Kundur Hatzinakos Digital Watermarking-I

[1]R.DIVIJA,
[1]Assisstant Professor
[1]Computer science Engineering
[1]Vaagdevi college of Engineering, Warangal,India

Abstract : Digital watermarking is used to hide the information inside a signal, which can not be easily extracted by the third party. Its widely used application is copyright protection of digital information. It is different from the encryption in the sense that it allows the user to access, view and interpret the signal but protect the ownership of the content. One of the current research areas is to protect digital watermark inside the information so that ownership of the information cannot be claimed by third party. With a lot of information available on various search engines, to protect the ownership of information is a crucial area of research. In latest years, several digital watermarking techniques are presented based on discrete cosine transform (DCT), discrete wavelets transform (DWT) and discrete fourier transforms (DFT). In this paper, we propose an algorithm for digital image watermarking technique based on singular value decomposition; both of the L and U components are explored for watermarking algorithm. This technique refers to the watermark embedding algorithm and watermark extracting algorithm. The experimental results prove that the quality of the watermarked image is excellent and there is strong resistant against many geometrical attacks

IndexTerms **-discrete cosine transform (DCT), discrete wavelets transform (DWT) and discrete fourier transforms (DFT).**

INTRODUCTION

The Kundur-Hatzinakos (KH) watermarking algorithm is a technique used primarily for embedding digital watermarks into digital media, particularly images. Developed by Deepa Kundur and Dimitrios Hatzinakos, this algorithm focuses on imperceptibly embedding watermarks to ensure robustness against common image processing operations while maintaining relative invisibility to the human eye.

The key aspects of the KH algorithm involve:

Robustness :The watermark should persist even after common image manipulations like compression, resizing, or noise addition.

Perpetual Transparency :The watermark should ideally remain invisible or imperceptible to human observers. This means that it should not significantly degrade the visual quality of the image.

Security: The algorithm should be designed in a way that prevents or at least makes it difficult for unauthorized parties to remove or tamper with the watermark without affecting the image's integrity

The exact workings of the KH algorithm might involve different mathematical transforms, such as the use of discrete wavelet transforms or other frequency-based methods, to embed the watermark information into the image.

However, specific details of the algorithm's implementation might not be publicly available due to proprietary reasons or ongoing research in the field of digital watermarking.

The algorithm's success relies on achieving a delicate balance between imperceptibility and robustness against attacks aimed at removing or altering the embedded watermark. It's often used in applications where copyright protection, authentication, or ownership verification of digital images is crucial.

APPLICATION OF DISCRETE WAVELET TRANSFORM IN WATERMARKING

Proliferation of multimedia data on the Internet and the ease of copying this data have brought an interest for copyright protection(Cox et al., 2002). During transmission, data can be protected using encryption; however after decrypting it, it is no longer protected. As an alternative to encryption, watermarking has been proposed as a means of identifying the owner, by secretly embedding an imperceptible signal into the host signal (Cox, 2005) – see Fig. 1.
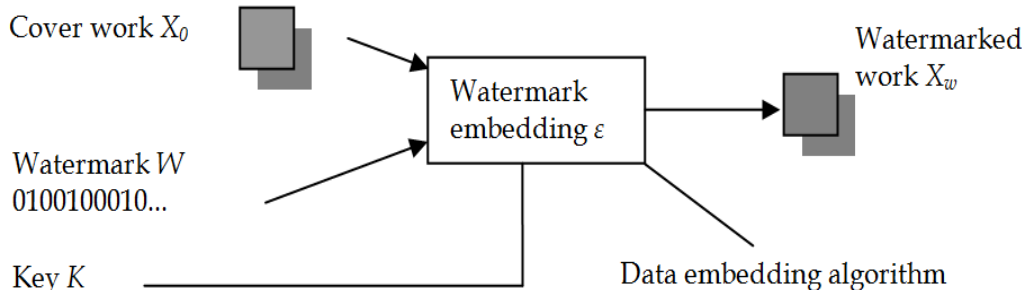

Cover work X_0

Watermark embedding ε

Watermarked work X_w

Watermark W
0100100010...

