9

Comparison of "Spread-Quantization" Video Watermarking Techniques for Copyright Protection in the Spatial and Transform Domain

Radu Ovidiu Preda and Nicolae Vizireanu
Politehnica University of Bucharest
Romania

1. Introduction

In spite of the existence of watermarking technique for all kinds of digital data, most of the literature addresses the watermarking of still images for copyright protection and only some work is extended to video watermarking. Video watermarking is distinct from image watermarking, because there is more data available to both the attacker as well as to the watermarker. This additional data volume allows the payload to be more redundantly and reliably embedded.

Video watermarking schemes are characterized by the domain that the watermark is being embedded or detected, their capacity, the perceptual quality of the watermarked videos and their robustness to particular types of attacks. They can be divided into three main groups according to the domain in which the watermark is embedded: spatial domain, frequency domain and compressed domain watermarking. An overview of video watermarking techniques can be found in (Gwenael & Dugelay, 2003).

The spatial domain algorithms embed the watermark directly into the pixel values and no transforms are applied to the host signal during the embedding process. The most common techniques to insert the watermark into the host data in the spatial domain is via Least Significant Bit modification, Spread Spectrum Modulation and Quantization Index Modulation.

The easiest way to embed a watermark in the spatial domain is the LSB method. If each pixel in an image is represented by an 8-bit value, the image/frame can be sliced up in 8 bit planes. The least significant bit plane does not contain visually significant information and can easily be replaced by the watermark bits. There are also some more sophisticated algorithm that makes use of LSB modification (Kinoshita, 1996). These techniques are not very robust to attacks because the LSB plane can be easily replaced by random bits, removing the watermark.

Spread spectrum watermarking views watermarking as a problem of communication through a noisy channel. As a means to combatting this noise or interference, spread-spectrum techniques are employed to allow reliable communication in such noisy environments. In this case, the watermark data is coded with a pseudorandom code sequence to spread its power spectrum in the image or video, thus increasing its robustness to attacks. One of the first methods was the one-dimensional spread spectrum approach (Hartung & Girod, 1998). Here, the watermark is a pseudo-random sequence spread over the video frames by direct spatial domain addition. The watermark is repeatedly embedded throughout the video in a sequential manner. Other more complicated spread-spectrum methods were proposed in (Celik et al., 2008), (Altun et al., 2009), (Maity, S.P. & Maity, S., 2009).

Quantization IndexModulation (QIM) refers to a class of data hiding schemes that exploit Costa's (Costa, 1983) now famous findings by embedding information in the choice of quantizers. Over the past few years, QIM-based data hiding has received increasing attention from the data hiding community because it is more robust than techniques such as spread spectrum and LSB modification. State of the art proposed QIM schemes include Chen and Wornell's QIM and dither modulation (Chen & Wornell, 2001), Eggers et al's scalar Costa scheme (SCS) (Eggers et al., 2003), Jie and Zhiqiang's color image QIM scheme (Jie & Zhiqiang, 2009) and Kalantari and Ahadi's logarithmic QIM scheme (Kalantari & Ahadi, 2010).

For frequency domain watermarking, the most common transforms being used are the Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT) and Discrete Wavelet Transform. The main advantage offered by transform domain techniques is that they can take advantage of special properties of the alternate domains to address the limitations of pixel-based methods or to support additional features. For instance, a watermarking scheme in the DCT domain achieves better implementation compatibility with popular video coding algorithms such as MPEG. Also, they have better resistance to compression based attacks. Generally, the main drawback of transform domain methods is their higher computational requirements.

Image and video watermarking in the Discrete Cosine Transform domain is very popular, because the DCT is still the most popular domain for digital image processing. The DCT allows an image to be broken up into different frequency sub-bands, making it much easier to embed watermarking information into the middle frequency sub-bands of an image or video frame. One of the first DCT based algorithms, upon which many variations have been based, is presented in (Cox et al., 1997). The watermark is a normally distributed sequence of real numbers added to the full-frame DCT of each video frame. More advanced techniques were also proposed in (Suhail & Obaidat, 2003), (Liu, L. et al., 2005), (Yang et al., 2008). The choice of the DCT coefficients for watermark embedding is a compromise between the quality degradation of the image/frame (frequency of the coefficients should be high) and the resilience of the watermarking scheme to attacks (frequency of the coefficients should be low).

Lately, algorithms in the Wavelet domain have gained more popularity due to their excellent spatial localization, frequency spread, and multi-resolution characteristics (Barni et al., 2001), (Reddy & Chatterji, 2005), (Ellinas & Kenterlis, 2006), (Zou et al., 2006), (El-Taweel, 2007), (Coria et al., 2008), (Preda & Vizireanu, 2011). The Discrete Wavelet Transform (DWT) separates an image into a lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components. The process can then be repeated to compute multiple scale wavelet decompositions. Many embedding techniques in the wavelet domain use similar approaches to those in the DCT domain.

Watermarking schemes performed in the compressed domain include those for MPEG 1-4 (Liu Z. et al., 2004), (Biswas et al., 2005), (Preda & Vizireanu, 2007) and H.26x (Zhang et al., 2007) compressed videos. Video watermarking techniques that use MPEG/H.26x coding structures as primitive components are primarily motivated with the goal of integrating watermarking and compression to reduce overall real-time video processing complexity. Such methods usually embed the watermark directly into the VLC code by modifying the transform domain coefficients (Biswas et al., 2005), (Preda & Vizireanu, 2007), (Zhang et al., 2007) or the motion vector information (Liu Z. et al., 2004). The main drawback of such methods is that they are bound to a specific compression standard and any transcoding to a different format would destroy the watermark.

The goal of this chapter is to compare the performances of three different proposed video watermarking schemes in the spatial, DCT and Wavelet domain. A lot of research has been done lately in developing new and improved watermarking techniques, but there is a difficulty in comparing the research results, because independent researchers use very different watermarks, watermark capacity, test videos, parameters for watermark embedding and extraction and attacks with different parameters to test the robustness of their schemes. There is a need to compare the watermarking methods in different domains. Our chapter addresses this issue by proposing three approaches in the spatial, DCT and Wavelet domain that have similar specifications, like watermark, watermark capacity, test videos, attacks with the same parameters. All approaches embed the same watermark (binary image) with spatial and temporal redundancy and use a blind method for watermark extraction.

The rest of this chapter is organized as follows: Section 2 describes the three proposed video watermarking techniques, providing detailed diagrams and description of the watermark embedding and extraction strategies. Section 3 contains the experimental results and a detailed comparison of the proposed methods in terms of perceptual quality and robustness to different attacks. Finally, Section 4 presents the conclusions of our work and possible future research.

2. Proposed "Spread-Quantization" video watermarking techniques

This section presents our watermarking schemes in the spatial, Discrete Cosine Transform (DCT) and Wavelet domain. First we will summarize some common properties of the proposed algorithms and then, in Subsections 2.1 to 2.3 the detailed embedding and extraction schemes will be presented for every method.

The proposed watermarking techniques are a combination of spread-spectrum and quantization based watermarking. That is why we call them "spread-quatization" techniques.

Our methods embed the watermark into the luminance values of the pixels or into some selected coefficients in a transform domain, thus all algorithms will first do a conversion of the RGB (Red, Green, Blue) color space into the YC_bC_r (ITU-R BT.601) color space, as shown in Equation (1):

$$\begin{aligned} Y &= 0.257R + 0.504G + 0.098B + 16 \\ C_b &= -0.148R - 0.291G + 0.439B + 128 \\ C_r &= 0.439R + 0.368G - 0.071B + 128 \end{aligned} \tag{1}$$

After the watermark embedding, the video is converted back to the RGB format using Equation (2):

$$\begin{aligned} R &= 1.164(Y-16) + 1.596(C_r - 128) \\ G &= 1.164(Y-16) - 0.813(C_r - 128) - 0.391(C_b - 128) \\ B &= 1.164(Y-16) + 2.018(C_b - 128) \end{aligned} \tag{2}$$

To improve the resilience of the proposed algorithms to attacks, two protection mechanisms are used:

- The watermark is coded using a low complexity error correction code (*m,n*), where *n* is the dataword length and *m* is the codeword length. Using the error correction code, the useful size of the watermark will be *m/n* times smaller in comparison to the case when no error correction code is used.
- The same watermark is redundantly embedded in a number of *k* frames. Thus, the useful size of the watermark will be *k* times smaller, but the resilience to attacks is improved. At the watermark decoder, after extracting the watermark sequence w_i' of size *P′* bits from every frame of a number of *k* frames, a bit of the useful watermark $w'(j)$ is computed using Equation (3).

$$w'(j) = \begin{cases} 0, & \text{if } \sum_{i=1}^{k} w_i'(j) \le \frac{k}{2} \\ 1, & \text{if } \sum_{i=1}^{k} w_i'(j) > \frac{k}{2} \end{cases}, \quad j \in \{1,2,\ldots,P'\} \tag{3}$$

2.1 Video watermarking scheme in the spatial domain

The watermark embedding process, illustrated in Fig. 1, is described in the following steps:

1. The original video is partitioned into groups of *k* frames.
2. Every frame of the group is converted to the YC_bC_r format as in Equation (1).
3. The binary image matrix is transformed into a binary row vector *w* of size $P = h \times v$.
4. To protect the watermark against bit errors, a Hamming error correction code (*m,n*) with codeword length of *m* bits and data-word length of *n* bits is applied to the vector *w*. The size of the resulting watermark vector w_c is:

$$P^{'} = P\frac{m}{n} \tag{4}$$

The binary sequence w_c is partitioned into a number of $\frac{F}{k}$ sequences $w_c(j)$ of size $P'\frac{k}{F}$, where $j = \overline{1,\frac{F}{k}}$, *F* is the number of frames of the video and *k* is the number of redundant frames. The dimensions *h* and *v* of the watermark are chosen so that $P'\frac{k}{F}$ is an integer. The same sequence $w_c(j)$ will be inserted into every frame of a group *j* of *k* frames.

