A Robust Content-Dependent Algorithm for Video Watermarking

Lino Coria
Panos Nasiopoulos
Rabab Ward

The University of British Columbia
2356 Main Mall
Vancouver, BC, Canada, V6T 1Z4

(604) 822 4988
(604) 822 2646
(604) 822 6894

linoc@ece.ubc.ca
panos@ece.ubc.ca
rababw@ece.ubc.ca

ABSTRACT

A watermarking method that relies on informed coding and informed embedding is presented. Our method uses a subset of various codewords to represent the 0 and 1 message bits to be embedded. We propose a codeword generation scheme that keeps control of the distance between codewords in order to secure fidelity and robustness of the watermark. When compared to existing video watermarking schemes, our method yields superior robustness to video compression.

Categories and Subject Descriptors

E.4 **[Coding and Information Theory]** - *data compaction and compression*. I.4 **[Image Processing and Computer Vision]**: Miscellaneous.

General Terms

Algorithms, experimentation.

Keywords

Compression, DCT, digital video, informed coding, informed embedding, watermarking.

1. INTRODUCTION AND OVERVIEW

Watermarking has become the technology of choice for enforcing copyright protection of digital content [1]. This technique imperceptibly alters the media content by embedding a message. This message is used to either identify the owner of the content or the device that created the illegal copy. When it comes to digital video, watermarks must not only be carefully designed so that they are invisible when the content is being displayed but they must also be robust to regular distortions, and in particular to those arising from video compression (e.g., MPEG-2).

Watermarking algorithms usually embed binary messages in the frequency domain. One of the most successful approaches is Spread Spectrum [2], which is a watermarking process that represents a message (to be embedded) by a set of pseudorandom codewords. Some advantages of this method are: 1) the signal energy inserted in the frequency components is very small relative to the energy of these components, and 2) it provides robustness to common distortions since the watermark is dispersed over several frequency bands. An updated version of this approach uses informed embedding and coding in its schemes [3]. Informed embedding examines the original content before encoding the watermark, in order to find the appropriate trade off between robustness to common distortions and the perceptual impact that the watermark will have on the image (fidelity). Informed coding uses content during the coding process to help select among several alternative codewords the one that, after embedding, results in the least distortion of the original content.

A modified method based on the ideas of informed coding and informed embedding from [3] is presented in [4]. Since the modified scheme requires fewer computations, it is more suitable for video applications. Furthermore, the Bit Error Rate (the percentage of lost message bits) is better than the one in [3] since the message bits are not tied via a trellis. However, the Message Error Rate (the percentage of frames that show at least one message bit wrong when decoded) may or may not improve, depending on the type of attack.

A scheme proposed in [5] introduced the use of Independent Components Analysis (ICA) to the watermarking field. This idea was further developed in [6] where a video watermarking scheme, the ICA-Trellis, was presented. This scheme, which belongs to the Spread Spectrum category, uses ICA to de-correlate the different regions of a video frame. This de-correlation yields independent signals, which help reduce the level of distortion caused by a watermark. In this approach, ICA is applied to the prediction error frames before the message is embedded in a set of statistically independent signals. A modified trellis code is used to generate a variety of codeword arrays which are then used to embed the best possible watermark on a frame. The entire frame is considered when determining the watermark that causes the least distortion.

In this paper, we introduce a new algorithm that yields better performance to video compression than the ICA-Trellis method [6]. Our algorithm employs a codeword generation scheme that keeps control of the distance between codewords in order to secure fidelity and robustness of the watermark.

DRM'06, October 30, 2006, Alexandria, Virginia, USA.

This paper is organized as follows: Our watermarking method is described in detail in section 2. Performance evaluations are discussed in section 3. Section 4 presents the conclusions.

2. OUR WATERMARKING ALGORITHM

Our method incorporates informed coding and embedding techniques. Instead of taking decisions based on the image as a whole (as in [3]), the codewords that represent the 0 or 1 message bits to be embedded are selected by using independent features from 8 × 8 pixel blocks. The embedded message is binary and the codeword that will represent each of these bits is hidden in one of the 8 × 8 blocks. Thus, the length of the message must not exceed the number of blocks in the image. The Discrete Cosine Transform (DCT) is applied to every image block and the L lowest AC coefficients are modified to include representation of the codewords (see Figure 1). First, we copy the L coefficients of each image block into a one-dimensional array resulting in a vector of length L. We call this array of coefficients the extracted vector, $\mathbf{v_o}$.