Key K

Data embedding algorithm

Figure 1.

Watermark embedding. The watermark is embedded using a secret or public key, making invisible changes to the cover work.

The main properties of a watermarking system are perceptual transparency, robustness, security, and data hiding capacity (Cox et al., 1997). Some of the terms used in watermarking are (Cox et al., 2002):

- The original data where the watermark is to be inserted is referred to as host or cover work.

- The hidden information is called payload.

- Visible watermarks are visual patterns (images, logos) inserted or overlaid on images/video. Visible watermarks are applied to photos publicly available on the web, to prevent commercial use of such images. One example of visible watermarking has been implemented by IBM for the Vatican library (Braudaway et al., 1996).

- Most watermarking systems involve making the watermark imperceptible.

- The key is required for embedding the watermark. If the same key is used for retrieving the watermark, the system is private, while if another key is used to retrieve it, the system is known as public.

- If the cover work is required at the detector, the system is informed (non-blind); if it's not required at the detector, the system is blind.

- Watermarking systems are robust or fragile. Robust watermarks should resist any modifications and are designed for copyright protection. Fragile watermarks are designed to fail whenever the cover work is modified and to give some measure of the tampering. Fragile watermarks are used in authentication.

Most of existing watermarking systems proposed in the literature can be classified depending on the watermarking domain, where the embedding takes place: spatial domain techniques (Nikolaidis & Pitas, 1998), where the pixels are directly modified, or transform domain techniques.

The majority of watermarking algorithms operate based on the spread spectrum (SS) communication principle. A pseudorandom sequence is added to the host signal in some critically sampled domain and the watermarked signal is obtained by inverse transforming the modified coefficients. Typical transform domains are the Discrete Wavelet Transform (DWT), the Discrete Cosine Transform (DCT) and the Discrete Fourier Transform (DFT). The DWT based algorithms usually produce watermarked images with the best balance between visual quality and robustness due to the absence of blocking artefacts (Nafornita, 2008).

Watermarks can be robust or fragile, depending on the application. For copyright protection, robustness is required. This can be assured with encoding of the watermark using a repetition code or an error correcting code. Robustness is increased with the increase of the correction capacity of the code. Despite of their efficient use in telecommunications, turbo codes have been rarely used in watermarking (Abdulaziz et al., 2002, Serdean et al., 2003, Balado & Perez-Gonzalez, 2001, Nafornita et al., 2009).

At the embedding side, the watermark can be added to coefficients of known robustness (large valued coefficients) or perceptually significant regions (Cox, 2005), such as contours and textures of an image. This can be done empirically, selecting larger coefficients (Cox et al., 1997) or using a thresholding scheme in the transform domain (Podilchuk & Zeng, 1998, Nafornita et al., 2005). Another approach is to insert the watermark in all coefficients of a transform, using a variable strength for each coefficient (Barni et al., 2001). Hybrid techniques, based on compression schemes, embed the watermark using a thresholding scheme and variable strength (Podilchuk & Zeng, 1998). The performance of such a system depends on the quality of the wavelet transform.

This chapter will focus on the application of the wavelet transforms in robust watermarking for static images. We will present the classical techniques of watermarking; starting with the spread spectrum DCT based watermarking system proposed by Cox et al. (Cox et al., 1997) and continuing with those proposed in the wavelet domain.

Other wavelet transforms as the Double Tree Complex Wavelet Transform (DTCWT) (Selesnick et al., 2005) or the Hyperanalytic Wavelet Transform (HWT) (Nafornita et al., 2008, Firoiu et al., 2009) could also be considered. The advantages of such transforms compared to DWT are: quasi-shift invariance and enhanced directional selectivity. The data hiding capacity increases with the increase of redundancy (4x for DTCWT and HWT). We will compare the efficiency of those wavelet transforms in watermarking.