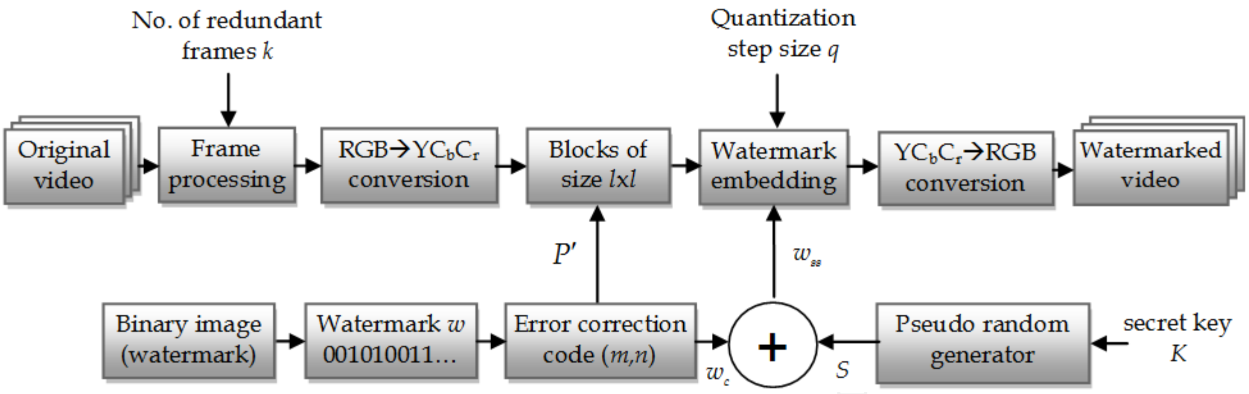


Fig. 1. Block diagram of the spatial watermark encoder

5. The size l of a square bloc of $l \times l$ luminance values is calculated to embed a bit of the watermark:

$$l = \left[\sqrt{\frac{MNC}{P'k}} \right] \tag{5}$$

where [.] is the integer part operator.

6. A spread-spectrum technique is used to spread the power spectrum of the watermark data, thus, increasing its robustness against attacks. First a binary pseudo-random sequence $S = \left\{ s_r \middle| s_r \in \{0,1\}, r = 1, \ldots, l^2 \right\}$ of size l^2 with equal number of zeros and ones is generated using the Mersenne-Twister algorithm proposed in (Matsumoto & Nishimura, 1998) with the use of the last 64 bits of the secret key K as seed for the generator. This method generates numbers with a period of $(2^{19937} - 1)/2$.
7. For every bit of the watermark $w_c(j)$, the corresponding spread spectrum sequence is:

$$w_{ss} = \begin{cases} [s_1, s_2, \ldots, s_{l^2}], & \text{if } w_c = 0 \\ [\bar{s}_1, \bar{s}_2, \ldots, \bar{s}_{l^2}], & \text{if } w_c = 1 \end{cases} \tag{6}$$

8. A sequence S (representing one bit of the original watermark) is embedded in every bloc of $l \times l$ luminance values.
9. A bit of S is embedded into the luminance value of the pixel of the same index by rounding its value to an even or odd quantization level. Rounding to an even quantization level embeds a “0”, while rounding to an odd quantization level embeds a “1”, as shown in Equation 6:

$$L_w(i,j) = \left[\frac{L}{2q} \right] \cdot 2q + q \cdot w \cdot sign\left(L(i,j) - \left[\frac{L(i,j)}{2q} \right] \cdot 2q \right), \tag{7}$$

where $L(i,j)$ is the original luminance value, $L_w(i,j)$ is the watermarked luminance value, q is the quantization step size and $sign()$ is defined as:

$$sign(x) = \begin{cases} -1\,, & if\ x \le 0 \\ 1\,, & if\ x > 0 \end{cases} \tag{8}$$

Wat. bit	Pseudo-random sequence S	Spread spectrum watermark $w_{ss} = S \oplus w$	Quant. step size	Original luminance block	Watermarked luminance block
w=0	$\begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}$	q=4	$\begin{bmatrix} 224 & 75 & 86 & 20 \\ 62 & 45 & 12 & 123 \\ 45 & 5 & 68 & 74 \\ 145 & 59 & 247 & 23 \end{bmatrix}$	$\begin{bmatrix} 224 & 76 & 84 & 24 \\ 60 & 48 & 12 & 120 \\ 48 & 4 & 72 & 76 \\ 148 & 60 & 248 & 24 \end{bmatrix}$
w=1		$\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$			$\begin{bmatrix} 228 & 72 & 88 & 20 \\ 64 & 44 & 16 & 124 \\ 44 & 8 & 68 & 72 \\ 144 & 56 & 244 & 20 \end{bmatrix}$

Table 1. Example of embedding a watermark bit into a block of 4x4 luminance pixels

10. The video is converted back to the RGB format using Equation 2, obtaining the watermark video.

The choice of the quantization step *q* is a tradeoff between the perceptual quality of the watermarked video (*q* must have a small value) and the resilience of the watermarking scheme to attacks (*q* must have a big value). An example of embedding a watermark bit into a block of 4x4 pixels is given in Table 1.

The watermark extraction process, shown in Fig. 2, implies the following steps:

1. The watermarked video is partitioned into groups of *k* frames.
2. Every frame of the group is converted to the YC_bC_r format using Equation 1.
3. Every luminance frame is partitioned into square blocks of $l \times l$ luminance values.
4. A bit of the spread spectrum sequence w_{ss}' of size l^2 is extracted from every luminance value of a block of size $l \times l$ using Equation (9):

$$w' = \mathrm{mod}\,2\left(round\left(\frac{L_w(i,j)}{q} \right) \right), \tag{9}$$

where w' is the extracted watermark bit, $L_w(i,j)$ is the luminance value of the pixel at position (*i,j*), *q* is the quantization step size and *mod2* is the modulo2 function.

5. Using the 64 bit seed from the secret key *K* the binary sequence *S* is generated locally.
6. The extracted watermark bit for the corresponding block is:

$$w_b{}' = \begin{cases} 0, & \text{if } \sum_{r=1}^{l^2} \left| w_{ss,r}{}' - s_r \right| \le \frac{l^2}{2} \\ 1, & \text{if } \sum_{r=1}^{l^2} \left| w_{ss,r}{}' - s_r \right| > \frac{l^2}{2} \end{cases} \tag{10}$$

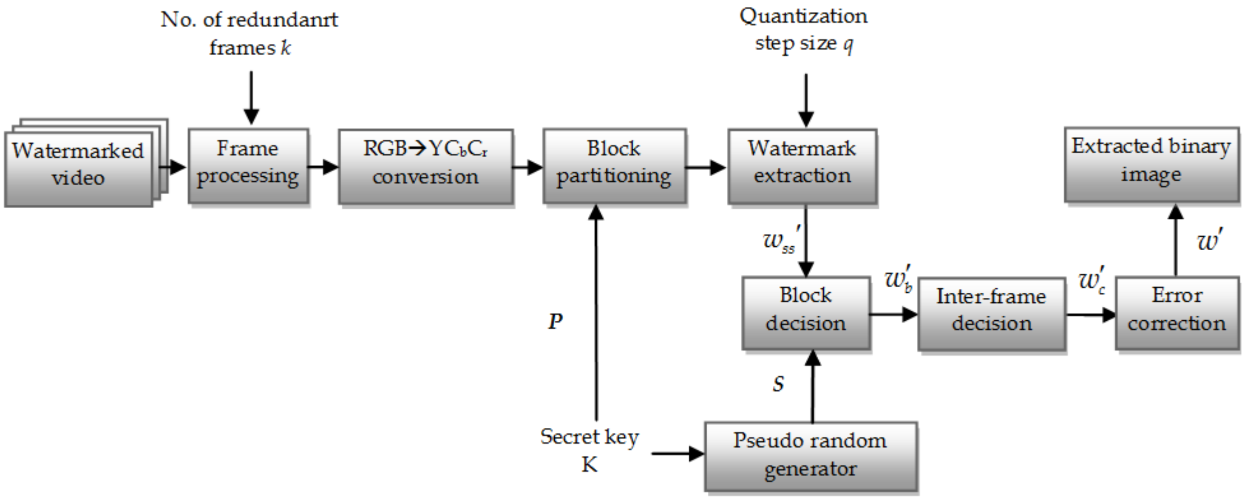


Fig. 2. Block diagram of the spatial watermark decoder

7. A binary sequence $w'_{c,i}(j)$ is extracted from every frame of a group of k frames, where $i = \overline{1,k}$. The sequence $w'_c(j)$ is computed from $w'_{c,i}(j)$ using Equation (11):

$$w'_c(j) = \begin{cases} 0, & \text{if } \sum_{i=1}^{k} w'_{c,i}(j) \le \frac{k}{2} \\ 1, & \text{if } \sum_{i=1}^{k} w'_{c,i}(j) > \frac{k}{2} \end{cases} \quad , \quad j \in \{1,2,\ldots,P'\} \tag{11}$$

8. The resulting watermark bitstream w'_c of size P' is error corrected and the watermark w' of size P is obtained.
9. The extracted binary image is obtained by reshaping the vector w' to a matrix of size $h \times v$.

The choice of the quantization step size q is a tradeoff between the perceptual quality of the watermarked video (q should have a small value) and the resilience of the watermarking scheme to attacks (q should have a big value).

2.2 Video watermarking scheme in the Discrete Cosine Transform domain (DCT)

For this method, the watermark is redundantly inserted in the DCT domain. Compared to the previous method in the spatial domain this technique works with blocks of 8x8 luminance pixels. Every Y block is transformed into a 8x8 DCT coefficient block. To insert the watermark, only 22 DCT coefficients from every block are used, as shown in Fig. 3, where the white coefficients are ignored and only the gray coefficients are used for redundant watermark embedding. Instead of step 6 of the spatial domain embedding strategy, this algorithm calculates the number b of 8x8 DCT coefficient blocks, where the same watermark bit can be redundantly embedded, as shown in Equation (12).

$$b = \left\lfloor \frac{1}{64} \frac{MNF}{P'k} \right\rfloor \tag{12}$$

where *MxN* is the resolution of the video, *F* is the number of frames of the video, k is the number of redundant frames, P' is the watermark size after applying the error correction code and [.] is the the integer part operator.