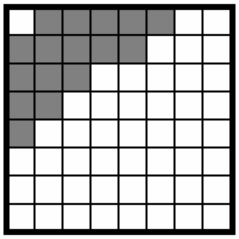


Figure 1. The DCT is applied to an 8 × 8 pixel block. Shaded coefficients indicate the AC terms used for constructing the extracted vector of length L = 16.

The objective now is to find a codeword that has the highest correlation with vector $\mathbf{v_o}$. This codeword will then be embedded in this block. If a good correlation cannot be found, $\mathbf{v_o}$ is modified in order to make that possible. We call this modified vector the watermarked vector $\mathbf{v_w}$. Note that in some cases this vector may be identical to the original vector $\mathbf{v_o}$. The codeword is chosen from a set of codewords whose generation is described below.

P Codewords are generated in a pseudorandom fashion and are of length L. Half of these codewords (P/2) represent bit 0 and the other half represent bit 1. These subsets are called A and B such that:

$$A = \{\mathbf{a}_1, \mathbf{a}_2, \cdots, \mathbf{a}_{P/2}\} \text{ represents bit 0.} \tag{1}$$

$$B = \{\mathbf{b}_1, \mathbf{b}_2, \cdots, \mathbf{b}_{P/2}\} \text{ represents bit 1.} \tag{2}$$

The way these subsets are constructed has a big impact on the robustness of the watermark to common attacks as well as on the fidelity of the watermarked image. Therefore, we design these codewords using the following approach. First, we use a watermark key K, which is a number that is only known to the user, as the seed to generate codeword $\mathbf{a}_1$. This codeword is normalized so that its length is equal to one. Then the value for a parameter d_0 which will be the distance between two consecutive codewords is established. The second codeword $\mathbf{a}_2$ is generated by adding a vector of magnitude d_0 to the first codeword. $\mathbf{a}_2$ is then normalized so that its length is equal to 1. The direction of this vector is obtained pseudorandomly by using a multiple of the original key K as its seed. The remaining codewords are created in a similar way, always obeying the following restriction:

$$|\mathbf{a}_{i-1} - \mathbf{a}_i| = d_0 \quad \text{for } i = 2, 3, ..., P/2. \tag{3}$$

Where $\mathbf{a}_{i-1}$ and $\mathbf{a}_i$ are normalized so that the length is equal to 1. Subset B is constructed so that

$$\mathbf{b}_i = -\mathbf{a}_i \quad \text{for } i = 1, 2, ..., P/2. \tag{4}$$

It has been found by computer experiments that employing this method to construct the codewords provides better watermarking results in terms of both fidelity and robustness than when codewords are generated in a total random fashion. Choosing the appropriate values for d_0, L and P will result in two subsets of codewords that offer a tradeoff between watermark robustness and image fidelity as exemplified in Figure 2 where, for illustration purposes, L has been set to 3. Irrespective of the value of d_0, the larger the value of P the less distortion the image endures; this is because the wide variety of codewords will result in higher likelihood of finding a close match with vector $\mathbf{v_o}$. For example, if the bit to be inserted is represented by an $\mathbf{a}_i$ vector then there is a wide variety of $\mathbf{a}_i$'s to choose from. This means better overall picture fidelity. However, the large number of codewords in the other subset (i.e., subset B in this case) will unfortunately reduce the robustness of the watermark as the codewords from both subsets are very close to each other. Thus, P must not be large. A very small value of d_0 will result in a more robust watermark but the visual quality of the 8 × 8 block will likely deteriorate. This case is shown in Figure 2b where a reasonable value of P (= 60) and a small d_0 (= 0.1) generate two subsets that are far away from each other. Finally, Figure 2c illustrates the case when reasonable values for P (=60) and d_0 (=1) are chosen. We observe that, in this case, there is a suitable distance among the codewords of the subsets and yet each subset has an adequate number of codewords.