2. Watermarking methods

Most techniques embed the watermark in a transform domain as mentioned before. Early techniques have used the Discrete Cosine Transform. One of the most influential watermarking works is a spread spectrum approach proposed in (Cox et al., 1997). They argue that the watermark be placed explicitly in the perceptually most significant components of the data, and that the watermark be composed of random numbers drawn from a Gaussian distribution $N(0,1)$, in order to make it invisible and robust to attacks:

$$v'(i)=v(i)(1+\alpha w(i)) \quad E1$$

where $v(i)$ is the DCT coefficient to be watermarked, $w(i)$ is the watermark bit, α is the embedding strength and $v'(i)$ is the watermarked coefficient. Detection is made using the similarity between the original W and extracted Ŵ watermarks:

$$sim(W,W^\wedge)=W^\wedge \cdot W / W^\wedge \cdot W^\wedge \quad E2$$

The fact that the transform is performed over the entire image increases the computation time. Other methods have been proposed that use the block-based DCT transform, just like in the JPEG compression (see for example Podilchuk & Zeng, 1998).

Other authors have proposed the use of the Discrete Fourier Transform or its variant – the Fourier-Mellin transform. This is useful in order to perform phase modulation between the watermark and the original signal (Ó Ruanaidh et al., 1996). The phase is more important than the amplitude; hence it will be difficult for an attacker to remove the watermark. Phase modulation often possesses superior noise immunity in comparison with amplitude modulation. Many watermarking techniques use DFT amplitude modulation because the watermark will be translation invariant. The DFT is more often used in its derived forms such as the Fourier-Mellin transform. This Fourier-Mellin transform approach has arisen out of the need for Rotation, Scale and Translation invariant (RST-invariant) watermarking techniques. It involves creating a Log Polar map of the DFT amplitudes of the image, where the embedding takes place. This method is said to be extremely RST invariant and uses a RST invariant watermark (Lin et al., 2001, Ó Ruanaidh & Pun, 1998).

3. Watermarking using wavelets

3.1. Discrete wavelet transform methods

There are different approaches to embed the watermark in the wavelet domain. Almost all methods rely on masking in some way the watermark, either by selecting a few coefficients, or using adaptive embedding strength.

Podilchuk & Zeng, 1998 propose an image-adaptive (IA) approach. They use the just difference noticeable difference (JND) to determine the image dependent perceptual mask for the watermark. They applied this method in both DCT and wavelet domain:

$$I^*u,v=\{Iu,v+JNDu,v\times wu,v,ifIu,v>JNDu,v,vIu,v,otherwise \quad E3$$

Iu,v are the coefficients of the original image, wu,v are the watermark bits, and $JNDu,v$ are the JND values computed using visual models. In the case of DCT, they are computed using Watson's perceptual model; for the wavelet domain, the weight is computed for each frequency band based on typical viewing conditions. Detection is made using correlation between the image difference and the watermark sequence. This method is more robust than the spread-spectrum method by Cox et al., 1997. Although more robust than IA-DCT, the IA-W method does not take into account perceptual significant regions, so the watermark can be erased from perceptually insignificant coefficients. For example, low-pass filtering will affect the watermark inserted in high frequency components.

Xia et al., 1998 propose a watermarking algorithm using the Haar mother wavelet, and two levels of decomposition. A pseudo-random sequence is added to the highest coefficients not located in the lowest resolution:

$$f'(m,n)=f(m,n)+\alpha \cdot f(m,n)\beta wi \quad E4$$

where α is the watermark strength, and β is the amplification for large coefficients. This algorithm concentrates most of the energy in edges and textures, which are the coefficients in detail subbands. This increases the invisibility of the watermark, because human observers are less sensitive to change in edges and textures compared to changes in smooth areas of an image. More watermarks are inserted in each subband, and detection is done hierarchically, for each resolution level, using intercorrelation between original watermark and the difference of the two images. The method is robust to a series of distortions, but low-pass and median filtering affect the watermark.

Kundur & Hatzinakos, 1998 use the Daubechies wavelet family to compute the DWT on three levels of decomposition. The watermarking algorithm selects in a pseudo-random manner the embedding locations from the detail subbands. The authors state that the spread-spectrum technique is not appropriate for transmitting the watermark because the correlator used for watermark detection is not effective in the presence of fading. Hence, they use quantization for embedding the watermark bits. To increase robustness, they use a reference watermark in order to estimate if the watermark bit has been embedded (Kundur & Hatzinakos, 2001).