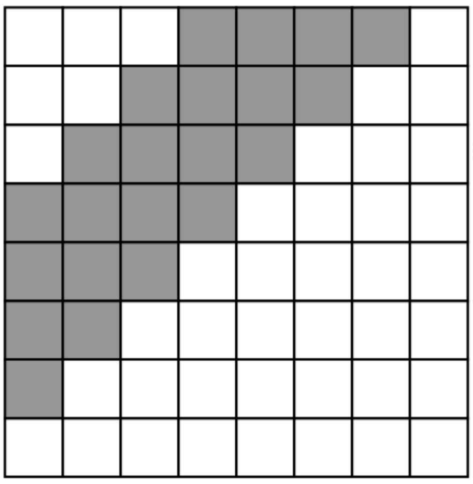


Fig. 3. DCT coefficient selection for watermark embedding

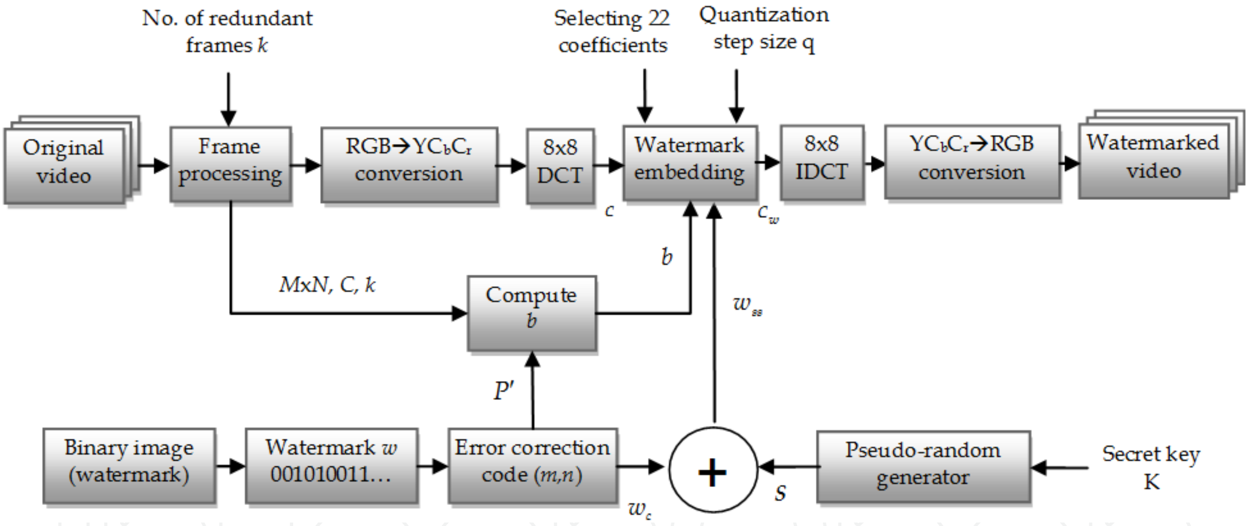


Fig. 4. Block diagram of the DCT watermark encoder

The binary pseudo-random sequence S generated using the secret key K has a fixed size, equal to the number of DCT coefficients selected from every 8x8 coefficient block.

$$S=\left\{s_r \middle| s_r \in\{0,1\}, r=1,\ldots,22\right\} \tag{13}$$

The same watermark bit will be inserted in a number of *22* DCT coefficients using the spread-spectrum sequence $w_{ss}(i)$ obtained using Equation (14).

$$w_{ss}=\begin{cases}[s_1,s_2,\ldots,s_{22}], & \text{if } w_c=0\\ [\bar{s}_1,\bar{s}_2,\ldots,\bar{s}_{22}], & \text{if } w_c=1\end{cases} \tag{14}$$

Every coefficient of index *i* is quantized to an even or odd number of quantization step sizes according to the value of the bit $w_{ss}(i)$, using Equation (15). The watermark embedding process is illustrated in Fig. 4.

$$c_w(i) = \left[\frac{c(i)}{2q}\right] \cdot 2q + q \cdot w_{ss}(i) \cdot sign\left(c(i) - \left[\frac{c(i)}{2q}\right] \cdot 2q\right),\ i = 1,2,...,22 \tag{15}$$

where $c(i)$ is the original DCT coefficient and $c_w(i)$ is the watermarked DCT coefficient.

At the decoder side (Fig. 5) first the number *b* of DCT coefficient blocks is calculated. From every coefficient selected according to Fig. 3 a bit is extracted using Equation (16), resulting in a sequence $w'_{ss}(j)$ of 22 bits from every block.

$$w' = \mathrm{mod}\,2\left(round\left(\frac{c_w}{q}\right)\right) \tag{16}$$

The spread-spectrum sequence w''_{ss} corresponding to an inserted watermark bit is obtained from *b* blocks of coefficients as in Equation (17).

$$w''_{ss,r} = \begin{cases} 0, & \text{if } \sum_{j=1}^{b} w'_{ss,r}(j) \le \frac{b}{2} \\ 1, & \text{if } \sum_{j=1}^{b} w'_{ss,r}(j) > \frac{b}{2} \end{cases},\quad r \in \{1,2,\ldots,22\} \tag{17}$$

Then the pseudo-random bit sequence *S* is locally generated using the secret key *K*. The extracted watermark bit $w_b{}'$ corresponding to a group of *b* coefficient blocks is computed in Equation (18).

$$w_b{}' = \begin{cases} 0, & \text{if } \sum_{r=1}^{22} \left| w''_{ss,r} - s_r \right| \le 11 \\ 1, & \text{if } \sum_{r=1}^{22} \left| w''_{ss,r} - s_r \right| > 11 \end{cases} \tag{18}$$

A binary sequence $w'_b(j)$ is extracted from every frame of a group of *k* frames, with $j = 1,2,...,k$. Every bit of the sequence w'_c corresponding to a group of *k* frames is determined using Equation (19):

$$w'_c(i) = \begin{cases} 0, & \text{if } \sum_{j=1}^{k} w'_b(j) \le \frac{k}{2} \\ 1, & \text{if } \sum_{j=1}^{k} w'_b(j) > \frac{k}{2} \end{cases},\quad i = 1,2,\ldots,P' \tag{19}$$

The bit sequence $w'_c(i)$ is then error corrected obtaining the extracted watermark sequence w'.

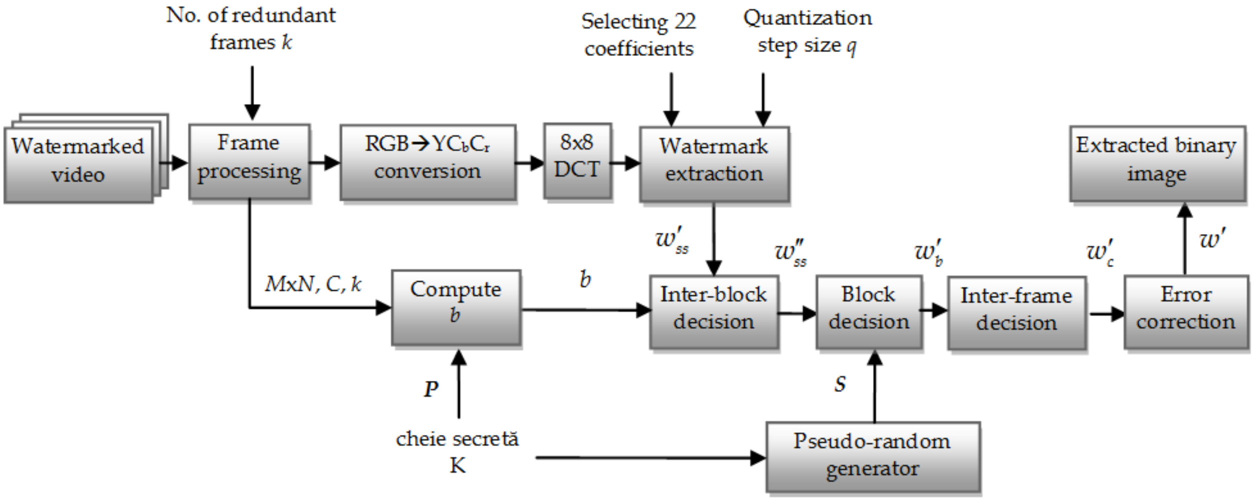


Fig. 5. Block diagram of the DCT watermark decoder

2.3 Video watermarking scheme in the wavelet domain

For this method the watermark is embedded in the selected wavelet coefficients of the luminance Y of every frame of the video. The wavelet decomposition of the luminance is done using the 2D Discrete Wavelet Transform. We have chosen a Wavelet decomposition on L=3 resolution levels. The watermark is embedded in the wavelet coefficients of the LH, HL and HH sub-bands of the second Wavelet decomposition level. The choice of the second decomposition level is a tradeoff between the invisibility of the watermark and the resilience to attacks. A watermark embedded in the wavelet coefficients of the LH_1, HL_1 and HH_1 sub-bands is very sensitive to attacks, because these sub-bands contain the finest details of the frame. On the other hand, if we embed the watermark in the LH_3, HL_3 and HH_3 sub-bands, the perceptual quality of the video will be significantly altered. For these reasons, the best choice for watermark embedding is the second wavelet decomposition level. Fig. 6 shows the sub-bands (gray color) selected for watermark embedding.

For videos of resolution $M \times N$, the number of selected wavelet coefficients for a frame is:

$$C = 3\frac{MN}{2^{2(L-1)}} \tag{20}$$

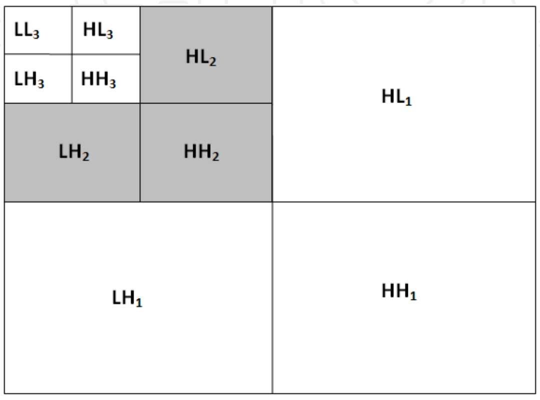


Fig. 6. Wavelet sub-bands selected for watermark embedding

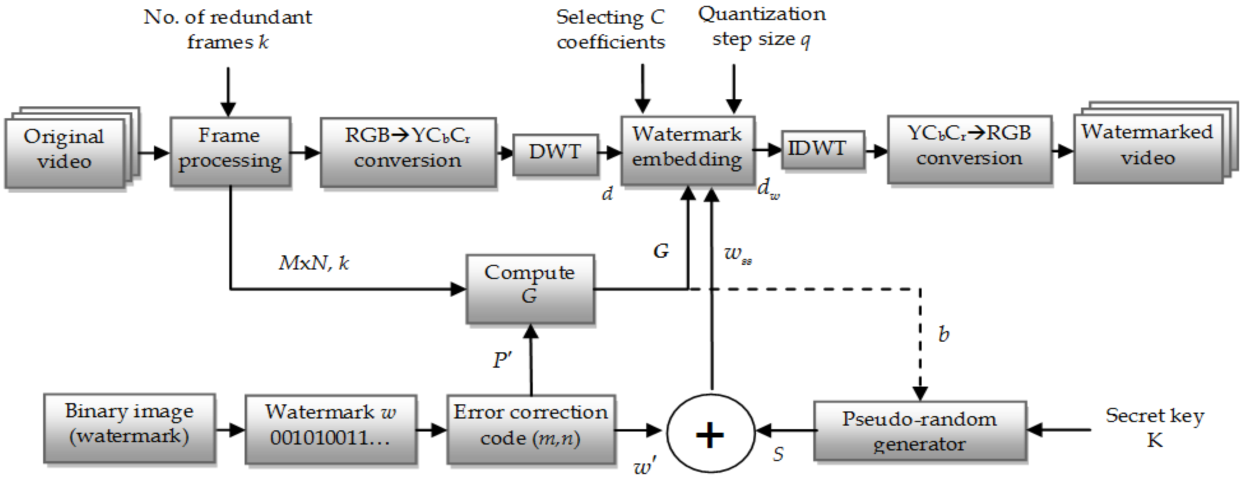


Fig. 7. Block diagram of the wavelet watermark encoder

The maximum capacity of the watermarking scheme is $C' = FC$ where F is the number of video frames and can be achieved by embedding a watermark bit in every selected wavelet coefficient. For example, for CIF videos of resolution 352x288 and 30 frames/s, the maximum capacity is 556kb/s. This maximum capacity is not needed in most applications, thus we will reduce it to improve the robustness of the scheme. Fig. 7 shows the block diagram of our Wavelet based watermark embedding scheme and is described in the following steps:

