A wavelet Based Object Watermarking System for Image and Video

Abdessamad Essaouabi, Ibnelhaj Elhassane

Abstract—Efficient storage, transmission and use of video information are key requirements in many multimedia applications currently being addressed by MPEG-4. To fulfill these requirements, a new approach for representing video information which relies on an object-based representation, has been adopted. Therefore, object-based watermarking schemes are needed for copyright protection. This paper proposes a novel blind object watermarking scheme for images and video using the in place lifting shape adaptive-discrete wavelet transform (SA-DWT). In order to make the watermark robust and transparent, the watermark is embedded in the average of wavelet blocks using the visual model based on the human visual system. Waterlet coefficients, a least significant bits (LSBs) are adjusted in concert with the average. Simulation results show that the proposed watermarking scheme is perceptually invisible and robust against many attacks such as lossy image/video compression (e.g. JPEG, JPEG2000 and MPEG-4), scaling, adding noise, filtering, etc.

Keywords—Watermark, Visual model, Robustness, in place lifting Shape adaptive-discrete wavelet transform.

I. INTRODUCTION

DIGITAL watermarking is a new technology proposed to solve the problem of digital media security. An invisible signal is embedded directly in the digital media so that it is inseparable from the digital media. There is a wide range of applications of digital watermarking, including copyright protection, authentication, etc. This paper mainly addresses the copyright protection problem of digital images and video. For this kind of application, digital watermarking should have properties such as invisibility, robustness, high detection reliability, etc.

Robustness is a very important property of digital watermarking for copyright protection applications. To be effective, a digital watermarking scheme should be robust against common signal processing operations such as JPEG compression and low pass filtering as well as other intentional attacks.

In recent years, many image watermarking algorithms have been proposed. Most of them embed a watermark in the spectrum domain of an image. Cox [2] first proposed that for a watermark to be robust, it must be embedded in significant components of an image. The image is first globally DCT transformed, then, the 1000 largest DCT coefficients are selected to embed a watermark using additive spread spectrum methods. The original image is needed for watermark detection. Piva relaxed this limitation in [3]. The watermark is embedded into middle frequency coefficients of an image and the watermark detector correlates the known watermark with the same middle frequency coefficients of the suspect image directly without the knowledge of the original image. There are some other algorithms that embed a watermark in the Discrete Wavelet domain [4], the Discrete Fourier domain [5] or the fractal domain [6] of an image. The problem with the current watermarking algorithms is that most of them embed a watermark in the entire image without taking the content of the image into account. In some situations, the image owner may be more interested in an object of an image than the whole image, so it’s desirable to embed a watermark in the object to protect it better.

With the emergence of new multimedia standards such as Mpeg-4 and Jpeg2000, the notion of video-object or image object is more and more widespread. Consequently, protecting the different objects of an image or a video appeared necessary. Therefore several object-based watermarking techniques have been proposed. Wu et al. [7] proposed a multiresolution object watermarking approach based on 2D and 3D shape adaptive wavelet transforms. The advantage of the multiresolution watermarking method is its robustness against image/video compression and computational saving. However, the main disadvantage is that original image/video object is required for watermark detection. Kim et al. [8] proposed an object-based video watermarking method using the shape adaptive-discrete cosine transforms (SA-DCT). The SA-DCT method is superior to all other padding methods in terms of robustness against the image deformations. Yet, the watermark can be damaged by a wavelet-based image codec in the quantization stage. Therefore, this method limits their applications in the context of JPEG2000 and MPEG-4 due to the fact that the wavelet transform is playing an important role in JPEG2000 and MPEG-4. Piva et al. [9] propose an object watermarking system for MPEG-4 streams. Since this method applies the discrete wavelet transform (DWT) to the whole image and the watermark is embedded in all the wavelet coefficients belonging to the three detail bands at level 0, this may lead to loss of the watermark which is embedded in the region outside the object. Barni et Bartolini [10] proposed a method that consists in embedding a watermark in each video object of an MPEG-4 coded video bit-stream by imposing specific relationships between some predefined pairs of quantized DCT middle frequency coefficients in the luminance blocks of pseudo-randomly selected macroblocks. The quantized coefficients are recovered from the MPEG-4 bit-stream, they are modified to embed the watermark and then encoded again.