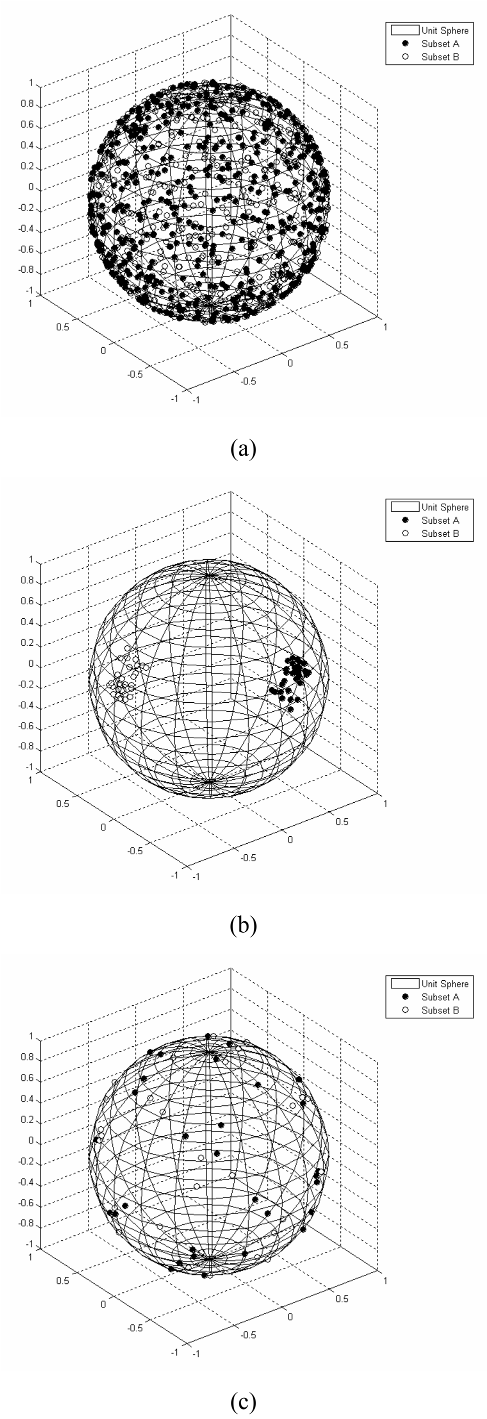
Regarding L (the length of vector $\mathbf{v_o}$), as this is the number of coefficients that might be modified by the watermark in every block, it is recommended to keep it lower than 20 since the watermark must only be embedded in the lower AC frequency coefficients [3].

Once the codewords are constructed, we proceed to embed the message in the image. For every 8 × 8 block, the correlation between the extracted vector $\mathbf{v_o}$ and each of the P/2 codewords representing the desired bit (0 or 1) to be embedded in that particular block is computed. It should be noted that although all the codewords are normalized, $\mathbf{v_o}$ is not. This is because changing its magnitude will not affect the performance of the proposed method. Assume that we wish to embed bit 0, which is represented by subset A. Let the codeword with the highest correlation with $\mathbf{v_o}$ be $\mathbf{a}_{\max}$:

$$\mathbf{a}_{\max} = \max_{\mathbf{a}_i}(\mathbf{a}_i \bullet \mathbf{v_o}) \quad \text{for } i = 1, 2, \dots P/2. \tag{5}$$

Let us also assume that the correlation between $\mathbf{v_o}$ and $\mathbf{a}_{\max}$ minus the correlation between $\mathbf{v_o}$ and every $\mathbf{b}_i$, $\forall\, i$ = 1, ..., P/2 is represented by R_{0i}. Thus

$$R_{0i} = (\mathbf{a_{max}} - \mathbf{b}_i) \bullet \mathbf{v_o} \quad \forall\, i = 1, 2, ..., P/2\,. \tag{6}$$



(a)

(b)

(c)

Figure 2. Two subsets of codewords of length *L* = 3 are generated with different values of *P* and d_0; (a) *P* is large (*P* = 1,000). This results in watermarked images with high fidelity but low robustness; (b) A reasonable value for *P* but a very small value for d_0 (*P* = 60; d_0 = 0.1). Consequently, codewords from subset *A* are highly uncorrelated with codewords from subset *B*. This results in robust watermarks but with low image fidelity; (c) A reasonable value for *P* and a middle value for d_0 (*P* = 60; d_0 = 1). This results in watermarked images with a good tradeoff between robustness and fidelity.

If

$$R_{0i} > 0 \quad \forall\, i = 1, 2, ..., P/2 \tag{7}$$

and if there is no image distortion, then condition (7) is enough for a decoder to be able to retrieve the correct watermark. However, in case of an attack or other image distortion, condition (7) is not enough to guarantee a robust watermark. Therefore, it must be ensured that R_{0i} has a larger positive value. We achieve that by introducing a robustness threshold R_t resulting in the condition

$$R_{0i} > R_t \quad \forall i = 1,2,..., P/2. \tag{8}$$

This implies that there is a large enough distance between the vector $\mathbf{v_o}$ and the unwanted codewords of subset *B*.