1. The binary image matrix is transformed into a binary row vector w of size $P = h \times v$.
2. To protect the watermark against bit errors, a Hamming error correction code with codeword length of m bits and dataword length of n bits is applied to vector w. The size of the resulting watermark vector w' is:

$$P' = P\frac{m}{n} \tag{21}$$

3. A same spread-spectrum technique is used to spread the power spectrum of the watermark data, thus, increasing its robustness against attacks. First the binary pseudorandom code sequence $S = \left\{ s_j \middle| s_j \in \{0,1\}, j = 0,1,...,G \right\}$ with equal number of zeros and ones is generated using the Mersenne-Twister algorithm with the use of 64 bits of the secret key K as seed for the generator. For every bit of the watermark w', the corresponding spread spectrum sequence is:

$$w_{ss}(i) = \begin{cases} [s_1, s_2, ..., s_G], & if\ w'(i) = 0 \\ [\bar{s}_1, \bar{s}_2, ..., \bar{s}_G], & if\ w'(i) = 1 \end{cases}, \ i = 1, ..., P' \tag{22}$$

4. Every sequence $w_{ss}(i)$ (representing one bit of the original watermark) is embedded into a number G of wavelet coefficients, every bit of $w_{ss}(i)$ in a wavelet coefficient. The number G depends on the number C of the selected wavelet coefficients, the number of frames F of the original video and the size $P^{'}$ of the watermark:

$$G = \left[\frac{C \cdot F}{P'} \right] \tag{23}$$

where [.] is the integer part operator.

5. A bit of the binary sequence S is embedded in the selected wavelet coefficient by rounding its value to an even or odd quantization level. Rounding to an even quantization level embeds a "0", while rounding to an odd quantization level embeds a "1", as shown in Equation (5):

$$d_w = \left[\frac{d}{2q}\right]\cdot 2q + q\cdot w\cdot sign\left(d \; - \left[\frac{d}{2q}\right]\cdot 2q\right), \tag{24}$$

where d is the original wavelet coefficient, d_w is the watermarked wavelet coefficient and q is the quantization step size.

6. After the entire watermark has been embedded, the 2D Inverse Discrete Wavelet Transform is computed for every frame to obtain the watermarked video.

The watermark extraction process, shown in Fig. 8, implies the following steps:

1. Wavelet decomposition of the watermarked, possibly attacked video;
2. Selection of the wavelet coefficients used for embedding;
3. Computation of the parameter G using the information about the size of the watermark provided by the secret key K;
4. From every coefficient selected according to Fig. 6 a bit is extracted according to Equation (25), resulting in a sequence $w'_{ss}(j)$ of G bits from every group.

$$w' \; = \mathrm{mod}_2\left(round\left(\frac{d_w}{q}\right)\right), \tag{25}$$

where d_w is the watermarked wavelet coefficient.

5. Using the 64 bit seed from the secret key K the binary sequence S of size G is generated.
6. The extracted watermark bit $w''(i)$ corresponding to a group of G wavelet coefficients is computed in Equation (26).

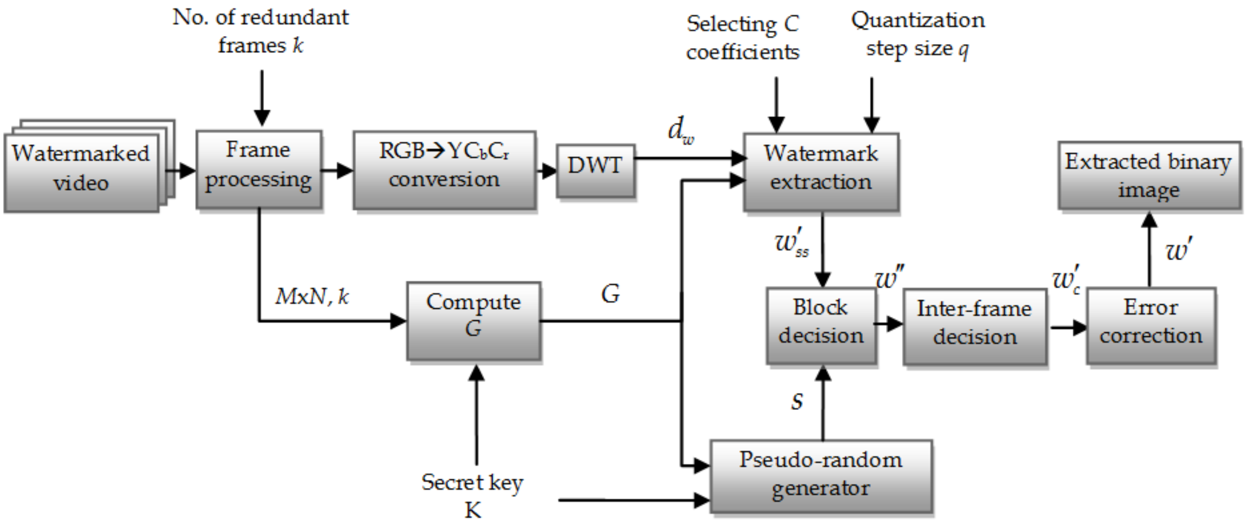


Fig. 8. Block diagram of the wavelet watermark decoder

$$w''(i) = \begin{cases} 0, if \ \sum_{j=1}^{G} [w'_j(i) - s_j] \le \frac{G}{2} \\ 1, if \ \sum_{j=1}^{G} [w'_j(i) - s_j] > \frac{G}{2} \end{cases}, i = 1,...,P' \quad (26)$$

7. The resulting watermark bitstream of size P' is error corrected and the watermark w' of size P is obtained.
8. The extracted binary image is obtained by reshaping the vector w' to a matrix of size $h \times v$.

To improve the resilience of the algorithm against temporal attacks we embedded the same watermark redundantly in every *k* frames. Thus, the number of wavelet coefficients used for embedding a watermark bit is decreased from *G* to *G/k*.

3. Comparison of the proposed “Spread-Quantization” video watermarking techniques

The simulation results were conducted on the first 27 frames of the videos “stefan”, “forman” and “bus” in RGB uncompressed avi format, of resolution 352x288 (Common Intermediate Format), 24 bits/pixel and frame rate of 30 frames/s. The binary image used as watermark is shown in Fig. 9. The resolution of the image depends on the error correction code used, the number of redundant frames and the resolution of the initial video.

Fig. 9. Binary image used as watermark

We have conducted the experiments for every proposed method using the quantization step sizes $q = 2$, $q = 4$ and $q = 8$, no redundant frame embedding, embedding of the same watermark in $k = 3$ and $k = 9$ frames, without using an error correction code and using a Hamming (7,4) error correction code.

First we wanted to test the perceptual quality of the watermarked videos. To compare the watermarked video with the original one, we computed the mean Peak Signal to Noise Ration (PSNR) of all frames of the video.

$$PSNR = \frac{\sum_{i=1}^{F} PSNR(i)}{F} \quad (27)$$

where F is the number of frames of the video.

The PSNR results are shown in Fig. 10. We can see that the best quality for every quantization step size chosen is obtained using the Wavelet approach, followed by the DCT and the spatial method. The PSNR results for the spatial watermarking scheme are quite low for quantization with bigger quantization step sizes (for $q = 4$ and $q = 8$ below the accepted

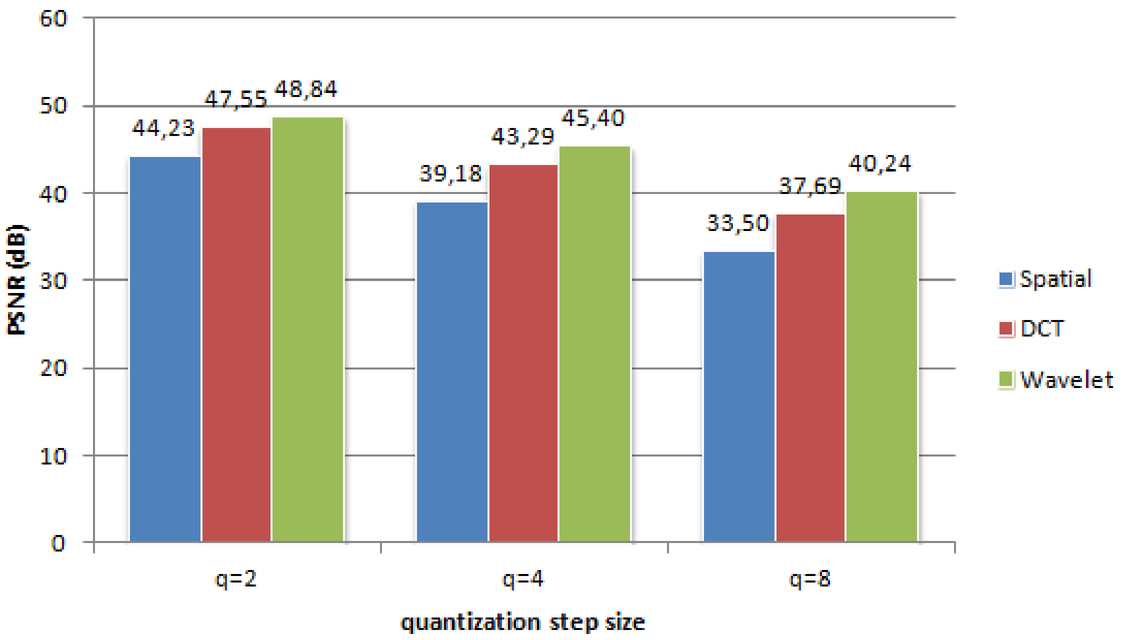


Fig. 10. PSNR values for the three proposed methods for different quantization step sizes

value of 40 dB). For $q = 8$ only the wavelet based technique achieves a PSNR value higher than 40 dB.