The main drawback of this technique is that, since the code is...
II. IN-PLACE LIFTING SA-DWT

Given an arbitrarily shaped object with shape mask information, with in place lifting SA-DWT[11], the number of the transformed coefficients is equal to the number of pixels in the arbitrarily shaped segment image, and the spatial correlation across subbands is well preserved. Fig. 1 illustrates the result of one-level wavelet decomposition of an arbitrarily shaped object. The in-place lifting DWT implementation has special implications for the SA-DWT[12], which can best be understood visually as shown in Fig. 1. As the SA-DWT is performed, the spatial domain shape mask remains intact with no requirement to derive a shape mask for each subband. How the subbands are arranged in this pseudo-spatial domain arrangement is shown in Fig. 2. Each subband can in fact be extracted from the interleaved subband arrangement using the lazy wavelet transform (LWT) [13]. After the one-level SA-DWT is performed, the LL subband can be extracted using a coordinate mapping from the interleaved subband coordinates \( (i, j) \) to the LL subband coordinates \( (i_{LL1}, j_{LL1}) \) as follows:

\[
(i_{LL1}, j_{LL1}) = (i/2, j/2)
\]  

(1)

Similarly, the mapping for the HL subband is \( (i_{HL1}, j_{HL1}) \) \( \leftarrow (i/2 + 1, j/2) \); for the LH subband \( (i_{LH1}, j_{LH1}) \) \( \leftarrow (i/2, j/2 + 1) \); and for the HH subband \( (i_{HH1}, j_{HH1}) \) \( \leftarrow (i/2 + 1, j/2 + 1) \). After the first level of the SA-DWT, the interleaved subband arrangement is made up of \( 2 \times 2 \) basic blocks of coefficients. As shown in the left side of Fig. 3, the top-left coefficient of each block is an LL subband coefficient, the top-right coefficient is an HL subband coefficient, and so on. The second level SA-DWT is performed by first extracting the LL subband using the coordinate mapping(1) and then performing the one-level SA-DWT using the LL subband as the new input. The output is the four interleaved subbands, LL, LH, HL, and HH. This is then placed back into the original interleaved subband arrangement where the LL coefficients were extracted from. This creates a two-level interleaved subband arrangement. As shown in the middle of Fig. 3, the two-level interleaved subband arrangement is made of a basic \( 4 \times 4 \) coefficient block, with the top-left coefficient of each block being an LL coefficient. The coordinate mappings to extract the second and subsequent level subbands are simply derived by applying the one level coordinate mappings iteratively to the LL subband coordinate mapping from the previous level.

![Fig. 1. One-level, two-dimensional SA-DWT using in-place lifting DWT implementation](image1)

![Fig. 2. Interleaved subband abstraction](image2)
A content-based watermarking system for content integrity protection is illustrated in Fig. 4.

III. PROPOSED WATERMARKING SCHEME

A content-based watermarking system for content integrity protection is illustrated in Fig. 4.