If condition (8) is not fulfilled, then $\mathbf{v_o}$ is modified in an iterative fashion until (8) is satisfied. Let the modified vector be denoted by $\mathbf{v_w}$, at any iteration. Referring to equation (6), the larger the value of R_{0i} $\forall$ *i*, the higher the likelihood that the codeword $\mathbf{a}_{\max}$ is the one embedded in the block. Also for every $\mathbf{b}_i$, if R_{0i} is greater than the robustness threshold R_t, then there is a large enough distance between the watermarked vector $\mathbf{v_w}$ and the unwanted codewords (subset *B*). On the other hand, if R_{0i} is smaller than R_t, then $\mathbf{v_w}$ must be modified so that each resulting R_{0i} is greater than R_t. The modification is performed by first finding the minimum R_{0i} over all the codewords from the unwanted subset *B*. That is

$$R_{0\min} = \min_{i=1}^{P/2} R_{0i}. \tag{9}$$

To minimize the change in the image fidelity, $R_{0\min}$ and the vector $\mathbf{b}_{\min}$ associated with it are then used to modify the watermarked vector $\mathbf{v_w}$, so that the next time R_{0i} is computed for that particular $\mathbf{b}_{\min}$ it yields a value exactly equal to R_t, while having a minimum Euclidian distance from the previous value of $\mathbf{v_w}$. This modification is achieved as follows:

$$\mathbf{v_w} \leftarrow \mathbf{v_w} + \left(R_t - R_{0\min}\right)\frac{\left(\mathbf{a_{max}} - \mathbf{b}_{\min}\right)}{\left|\mathbf{a_{max}} - \mathbf{b}_{\min}\right|}. \tag{10}$$

This procedure is iterated by recalculating $R_{0\min}$ and re-modifying the vector $\mathbf{v_w}$ until $R_{0\min}$ is larger than R_t. The resulting $\mathbf{v_w}$ becomes the watermarked vector, i.e., the modified coefficients of the 8 × 8 block. Finally, the inverse DCT is applied to this block to obtain the spatial values. This whole process is repeated for all the blocks of the image.

When decoding the message, the image is also partitioned into 8 × 8 blocks and the DCT is applied. Low frequency coefficients are used to obtain the watermarked vector $\mathbf{v_{wn}}$, which might be a noisy version of the encoded $\mathbf{v_w}$. Next, the correlation between $\mathbf{v_{wn}}$ and all *P* codewords is computed. The codeword with the largest correlation value is the one the decoder chooses as the codeword $\mathbf{a_{max}}$ and the bit from the subset $\mathbf{a_{max}}$ belongs to is chosen as the original message bit.

3. PERFORMANCE EVALUATION

We applied our watermarking algorithm to various video sequences. The robustness of this scheme was tested for MPEG-2 compression attacks. In this section, we compare the performance of our method with that of the ICA-Trellis watermarking scheme [6].

Five video sequences (Container, Hall Monitor, Mother and Daughter, News, Suzie), each consisting of 150 frames, were used for our tests. We worked with Groups of Pictures (GOP's) of size 15 and we watermarked only the luminance (Y) component of every frame. The sequences are in QCIF format (176 × 144), which means that a maximum of 396 message bits can be embedded in every frame by our algorithm. However, we decided to embed only 44 message bits per frame in order to have a similar payload to the one offered by the ICA-Trellis scheme. These 44 message bits were embedded nine times in the same frame. By having redundant information, we were able to use a very low robustness threshold R_t and, therefore, very low frame distortion was achieved. The payload of the ICA-Trellis scheme is only 31 bits per frame. The picture quality was kept the same (PSNR = 42 dB) for both methods. As an example, Figure 3 shows one frame of the video sequence Suzie before and after watermarking.

By setting P to 128 we created a subset of 64 codewords to represent bit 0, and another subset of 64 codewords to represent bit 1. This number of codewords is large enough to guarantee a watermarked video with satisfactory fidelity and small enough to ensure high robustness. This number also results in a reasonable number of computations at both the encoder and the decoder. The codewords were normalized and have a length L of 16. The distance d_0 was set to 0.4.

Figure 4 shows the performance of our watermarking scheme and the ICA-Trellis method at different compression rates for all five video streams. We observe that at compression ratio 20:1 (which corresponds to a bit rate of 758 kbps) our method yields an average BER of 0.2%. The BER for ICA-Trellis, on the other hand, varies from 2% to 4% (an average of 3%, which means 15 times more errors on average). When a compression ratio of 30:1 (505 kbps) is used, less than a 2% average of the embedded message is lost when our method is employed. ICA-Trellis yields BER's that range from 6% to 17% (an average of 12.2%, resulting in 6 times more errors). Finally, at compression ratio 40:1, which corresponds to 379 kbps, our method yields BER values that range from 2% to 9.8% (an average of 6.7%). ICA-Trellis yields BER values that range from 19% to 37% (an average of 27.8%, which is 4 times more errors).