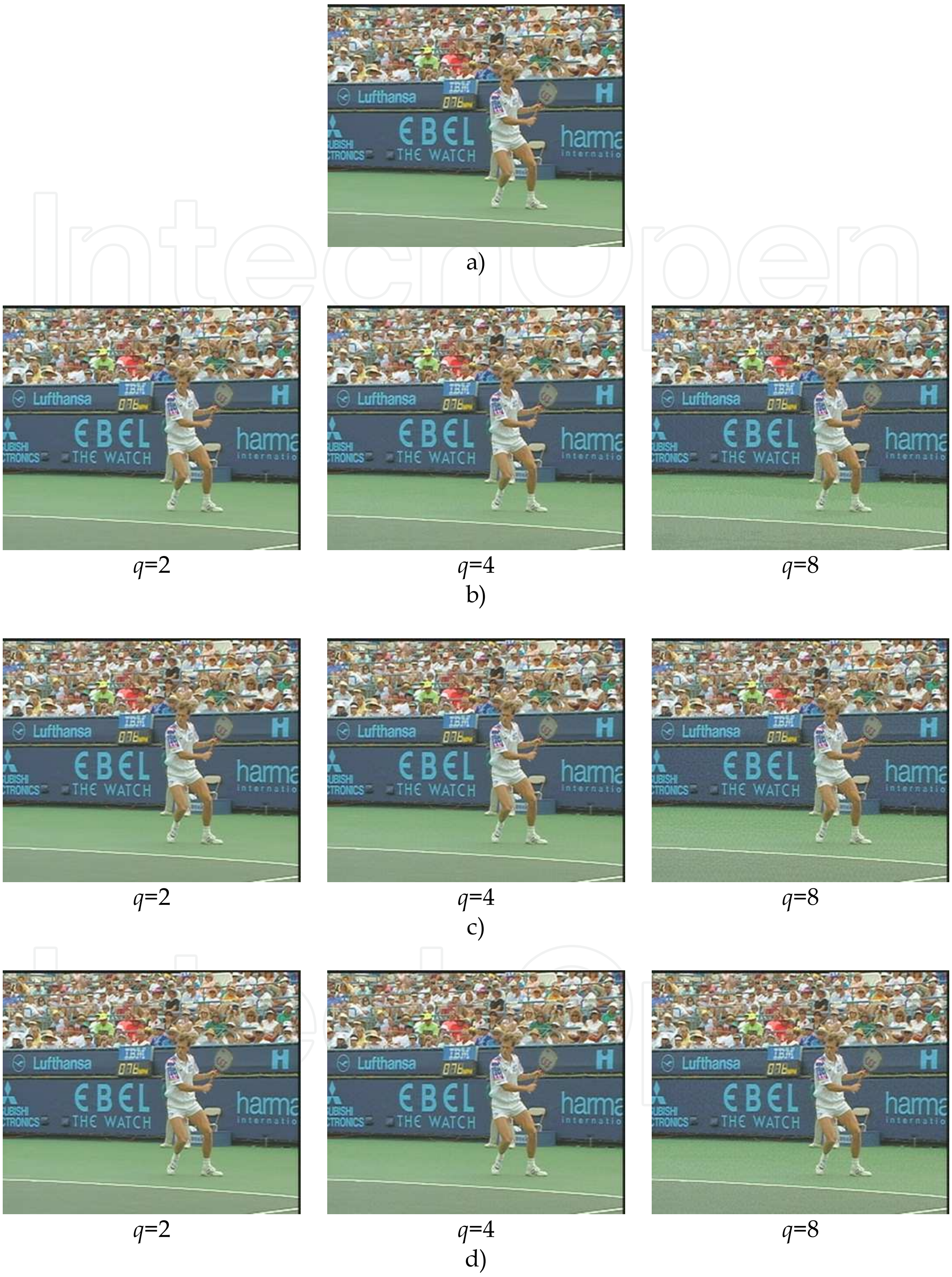
For a visual comparison, Figure 11 shows the fifth frame of the original stefan video and the corresponding watermarked frames for the three proposed methods using the quantization step sizes $q = 2$, $q = 4$ and $q = 8$.

Next, we wanted to test the robustness of the proposed watermarking schemes. For this purpose we have carried out a range of eight attacks on the watermarked videos (see Table 2). The parameters of the attacks were chosen in such a manner, that the visual degradation of the attacked videos is acceptable, because, by attacking a watermarked video, an attacker wants to destroy the watermark, but not the video quality.

To evaluate the robustness objectively, we have calculated the mean values of the decoding BER for the watermarks extracted from all test videos after they were attacked:

$$BER = \frac{1}{P}\sum_{j=1}^{P}\left|w_{out}(j) - w_{in}(j)\right|, \tag{28}$$

where w_{out} is the extracted watermark, w_{in} is the original watermark and P is the size of the watermark. We have plotted 9 different graphs (Fig. 12 - 20), where we represented the mean decoding BER for every method and every attack. The variables are the quantization step size q (chosen 2, 4 and 8) and the number of frames k used for embedding the same watermark (chosen 1, 3 and 9). For $q = 2$ no error correction code was used, because the corresponding BER values are quite high and the Hamming (7,4) error correction would not work for such high bit error rates. For $q = 4$ and $q = 8$, where the BER values are lower, we used the Hamming (7,4) error coreection code, which can correct single bit errors.



a)

q=2 *q*=4 *q*=8

b)

q=2 *q*=4 *q*=8

c)

q=2 *q*=4 *q*=8

d)

Fig. 11. Visual comparion of the proposed methods. The fifth frame of a) the original "stefan" video, b) the watermarked video using the spatial approach, c) the watermarked video using the DCT approach and d) the watermarked video using the Wavelet approach

Attack	Parameters
Blurring	blocks of 2x2 pixels
Brightening	adding Y_0=6 to the luminance of every pixel
Addition of Gaussian noise	mean 0 and variance 0,0003
Median filtering	using a 3x3 pixel neighborhood
Addition of "salt and pepper" noise	density 0,3%
Frame averaging	20% of the frames were averaged, where the current frame is the mean of the previous, current and next frame of the video
JPEG compression of every frame	quality factor Q=60
MPEG-2 compression	4 Mbps
MPEG-2 compression	2 Mbps

Table 2. Attacks against the watermarking schemes

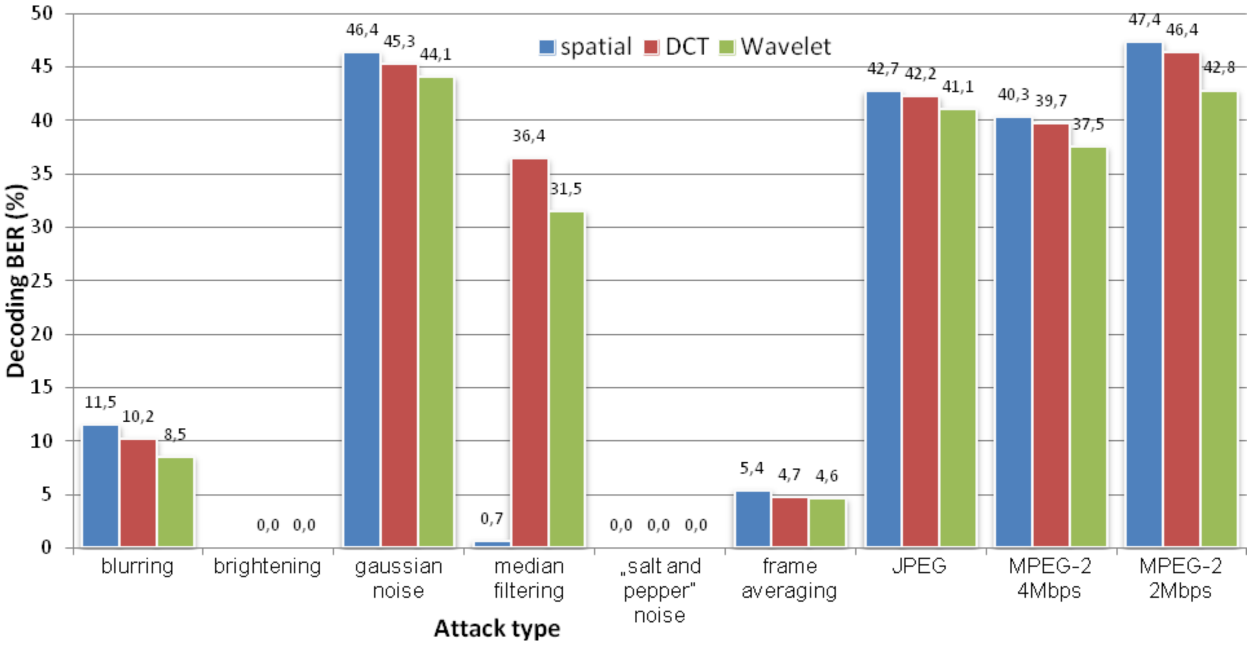


Fig. 12. Comparison of the decoding BER (%) for the proposed methods using $q = 2$, no redundant frame embedding and no error correction code

The method working in the spatial domain is very vulnerable to the brightening attack. For example by adding Y=6 to every luminance value, the decoding BER is 100% for every combination of parameters. We didn't represent this value on the graphs, because we didn't want to scale all BER values to 100%. On the other hand, the spatial embedding method has the best resilience to median filtering attacks. The DCT based technique is more vulnerable to the median filtering attack than the other two methods.

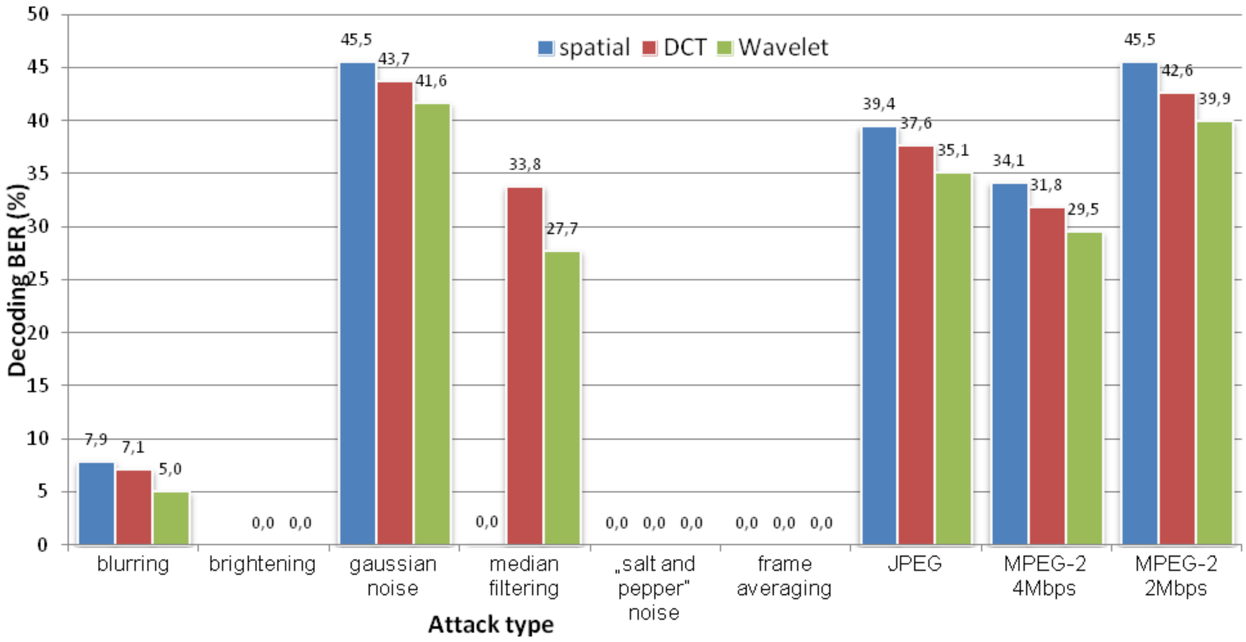


Fig. 13. Comparison of the decoding BER (%) for the proposed methods using $q = 2$, $k = 3$ and no error correction code