A. Watermark Embedding

Fig. 4(a) shows the watermarking embedding procedure. Firstly, the original image is segmented into foreground object and background and we apply the three levels in place lifting SA-DWT to foreground object. Then we take each third level basic block (see Fig. 3). \( N \times N \) is the size of the matrix wavelet block and \( I_i(k) \) is the ith wavelet coefficient in the kth wavelet block where \( i \in [1, N \times N] \). The rest of the watermarking procedure is presented in the following. The \( n \) LSBs of \( I_i(k) \) is defined as Subsection text here.

\[
\hat{I}_i(k) = \text{mod}(I_i(k), 2^n)
\]

In the proposed watermarking, we choose the blocks with an average value different from zero. If a few of \( I_i(k) \) are changed by \( \Omega \) due to some distortions, the average of the wavelet block will only have a small change[14]. Assuming that \( I_i(k) \) is the ith wavelet coefficient in the kth wavelet block after the watermark embedding, \( \hat{I}_i(k) \) is the \( n \) LSBs of \( I_i(k) \) and \( \text{Average}'(k) \) is the average of \( \hat{I}_i(k) \)in the kth wavelet block accordingly. The watermark \( W \), consisting of a binary pseudo random sequence, \( W(k) \in \{1, 1\} \), is embedded by adjusting the average of wavelet blocks in this way:

\[
\text{Average}'(k) = \begin{cases} 
[0, 2^{n-1}] & \text{if } W(k) = -1 \\
(2^{n-1}, 2^n] & \text{if } W(k) = 1
\end{cases}
\]

To adapt the watermark sequence to the local properties of the wavelet block, we use the model based on HVS in the watermark system. The visual model function \( V_m(k) \) is defined as: The average of the wavelet block is defined as:

\[
V_m(k) = \text{brightness}(k) \times \text{texture}(k)^eta
\]

where

\[
\text{texture}(k) = \frac{\sum_{i=1}^{N \times N} (\text{brightness}(k) - I_i(k))^2}{N \times N}
\]

\[
\text{brightness}(k) = \frac{\sum_{i=1}^{N \times N} I_i(k)}{N \times N}
\]

\( \beta \) a parameter used to control the degree of texture sensitivity. This visual model function indicates that the human eye is less sensitive to noise in the highly bright and the highly textured areas of the image. Hence, the wavelet blocks are divided into two parts depending on the value of \( V_m(k) \): high activity wavelet block and low activity wavelet block. For simplicity, the threshold \( T_c \) is set to the average of \( V_m(k) \). The following function can be applied to distinguish high or low activity wavelet block:

\[
T(k) = \text{sign}(\text{V_m(k)} - T_c)
\]

Considering the tradeoff between robustness and transparency, the proposed watermark embedding algorithm can be formulated as follows:

\[
I_i'(k) = I_i(k) + \alpha W(k) F_i(k) [2^{n-2-S(k)} + T(k) \times 2^{n-3}] \tag{7}
\]

where \( \alpha \) is a scaling factor used to control the strength of the inserted watermark. The flag function is defined as follows:

\[
F_i(k) = \text{sign}((2^{n-1} - I_i(k)) \times W(k)) \tag{8}
\]
where
\[ \text{sign}(x) = \begin{cases} +1 & \text{if } x \geq 0 \\ -1 & \text{else} \end{cases} \]

The strength function is defined as follows: Where
\[ X(k) = \left(2^{n-1} - \text{Average}(k)\right) \times W(k) \]

Details concerning the flag function and the strength function are described in Table I.

\[ S(k) = \text{sign}(X(k)) \quad (9) \]

In light of the above, the n LSBs of wavelet coefficients have been adjusted by using equation (6). Naturally, their average has been updated depending on the requirement of \( W(k) \) as shown in equation(3). In other word, the watermark has been embedded.

**B. Watermark Extraction and Detection**

The watermark sequence can be extracted without the original object. From the process of the watermark embedding, we can obtain the watermarked objects by applying the function of equation (3). Thus, for a given watermarked object, the watermark can be extracted as:

\[ W'(k) = \begin{cases} 1 & \text{if } \text{Average}(k) \in [0, 2^{n-1}) \\ -1 & \text{if } \text{Average}(k) \in [2^{n-1}, 2^n) \end{cases} \quad (10) \]

In order to detect the watermark \( W' \) extracted from the watermarked object, we firstly evaluate the detector response (or similarity of \( W' \) and \( W \)) as:

\[ \rho(W', W) = \frac{\sum_{k=1}^{L} W'(k) \times W(k)}{\sum_{k=1}^{L} ||W'(k)||^2} \quad (11) \]

where, \( L \) is the length of the watermark signal. The Threshold \( T_\rho \) is set so as to minimize the sum \( \rho \) of the probability of error detection and the probability of false alarm. if \( \rho \geq T_\rho \), we considered the watermark is present, otherwise absent.

