compute the frequency masking to adapt the watermark amplitude to the local frame content.

(b) Modify each selected quantized DCT coefficient pairs, say $\langle Q_1, Q_2 \rangle$, so that either a 0 or a 1 from the watermark is inserted into the block by imposing that $Q_1 < Q_2$ or $Q_1 > Q_2$, respectively.

Watermark Recovery

Watermark retrieval is performed on the whole MPEG-4 VOL according to the two steps depicted in Figure 2.
The first step is similar to the one used in the embedding process and requires the knowledge of the parameters used in the embedding phase (namely, the secret key used to generate the binary sequence and the number of pairs that were modified in each selected MB). This information is used to determine the MBs and the DCT pairs where the watermark was hidden within each VOP.

The second step involves the relationships between the coefficients of the selected DCT pairs as modified during the embedding phase. Every MB where the jth bit of the watermark was possibly inserted is now considered and the value of the difference between the DCT coefficients of every pair where that bit was coded is stored in an accumulator A_j. The jth bit is then recovered by comparing the value of A_j with a threshold $T > 0$. (The value of T depends on the received sequence, and it is computed so as to guarantee a low "false positive detection" probability [17].) In particular, $j = 0$ if $A_j < -T$, $j = 1$ if $A_j > T$ and j is indeterminate otherwise (which means that either no bit was inserted or the reading is not reliable). Notice that when bit j is detected, it is always $\frac{|A_j|}{T} > 1$, and the more $|A_j|$ is $> T$ the more "retrievable" is bit j.

III. Experimental Results

Our watermarking algorithm has been tested over different bit rates and "wireless" error conditions. We considered three test sequences: "Stefan," "News" and "Singer" which represent three different video scenarios. The first sequence is characterized by the presence of fast motion. The sequence "News" is instead a quasi-static video, with some motion in the background. In the sequence "Singer" a natural image is superimposed on a synthetic background. The three sequences, in CIF format (frame size: 352x288 pixels, progressive scan, 4:2:0 subsampling format), are coded in MPEG-4 at 116.4 Kbps and 360 Kbps. (These data rates are often used by the MPEG test group [18].) Being interested in measuring the robustness of our algorithm over a wireless channel, our coding made *no* use of the recently introduced MPEG-4 error resilient tools [2].[2]

The coded sequences are watermarked with a 15 bit watermark and then corrupted using different random bit errors. More specifically, we consider *burst errors* with Bit Error Rates (BERs) of 10^{-3}, 10^{-4} and 5×10^{-4} and duration of 5ms, and *packet loss errors* of varying lengths (96-400 bits) and PER (Packet Error Rate) of 5×10^{-4}. (These error rates and types describe the variability and error-prone nature which are typical of a wireless channel.) Several seeds have been used for the pseudo-random generation of the different errors for each of the three sequences. The errors have been generated by using the error generation software used to test the MPEG-4 error resilient tools [19].

We test the *robustness* of the watermark by measuring how its recovery is affected by the "wireless" corruption with respect to the recovery from the original (i.e., not corrupted) sequence. We start by defining the *confidence* c_j of each recovered watermark bit j ($1 \leq j \leq 15$). The confidence of a bit j is defined as the ratio between the value of the (modulus of the) accumulator A_j and the threshold T (see Section II above):

[2] To the best of the authors' knowledge, the error resilient tools are not publicly available outside the MPEG community anyway.

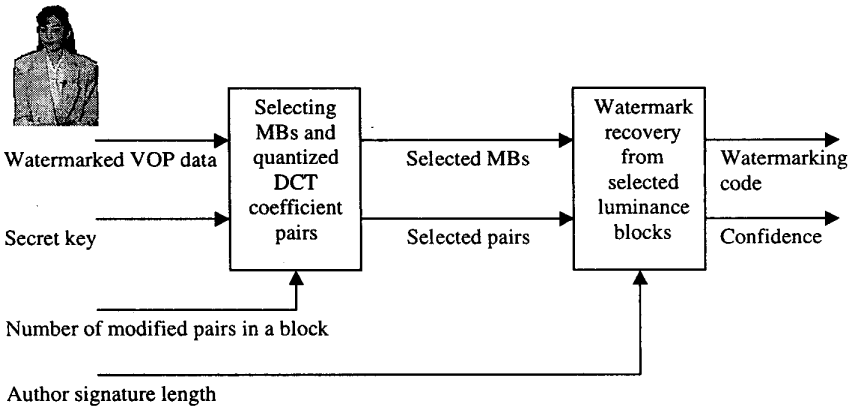


Figure 2: Watermark recovery phase.

$$c_j = \frac{|A_j|}{T}.$$

The more c_j is > 1 the more the jth bit is robust ("retrievable"): A high confidence indicates that the watermark bit j is present and that its estimated value is highly reliable. A low confidence suggests that either the reading is not reliable or that bit j is not present. In general, when for each j is $c_j > 2$, the watermark is considered highly robust (i.e., it is clearly retrieved from the marked sequence).