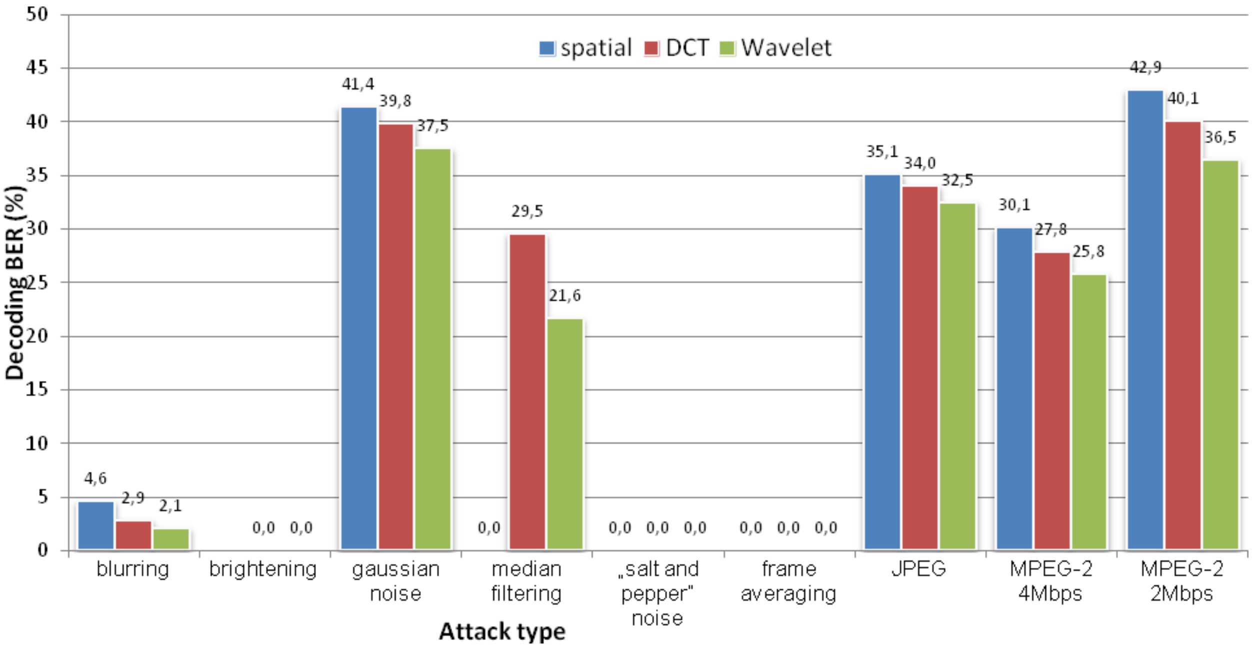


Fig. 14. Comparison of the decoding BER (%) for the proposed methods using $q = 2$, $k = 9$ and no error correction code

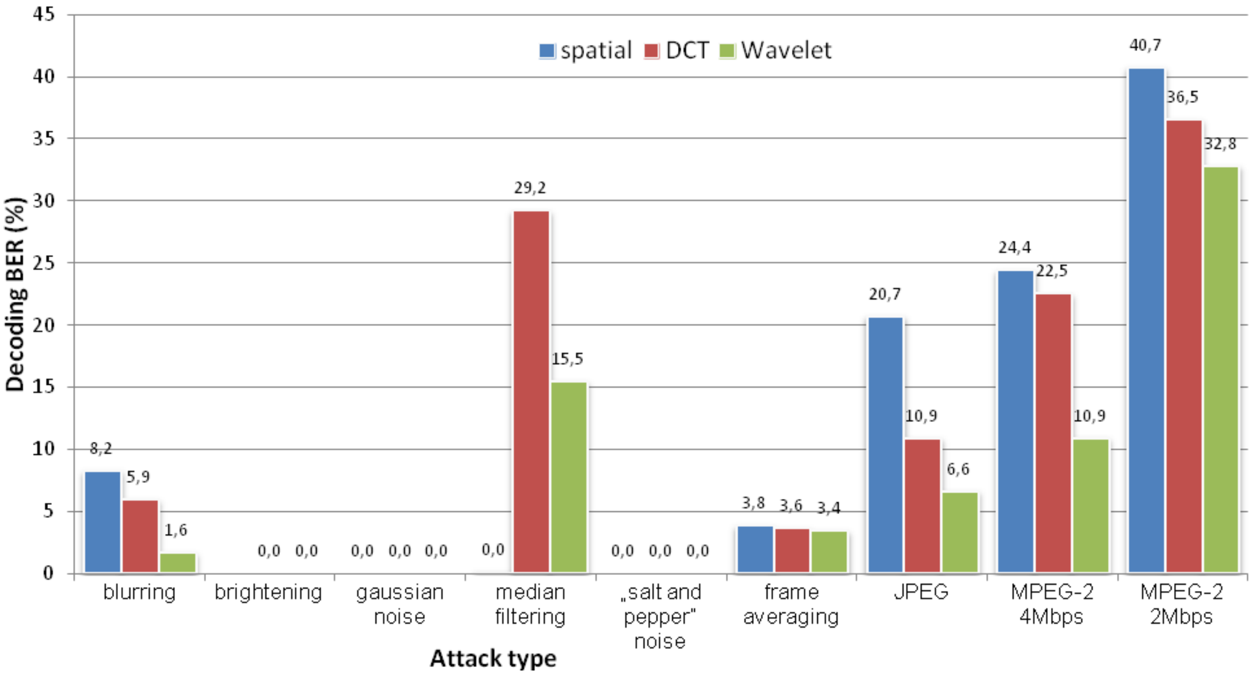


Fig. 15. Comparison of the decoding BER (%) for the proposed methods using $q = 4$, no redundant frame embedding and the Hamming (7,4) error correction code

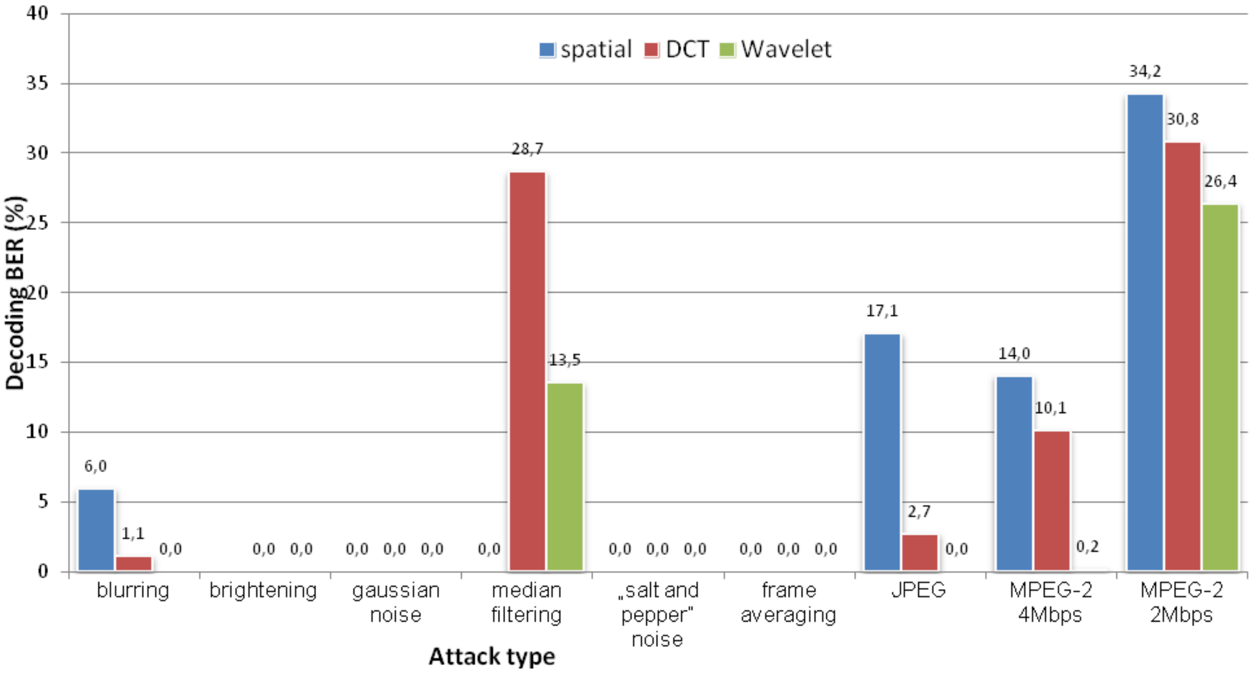


Fig. 16. Comparison of the decoding BER (%) for the proposed methods using $q = 4$, $k = 3$ and the Hamming (7,4) error correction code