**IV. EXPERIMENTS RESULTS**

Simulations are carried out for several standard monochrome images as shown in Figs. 5, 6, 7, 8 but only report result in detail for \( 704 \times 480 \) akiyo. In our experiments, the parameters considered are: the threshold \( T_\rho = 0.1 \), \( \beta = 0.318 \), \( n = 5 \), \( N = 8 \), \wavelet-\level = 3, \wavelettype = 'haar'. \( L \) = 1700 and scaling factor \( \alpha \in [0.1, 0.5] \). In order to test the performance of the proposed watermarking scheme, 200 watermarks were randomly generated. The PSNR result between the original object and the watermarked object is 39.26 dB. As shown in Fig. 9, the watermark is perceptual invisible and the object with watermark appears visually identical to the object without watermark. In Fig. 10 the absolute difference between the original object and the watermarked one, it is evident that there is no watermark embedded in the region outside the object. Fig. 11 shows the response of the watermark detector to 200 randomly generated watermarks of which only one matches the watermark present. The response to the correct watermark (i.e. number 100) is much higher than the responses to incorrect watermarks. To evaluate the robustness of our scheme against unintentional and intentional attacks, we test the watermarked object with JPEG, JPEG2000, scaling, adding noise, filtering and multiple watermarking attack. Added experiment results for other images are listed in Table II.
A. JPEG Compression Distortion

JPEG is a widely used compression format and the watermark should be resistant to it. As shown in Fig.12, with the decreasing of the quality of the JPEG compressed object, the response of the watermark detector also decreases. We have found that the proposed watermark can survive even with quality factor of 10% (see Fig.13), although the object is visibly non distorted (see Fig.14).

B. JPEG2000 Compression Distortion

JPEG2000 is the new generation compression standard, which is based on wavelet transform. In our experiments, we test the watermarked object with JPEG2000 compression. The detector response of the watermarked object Akiyo after the JPEG2000 compression with 75% quality is 0.6231. Fig. 15 shows the object after the JPEG2000 compression with 65% quality, which results in very significant distortion. The response of the watermark detector in this case is 0.5491, which is still above the threshold $T_c$ (see Fig.16).
C. Adding Noise

Noise is one of common distortions in the image processing and transmission. In the experiment, we add 30% uniform noise, 0.1% Gaussian noise and 20% Laplacian noise into the watermarked object as shown in Figs. 17, 18 and 19. The watermark can still be retrieved successfully, and the responses of the watermark detector are 0.7338, 0.3357 and 0.4298.

D. Filtering

Filtering is very common in image processing. The watermarked object was filtered with $3 \times 3$ blur filter and $5 \times 5$ median filter (see Fig. 20 and 21). The responses of the watermark detector are 0.3983 and 0.4224. These responses are well above the threshold $T_c$, even if the objects appeared degraded.

E. Rescaling

Scaling is also very easy to perform during the editing of digital images. So the watermark technique must be robust to the scaling attack. We test our scheme in the case of scaling the watermarked object by $0.5 \times 0.5$. The experiment results show the watermark can still be retrieved as shown in Fig. 23 with the detector response 0.3084.