The notation above refer to the confidence of each bit retrieved from a corrupted sequence. With c_j^* we indicate the confidence of the jth bit of the watermark retrieved from the original sequence. The *differential confidence* Δc_j of bit j can now be defined as the measure (%) of how the reading of the jth bit has been degraded by the wireless corruption with respect to c_j^*. More precisely:

$$\Delta c_j = 100 \left(\frac{c_j^* - c_j}{c_j^*} \right).$$

Finally, the robustness of the entire watermark is expressed by the *global differential confidence*:

$$\Delta C = \frac{1}{15} \sum_{j=1}^{15} \Delta c_j.$$

Table 1 below shows the global differential confidence of the watermark under burst errors with BERs of 10^{-4} and 5×10^{-4} and packet loss with PER of 5×10^{-4} when the coding rate is 116.4 Kbps (for such a coding rate it was not possible to test the watermark for BER of 10^{-3}, since the MPEG-4 decoder could not process the corrupted sequence). We observe that, with respect to the case of a non corrupted sequence, independently on the video typology (fast motion, quasi-static video, natural/synthetic combination), the percentage of degradation imposed by the wireless transmission is always less than 6.8%.

Table 2 shows the global differential confidence of the watermark under the BERs 5×10^{-4} and 10^{-3} and packet loss with PER of 5×10^{-4} when the coding rate is 360 Kbps. In this case the percentage of degradation imposed by the wireless transmission is always less than 7%.

For both coding rates, we notice that the highest degradation occurs for the sequence characterized by the presence of fast motion ("Stefan"). (This is due to the propagation of the introduced errors which is proportional to the "amount" of motion in the sequence. This propagation is related to the specific way in which MPEG-4 encodes a video sequence.) Even in this case, however, the global differential confidence is still low.

Overall, we observe that there is no relevant difference between the recovery of a watermark embedded in the original video sequence and the recovery of the corrupted one. Independently on the BER, every bit of the watermark is extremely robust (for each of the 15 bits of the watermark the confidence is always at least 2.5). Even in critical test conditions (when the BER is 10^{-3}, see Table 2), in which the coded video sequence may contain several highly corrupted frames (such as the one depicted in Figure 3(B)), each bit of the watermark has a confidence > 2.5, i.e., is clearly retrievable.

IV. Conclusions

We introduced a new algorithm for video watermarking, an emerging technology used for ownership assertion and

Sequence:	Stefan	News	Singer
$\Delta C(\%)$ (Burst Error: $BER = 10^{-4}$)	1.06	0.66	0.45
$\Delta C(\%)$ (Burst Error: $BER = 5 \times 10^{-4}$)	5.93	1.64	2.29
$\Delta C(\%)$ (Packet Loss: $PER = 5 \times 10^{-4}$)	6.8	6.42	3.9

Table 1: Global differential confidence for video coding rate of 116.4 Kbps.

Sequence:	Stefan	News	Singer
$\Delta C(\%)$ (Burst Error: $BER = 5 \times 10^{-4}$)	3.21	1.5	2.01
$\Delta C(\%)$ (Burst Error: $BER = 10^{-3}$)	6.96	2.13	2.91
$\Delta C(\%)$ (Packet Loss: $PER = 5 \times 10^{-4}$)	2.02	3.29	1.25

Table 2: Global differential confidence for video coding rate of 360 Kbps.

copyright protection in multimedia communications. In particular, in this paper the proposed algorithm has been tested in video sequences which have been corrupted with errors which describe the variable and error-prone nature of wireless channels. Experimental results show that, despite critical test conditions (BER of up to 10^{-3}) the watermark is extremely robust, i.e., it can be clearly retrieved even when the video sequence in which it is embedded has several highly corrupted frames.

REFERENCES

(1) N. Färber, B. Girod, and J. Villasenor. Extension if ITU-T recommendation H.234 for error-resilient video transmissions. *IEEE Communications Magazine*, 36(6):120–128, June 1998.

(2) R. Talluri. Error-resilient video coding in the ISO MPEG-4 standar. *IEEE Communications Magazine*, 36(6):112–119, June 1998.

(3) IEEE Communications Magazine. Special Issue on Wireless Video. *IEEE Communications Magazine*, 36(6), June 1998.

(4) Communications of the ACM. Special Issue on Digital Watermarking. *Communications of the ACM*, 41(7), July 1998.

(5) IEEE Journal of Selected Areas in Communications. Special Issue on Copyright and Privacy Protection. *IEEE JSAC*, 16(4), May 1998.

(6) J. K. Su, F. Hartung, and B. Girod. Digital watermarking of text, image and video documents. *Computers & Graphics*, 22(6):687–695, December 1998.