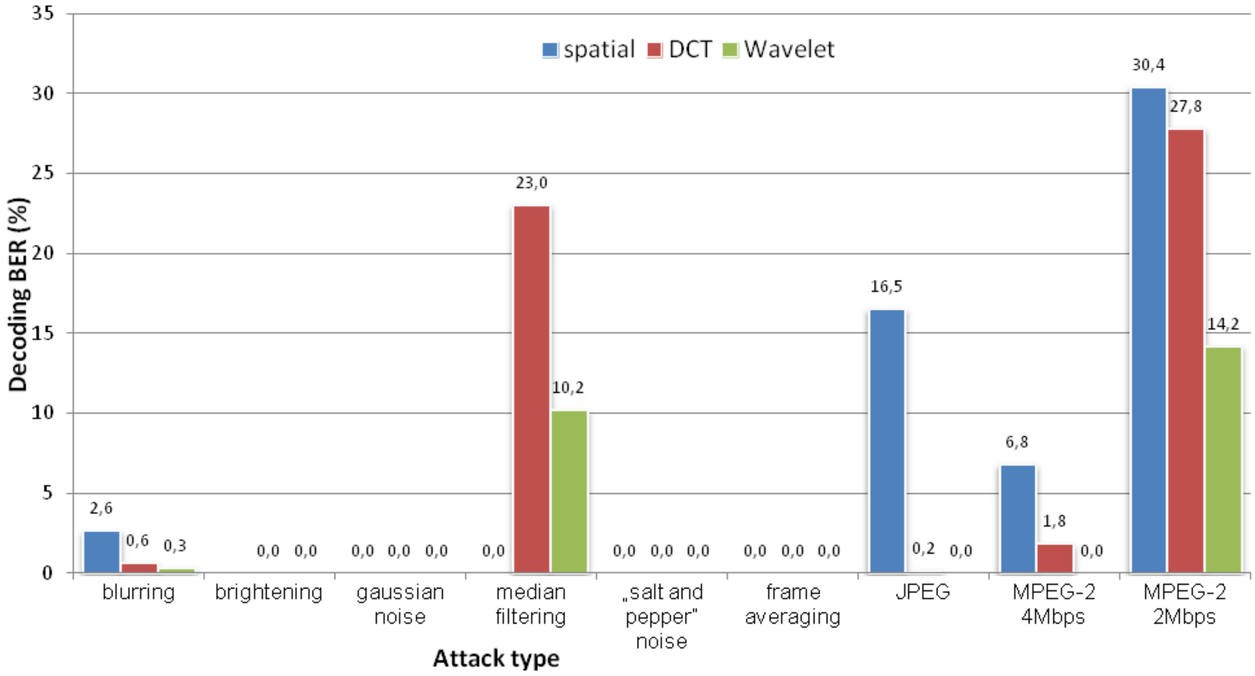


Fig. 17. Comparison of the decoding BER (%) for the proposed methods using $q = 4$, $k = 9$ and the Hamming (7,4) error correction code

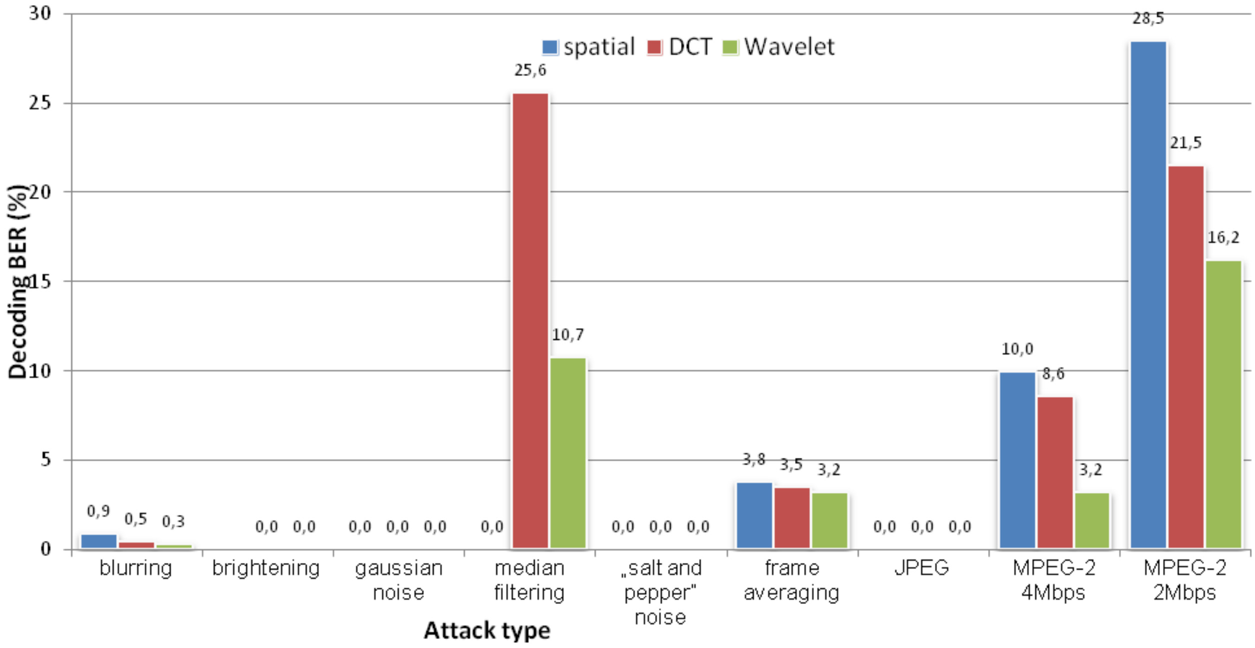


Fig. 18. Comparison of the decoding BER (%) for the proposed methods using $q = 8$, no redundant frame embedding and the Hamming (7,4) error correction code

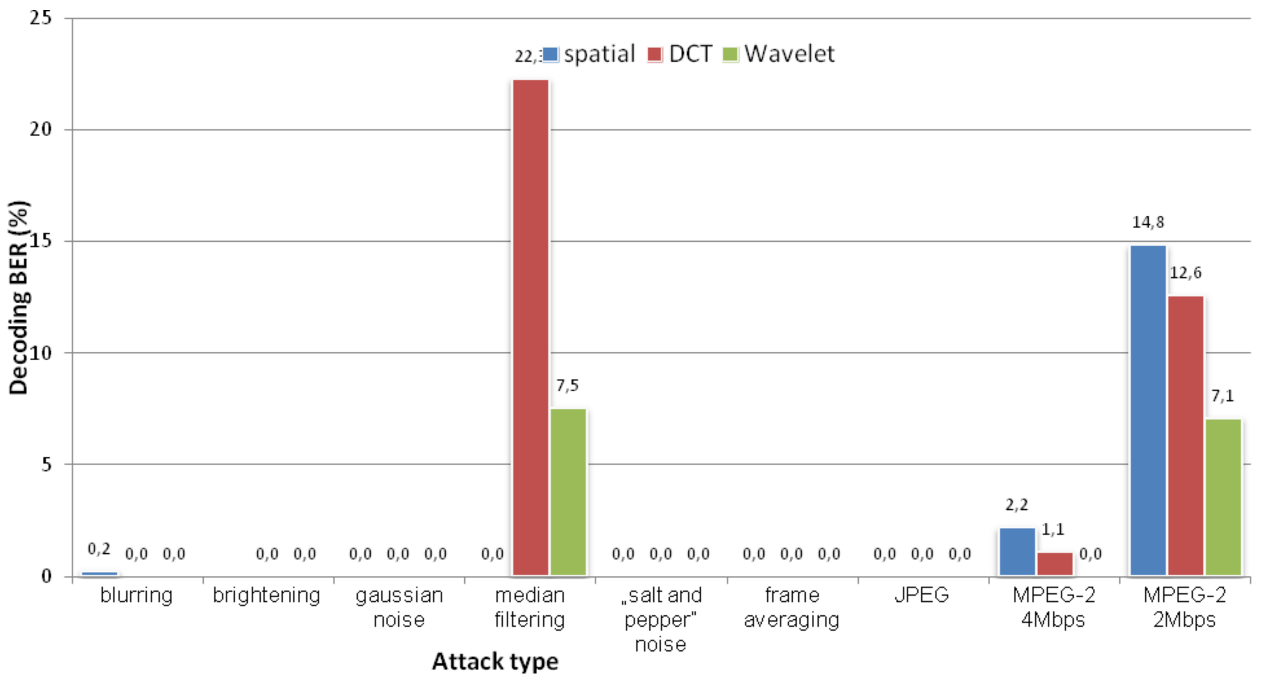


Fig. 19. Comparison of the decoding BER (%) for the proposed methods using $q = 8$, $k = 3$ and the Hamming (7,4) error correction code

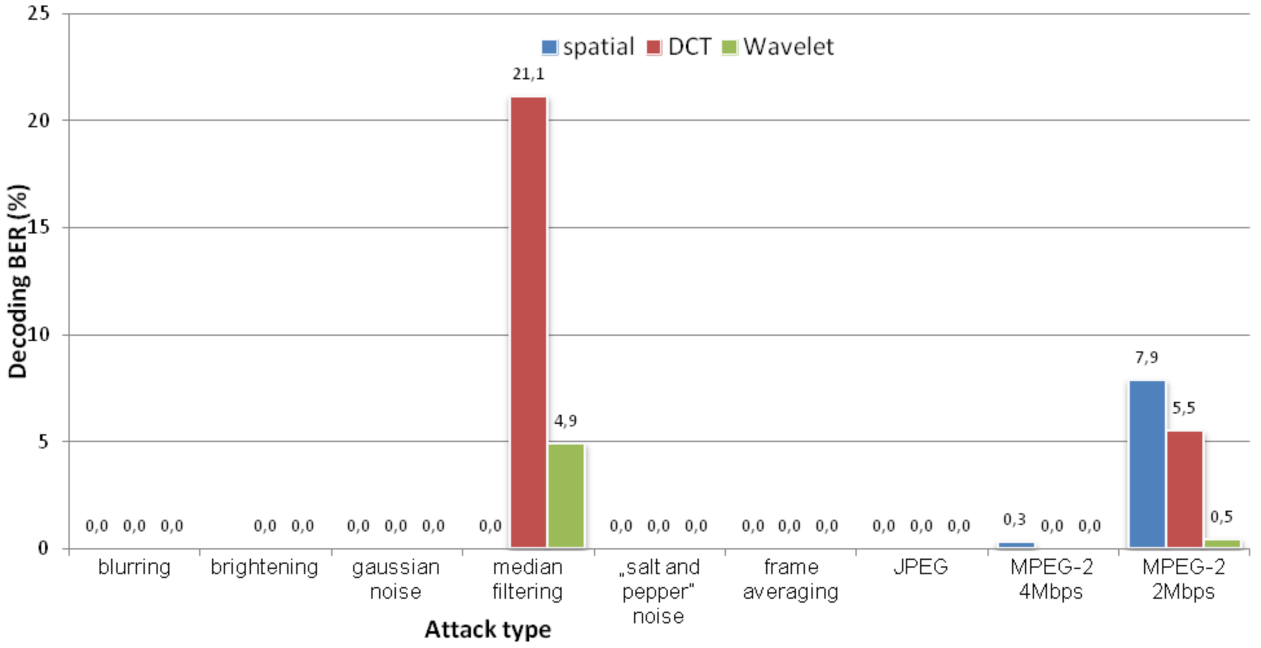


Fig. 20. Comparison of the decoding BER (%) for the proposed methods using $q = 8$, $k = 9$ and the Hamming (7,4) error correction code

Method	Original watermark	Blurr	Brighten	Gaussian noise	Median filtering
spatial					
DCT					
Wavelet					

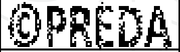
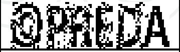
Method	Salt and pepper noise	Frame averaging	JPEG Q=60	MPEG-2 4 Mbps	MPEG-2 2 Mbps
spatial					
DCT					
Wavelet					

Table 3. Watermarks extracted from the watermarked “stefan” video after various attacks for $q = 4$, $k = 3$ and Hamming (7,4) error correction

Method	Original watermark	Blurr	Brighten	Gaussian noise	Median filtering
spatial					
DCT					
Wavelet					

Method	Salt and pepper noise	Frame averaging	JPEG Q=60	MPEG-2 4 Mbps	MPEG-2 2 Mbps
spatial					
DCT					
Wavelet					

Table 4. Watermarks extracted from the watermarked “stefan” video after various attacks for $q = 8$, $k = 3$ and Hamming (7,4) error correction

The best overall resilience is achieved by the method working in the wavelet domain, being the only technique with perfect decoding of the watermark for $q = 8$, $k = 9$ and Hamming (7,4) error correction. The second most resilient method is the DCT techniques, followed by the spatial technique.