F. Multiple Watermarking Attack

In some application scenarios, more than one watermark needs to be embedded in the object, and each watermark should be detected by the watermark detector. The original object is watermarked, then the watermarked object is again watermarked, and so on until the object with different watermarks is obtained (see Fig. 24). The detector performs well in retrieving all the two watermarks embedded in the object, as shown in Fig. 25.
G. Experiments for Video Object

In the next sections, we will give a watermark scheme for video object which is based on the previous image object watermark scheme. Fig. 26(a) shows the watermarking embedding procedure. Firstly, the MPEG-4 coded video bit stream is decoded obtaining a sequence of frames. Each frame is segmented into foreground (objects) and background and we apply the watermarking casting scheme frame by frame. The procedure of watermark embedding in MPEG-4 video object stream is performed using the following steps:

- Decode the MPEG-4 video stream using MPEG-4 decoder to obtain two different objects and shape information.
- In order to embed watermark into video objects, invoke Image Object Watermark Casting Scheme using each video object and shape information as input parameters.
- After watermark embedding, encode the two video objects into the MPEG-4 video stream using MPEG-4 encoder. Thus, we obtained the watermarked MPEG-4 video stream. In order to detect whether a MPEG-4 video stream has a watermark, we first decode the MPEG-4 video stream to obtain two different objects and shape information, and then invoke Image Object Watermark Detecting Scheme using each video object and shape information as input parameters. In this way, we obtained detection result for each video object as show in Fig. 26(b).

### Table II

<table>
<thead>
<tr>
<th>Detector responses</th>
<th>Akiyo</th>
<th>News</th>
<th>Sean</th>
<th>Lena</th>
</tr>
</thead>
<tbody>
<tr>
<td>No attack</td>
<td>0.9201</td>
<td>0.9212</td>
<td>0.9131</td>
<td>0.9251</td>
</tr>
<tr>
<td>JPEG quality 65%</td>
<td>0.6035</td>
<td>0.5535</td>
<td>0.5944</td>
<td>0.5832</td>
</tr>
<tr>
<td>JPEG quality 75%</td>
<td>0.6502</td>
<td>0.6077</td>
<td>0.6606</td>
<td>0.6321</td>
</tr>
<tr>
<td>JPEG quality 85%</td>
<td>0.6676</td>
<td>0.7253</td>
<td>0.7962</td>
<td>0.7523</td>
</tr>
<tr>
<td>JPEG2000 quality 65%</td>
<td>0.5491</td>
<td>0.5692</td>
<td>0.7245</td>
<td>0.7192</td>
</tr>
<tr>
<td>JPEG2000 quality 75%</td>
<td>0.6231</td>
<td>0.6179</td>
<td>0.8481</td>
<td>0.8256</td>
</tr>
<tr>
<td>JPEG2000 quality 85%</td>
<td>0.7296</td>
<td>0.7499</td>
<td>0.8922</td>
<td>0.8762</td>
</tr>
<tr>
<td>Uniform noise 10%</td>
<td>0.8673</td>
<td>0.8798</td>
<td>0.9022</td>
<td>0.8986</td>
</tr>
<tr>
<td>Uniform noise 20%</td>
<td>0.8024</td>
<td>0.8266</td>
<td>0.8470</td>
<td>0.8023</td>
</tr>
<tr>
<td>Uniform noise 30%</td>
<td>0.7338</td>
<td>0.7693</td>
<td>0.8040</td>
<td>0.8132</td>
</tr>
<tr>
<td>Uniform noise 100%</td>
<td>0.3565</td>
<td>0.3510</td>
<td>0.4984</td>
<td>0.4589</td>
</tr>
<tr>
<td>Laplacian noise 20%</td>
<td>0.4298</td>
<td>0.5478</td>
<td>0.5867</td>
<td>0.5867</td>
</tr>
<tr>
<td>Gaussian noise 10%</td>
<td>0.3357</td>
<td>0.3018</td>
<td>0.3307</td>
<td>0.3208</td>
</tr>
<tr>
<td>Blur filtering 3 * 3</td>
<td>0.3983</td>
<td>0.3714</td>
<td>0.4752</td>
<td>0.4684</td>
</tr>
<tr>
<td>Median filtering 5 * 5</td>
<td>0.4224</td>
<td>0.5790</td>
<td>0.6175</td>
<td>0.5869</td>
</tr>
<tr>
<td>Gaussian filtering</td>
<td>0.8404</td>
<td>0.8726</td>
<td>0.8801</td>
<td>0.8698</td>
</tr>
<tr>
<td>Scaling 75%</td>
<td>0.4382</td>
<td>0.4072</td>
<td>0.4918</td>
<td>0.4123</td>
</tr>
<tr>
<td>Scaling 50%</td>
<td>0.3084</td>
<td>0.3161</td>
<td>0.4190</td>
<td>0.4032</td>
</tr>
</tbody>
</table>