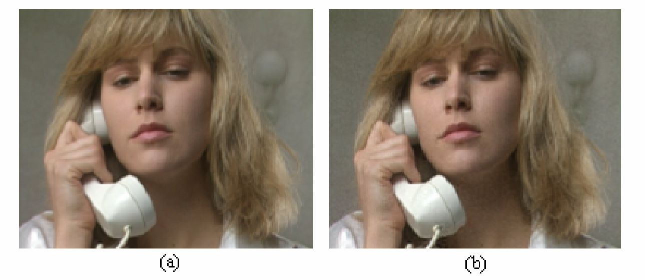


Figure 3. A frame from the QCIF video sequence Suzie: (a) unwatermarked; (b) watermarked with PSNR = 42.509 dB.

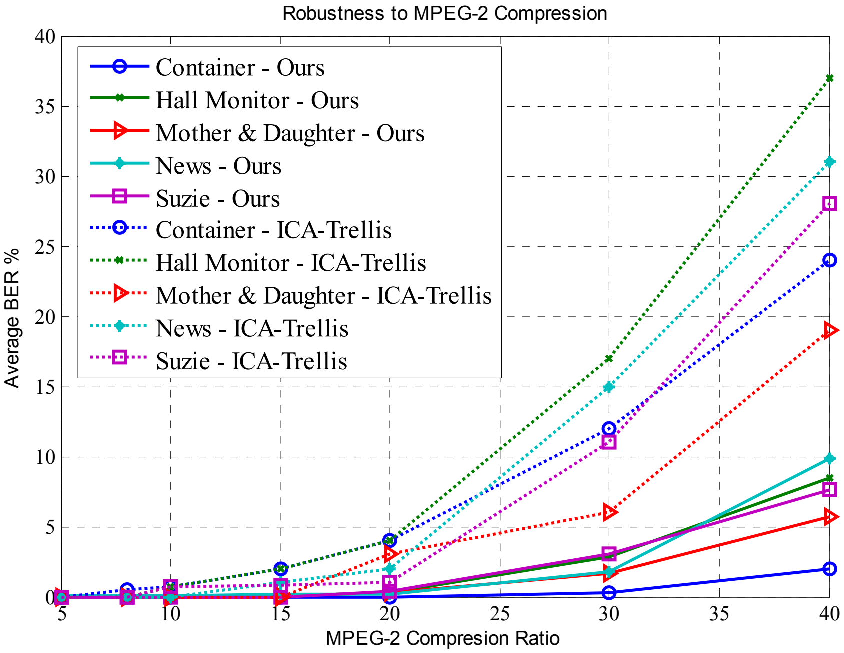


Figure 4. Robustness to MPEG-2 Compression of our method (solid lines) and ICA- Trellis scheme (dotted lines).

4. CONCLUSION

A content-dependent video watermarking scheme is presented. A binary message of adequate length (44 bits per frame) is embedded. The fidelity of the watermarked sequence is kept at the high level of 42 dB PSNR. Our method's robustness to MPEG-2 compression is proven to be superior to the performance of the ICA-Trellis scheme, the best recent video watermarking algorithm. Our method yielded on average a fifteen-time improvement over the ICA-Trellis method at compression ratio 20:1, a six-time improvement at compression ratio 30:1 and four-time improvement at compression ratio 40:1.

5. ACKNOWLEDGMENTS

Our thanks to the Mexican Council for Science and Technology (CONACYT) and ITESO University for partially sponsoring this work.

6. REFERENCES

[1] Doerr, G.; Dugelay, J.-L, "A guide tour of video watermarking," *Signal Processing: Image Commun*., vol. 18, no. 4, pp. 263-282, Apr. 2003.

[2] Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom. *Digital Watermarking*, New York: Morgan Kaufmann Publishers, 2002.

[3] M. L. Miller, G. J. Doërr, and I. J. Cox. "Applying Informed Coding and Embedding to Design a Robust High-Capacity Watermark," *IEEE Trans. on Image Processing*, Vol. 13, No. 6, pp. 792 - 807, June 2004.

[4] Lino Coria-Mendoza, Panos Nasiopoulos, Rabab Ward, "A Robust Watermarking Scheme Based on Informed Coding and Informed Embedding," *IEEE International Conference on Image Processing ICIP 2005*, Genoa, Italy, pp. 681-684, September 2005.

[5] S. Bounkong, B. Toch, D. Saad, D. Lowe, "ICA for Watermarking Digital Images," *Journal of Machine Learning Research*, vol. 4, pp. 1471-1498, 2003.

[6] Hussein Joumaa, Franck Davoine, "An ICA Based Algorithm for Video Watermarking," *IEEE International Conference on Acoustics, Speech, and Signal Processing ICASSP 2005*, Philadelphia, USA, pp. 805-808.