(7) F. Hartung and B. Girod. Watermarking of uncompressed and compressed video. *Signal Processing*, 66(3):283–301, May 1998.

(8) F. Hartung and B. Girod. Watermarking of raw and compressed video. In *Proceedings of SPIE, Digital Compression Technologies and Systems for Video Communications*, volume 2952, pages 205–213, Berlin, Germany, 7–9 October 1996.

(9) C. Hsu and J. Wu. Digital watermarking for video. In *Proc. IEEE International Conference on Digital Signal Processing*, volume 1, pages 217–220, July 1997.

(10) M. D. Swanson, B. Zhu, and A. H. Tewfik. Multiresolution scene-based video watermarking using perceptual models. *IEEE Journal on Selected Areas in Communications*, 16(4):540–550, May 1998.

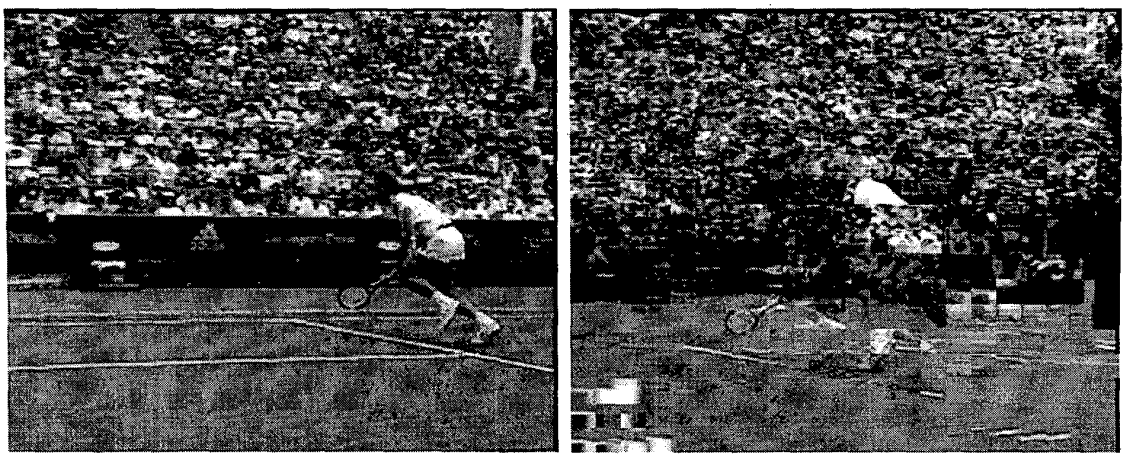
(11) T. Kalker, G. Depovere, J. Haitsma, and M. Maes. A video watermarking system for broadcast monitoring. In *Proc. IS&T/SPIE Conference on Security and Watermarking of Multimedia Contents*, pages 103–112, San Jose, California, January 1999.

(12) F. Deguillaume, G. Csurca, J. O'Ruanaidh, and T. Pun. Robust 3D DFT video watermarking. In *Proc. IS&T/SPIE Conference on Security and Watermarking of Multimedia Contents*, pages 113–124, San Jose, California, January 1999.

(13) F. Hartung and B. Girod. Digital watermarking of MPEG-2 coded video in the bitstream domain. In *Proceedings of the 1997 IEEE International Conference on Acoustics, Speech, and Signal*, volume 4, pages 2621–2624, Munich, Germany, 21–24 April 1997.

(14) G. C. Langelaar, R. L. Lagendijk, and Biemond J. Real-time labeling of MPEG-2 compressed video. *Journal of Visual Communication & Image Representation*, 9(4):256–270, December 1998.

(15) E. Koch and J. Zhao. Towards robust and hidden image copyright labeling. In *Proceedings of the IEEE*



(A) (B)

Figure 3: A frame from the video sequence "Stefan:" (A) original and (B) corrupted (the BER is 10^{-3}).

Workshop on Nonlinear Signal and Image Processing '95, Neos Marmaras, Greece, June 20–22 1995.

(16) T. Sikora. The MPEG-4 video standard verification model. *IEEE Transactions on Circuits & Systems for Video Technology*, 7(1):19–31, February 1997.

(17) N. Checcacci, M. Barni, F. Bartolini, and S. Basagni. MPEG-4 video objects watermarking. Technical Report UTD/EE-04-99, Department of Electrical Engineering, The University of Texas at Dallas, July 1999.

(18) ISO/IEC JTC1/SC29/WG11/N2604. Report of the formal verification tests on MPEG-4 video error resilience. December 1998.

(19) T. Miki, T. Kawahara, and T. Ohya. Revised error pattern generation program for core experiment on error resilience. *ISO/IEC JTC1/SC29/WG11 MPEG96/1492*, Maceio, Brazil, November 1996.