![Fig. 23. Detector response of 0.5 × 0.5 rescaling.](image1)

![Fig. 24. The object ‘Akiyo’ with two different watermarks.](image2)

![Fig. 25. Detector response of the multiple watermarked object ‘Akiyo’.](image3)

![Fig. 26. Block diagrams for Video Object Watermarking Scheme. (a) Watermark Embedding. (b) Watermark Detection.](image4)
1) MPEG-4 Compression: The video sequences are first compressed to obtain MPEG-4 coded video bitstream using easy video to mp4 converter with a rate of 500 kbits per Video Object Layer (VOL). Then, the watermarks are embedded in video objects, frame by frame, using MPEG-4 video object watermarking scheme, as shown in Fig. 26(a). The MPEG-4 video stream is next decompressed and two different objects are obtained, where the watermark detection process is applied, as shown in Fig. 26(b). The watermark detector responses of the decoded foreground objects of akiyo sequence are 0.7235 (VO 0) and 0.8834 (VO 1), as shown in Figs. 30 and 31. The responses are well above the threshold Tc and indicate that our proposed watermarking scheme is robust to MPEG4 compression.

Fig. 27. A frame of the video sequence 'akiyo'. The Video Object 3 'background'.

Fig. 28. A frame of the video sequence 'akiyo'. The Video Object 3 'foreground'.

Fig. 29. A frame of the video sequence 'akiyo'. The Video Object 3

Fig. 30. Watermark detection response relating to the Video Object 3(foreground), after MPEG-4 compression.

Fig. 31. Watermark detection response relating to the Video Object 3(background), after MPEG-4 compression.

2) Format Conversion From MPEG-4 To MPEG-2: The watermarked MPEG-4 video bitstream is decompressed and frames are obtained. These frames are compressed MPEG-2 coded video bitstream using AVS video converter 6.2 and Easy video converter V 4.2. Next, the MPEG-2 coded video bitstream is decompressed, and each frame is separated so different objects are obtained, where the watermark detection process is applied. As shown in Figs. 32 and 33 both watermarks embedded in the two objects are easily detected which indicates that the proposed scheme is robust to conversion from MPEG-4 to MPEG-2.

Fig. 32. Watermark detection response relating to the Video Object 3(foreground) after format conversion from MPEG-4 to MPEG-2.
V. Conclusion

In this article, a novel blind object watermarking scheme for images and video using the in place lifting SA-DWT has been proposed. To make the watermark robust and transparent, we embed it in the average of the wavelet blocks using visual mode. The visual model takes into account sensitivity to brightness and texture. Experimental results show that this scheme is robust to common signal processing procedures such as compression, median filtering and additive noise. Efficiency of the method is revealed on the basis of the following results:

- the average has a smaller change than that of individual coefficient. Thus, unlike most watermarking schemes, the watermark is not embedded by just an individual wavelet coefficient but by modulating the average of the wavelet blocks.
- visual model allowed to achieve the best tradeoff between transparency and robustness.
- watermark detection is accomplished without the original.
- many parameters can be used as private key to that they are unknown to public. However, the proposed approach needs some improvement to overcome low performance obtained in terms of robustness to Gaussian noise.

References