Tables 3 and 4 contain the watermarks extracted after each attack from the video sequence “stefan”, using the three different approaches, *k*=3 redundant frames, Hamming (7,4) error correction code, $q = 4$ and $q = 8$, respectively. These tables show the advantage of using a binary image as watermark. We can see that the extracted watermarks can be identified easily for bit error rates below approximately 15%.

4. Conclusion

In this chapter we have compared three blind “spread quantization” video watermarking techniques in the spatial, DCT and wavelet domain. The original watermark and the original, unwatermarked videos are not required for the watermark extraction process. The methods are combinations of spread-spectrum and quantization based techniques. All three schemes embed the watermark in the luminance channel or in the transform coefficients of the luminance. The watermarks used are binary images, containing the copyright information. The watermark is protected against singular bit errors using a Hamming error correction code.

The spatial domain technique embeds a watermark bit by spreading it in a luminance block. The actual embedding into a luminance value is done using a quantization based approach.

The DCT domain technique spreads the same watermark bit into a number of 8x8 DCT blocks. In every DCT block only 22 middle frequency DCT coefficients are used for embedding. The wavelet based technique embeds the same watermark bit into a number of detail wavelet coefficients of the middle wavelet sub-bands.

The resilience of the schemes is improved by redundantly embedding the same watermark in a number of *k* video frames.

We have tested the perceptual quality of the watermarked videos and the resilience of the schemes to eight different attacks in the spatial, temporal and compressed domain, for different quantization step sizes and different number of redundant frames.

The experimental results show, that the wavelet domain technique achieves the highest video quality and the best robustness to most attacks, followed by the DCT and spatial domain techniques. The spatial domain method is most vulnerable to the brightening attack and the DCT method to the median filtering attack. The wavelet based technique achieves very good overall scores, being the best candidate for robust video watermarking.

Future research directions include the improvement of our wavelet based watermarking techniques in terms of robustness to the proposed attacks, but also to other temporal and geometric attacks. The quality of the watermarked videos could also be improved by using a Human Visual System (HVS) approach. These techniques are usually time consuming and a tradeoff has to be made between the perceptual quality of the watermarked videos and the arithmetical complexity of the scheme.

5. References

Altun, H. O.; Orsdemir, A.; Sharma, G.; Bocko, M. F. (February 2009). Optimal Spread Spectrum Watermark Embedding via a Multistep Feasibility Formulation, *IEEE Transactions on Image Processing*, vol. 18, no. 2, pp. 371-387

Barni, M.; Bartolini, F. & Piva, A. (2001). Improved wavelet-based watermarking through pixel-wise masking, *IEEE Transactions on Image Processing*, vol. 10, no. 5, pp. 783-791

Biswas, S.; Das, S.R. & Petriu, E.M. (2005). An adaptive compressed MPEG-2 video watermarking scheme, *IEEE Transactions on Instrumentation and Measurement*, vol. 54, no. 5, pp. 1853-1861

Celik, M.U.; Lemma, A.N., Katzenbeisser, S., van der Veen, M. (September 2008). Lookup-Table-Based Secure Client-Side Embedding for Spread-Spectrum Watermarks, *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 3, pp. 475-487

Chen, B. & Wornell, G. W. (May 2001). Quantization index modulation: A class of provably good methods for digital watermarking and information embedding, *IEEE Transactions on Information Theory*, vol. 47, no. 4, pp. 1423–1443

Coria, L.E.; Pickering, M.R., Nasiopoulos, P. & Ward, R.K. (September 2008). A Video Watermarking Scheme Based on the Dual-Tree Complex Wavelet Transform, *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 3, pp. 466-474

Costa, M. H. M. (May 1983). Writing on dirty paper, *IEEE Transactions on Information Theory*, vol. IT-29, no. 3, pp. 439–441

Cox, I. J.; Kilian, J., Leighton, F. T. & Shamoon, T. (December 1997). Secure spread spectrum watermarking for multimedia, *IEEE Transactions on Image Processing*, vol. 6, no. 12, pp. 1673–1687

Eggers, J. J.; Bauml, R., Tzschoppe, R. & Girod, B. (2003). Scalar Costa scheme for information embedding, *IEEE Transactions On Signal Processing*, vol. 51, no. 4, pp. 1003–1019

Ellinas, J. N. & Kenterlis, P. (2006). A Wavelet-Based Watermarking Method Exploiting the Contrast Sensitivity Function, *International Journal of Signal Processing*, vol. 3, no. 4, pp. 266-272

El-Taweel, G. S.; Onsi, H. M., Samy, M. & Darwish, M.G. (2007). Secure and Non-Blind Watermarking Scheme for Color Images Based on DWT, *GVIP Special Issue on Watermarking*, 2007

Gwenael, A. D. & Dugelay, J. L. (April 2003). A guide tour of video watermarking, *Signal Processing: Image Communications*, vol. 18, no. 4, pp. 263–282

Hartung, F. & Girod, B. (May 1998). Watermarking of uncompressed and compressed video, *Signal Processing*, vol. 66, no. 3, pp. 283–301.

Jie, N. & Zhiqiang, W. (June 2009). A new public watermarking algorithm for RGB color image based on Quantization Index Modulation, *International Conference on Information and Automation, ICIA '09*, pp.837-841

Kalantari, N.K.; Ahadi, S.M. (June 2010). A Logarithmic Quantization Index Modulation for Perceptually Better Data Hiding, *IEEE Transactions on Image Processing*, vol. 19, no. 6, pp. 1504-1517

Kinoshita, H. (September 1996). An image digital signature system with ZKIP for the graph isomorphism, *Proceedings of IEEE International Conference on Image Processing*, vol. 3, Lussane, Switzerland

Liu, L.; Li, R. & Gao, Q. (August 2005). A robust video watermarking scheme based on DCT, *Proceeding of the IEEE International Conference on Machine Learning and Cybernetics*, vol. 8, pp. 5176-5180

Liu, Z.; Liang, H., Niu, X. et al. (2004). A Robust Video Watermarking in Motion Vectors, *7th International Conference on Signal Processing*, vol. 3, pp. 2358-2361

Maity, S. P. & Maity, S. (April 2009). Multistage Spread Spectrum Watermark Detection Technique Using Fuzzy Logic, *IEEE Signal Processing Letters*, vol. 16, no. 4, pp. 245-248

Matsumoto, M. & Nishimura, T., (1998). Mersenne Twister: A 623-Dimensionally Equidistributed Uniform Pseudorandom Number Generator, *ACM Transactions on Modeling and Computer Simulation*, vol. 8, no. 1, pp. 3-30

Preda, R. O. & Vizireanu, N. (2007). Blind Watermarking Capacity Analysis of MPEG2 Coded Video, *8th International Conference on Telecommunications in Modern Satellite,* *Cable and Broadcasting Services, IEEE TELSIKS 2007*, Nis, Serbia and Montenegro, pp. 465-468

Preda, R. O. & Vizireanu, D. N. (2011). Robust wavelet-based video watermarking scheme for copyright protection using the human visual system, *Journal of Electronic Imaging*, vol. 20, no. 1, 013022, DOI: 10.1117/1.3558734

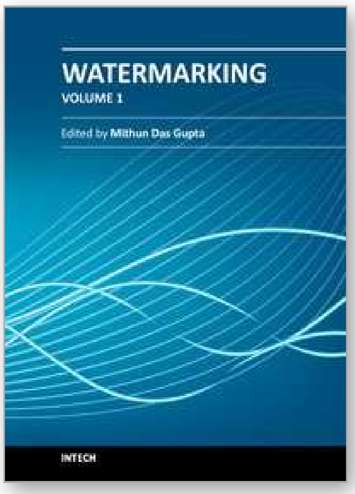
Reddy, A. A. & Chatterji, B. N. (2005). A new wavelet based logo-watermarking scheme, *Pattern Recognition Letters*, vol. 26, no. 7, pp. 1019-1027

Suhail, M.A. & Obaidat, M.S. (October 2003). Digital Watermarking-Based DCT and JPEG Model, *IEEE Transactions on Instrumentation & Measurement*, vol. 52, no. 5, pp. 1640-1647

Yang, C.; Huang, H. & Hsu, W. (July 2008). An adaptive video watermarking technique based on DCT domain, *8th IEEE International Conference on Computer and Information Technology, CIT 2008*, pp. 589-594

Zhang, J.; Ho, A., Qiu, G. & Marziliano, P. (February 2007). Robust video watermarking of H.264/AVC, *IEEE Transactions on Circuits and System-II: Express Briefs*, vol. 54, pp. 205–209

Zou, D.; Shi, Y.Q., Ni, Z. & Su, W. (October 2006). A Semi-Fragile Lossless Digital Watermarking Scheme Based on Integer Wavelet Transform, *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 16, no. 10, pp. 1294-1300



Watermarking - Volume 1

Edited by Dr. Mithun Das Gupta

ISBN 978-953-51-0618-0
Hard cover, 204 pages
Publisher InTech
Published online 16, May, 2012
Published in print edition May, 2012

This collection of books brings some of the latest developments in the field of watermarking. Researchers from varied background and expertise propose a remarkable collection of chapters to render this work an important piece of scientific research. The chapters deal with a gamut of fields where watermarking can be used to encode copyright information. The work also presents a wide array of algorithms ranging from intelligent bit replacement to more traditional methods like ICA. The current work is split into two books. Book one is more traditional in its approach dealing mostly with image watermarking applications. Book two deals with audio watermarking and describes an array of chapters on performance analysis of algorithms.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Radu Ovidiu Preda and Nicolae Vizireanu (2012). Comparison of "Spread-Quantization" Video Watermarking Techniques for Copyright Protection in the Spatial and Transform Domain, Watermarking - Volume 1, Dr. Mithun Das Gupta (Ed.), ISBN: 978-953-51-0618-0, InTech, Available from: http://www.intechopen.com/books/watermarking-volume-1/comparison-of-spread-quantization-video-watermarking-techniques-for-copyright-protection-in-the-spat

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821