One of the popular methods is the one proposed by Barni et al., 2001. The watermark is masked according to the characteristics of the human visual system (HVS), taking into account the texture and the luminance content of all the image subbands. For coefficients corresponding to contours of the image a higher strength is used, for textures a medium strength is used and for regions with high regularity a lower strength is used, in accordance with the analogy water-filling and watermarking (Kundur, 2000).

The image I, of size $2M\times 2N$, is decomposed into 4 levels using Daubechies-6 wavelet mother, where $Il\theta$ is the subband from level $l\in\{0, 1, 2, 3\}$, and orientation $\theta\in\{0, 1, 2, 3\}$ (horizontal, diagonal and vertical detail subbands, and approximation subband). A pseudorandom binary (± 1) sequence is casted into 2D binary watermarks, each of size $MN/4^l$, $xl\theta$. The watermark is embedded in all coefficients from level l=0 by addition

$$Ĩl\theta(i,j)=Il\theta(i,j)+\alpha wl\theta(i,j)xl\theta(i,j) \quad E5$$

where α is the embedding strength and $wl\theta(i,j)$ is half of the quantization step:

$$ql\theta(i,j)=\Theta(l,\theta)\Lambda(l,i,j)\Xi(l,i,j)0.2 \quad E6$$
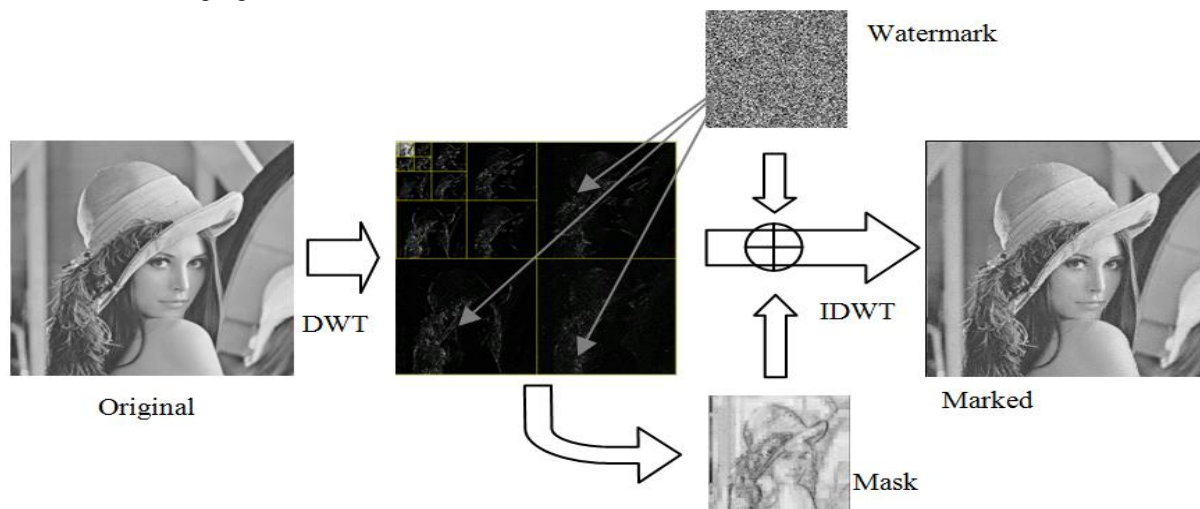
as it is presented in the following figure.

Figure 2.
Watermark embedding in the wavelet domain (Barni et al., 2001). The watermark is embedded in the first resolution level using a perceptual mask.

This is a product of three factors: sensitivity to noise, local brightness and texture activity around a pixel. They are computed as follows:

$$\Theta(l,\theta)=\{2,\theta=11otherwise\}\cdot\{1.00l=00.32l=10.16l=20.10l=3\} \quad E7$$

$$\Lambda(l,i,j)=1+L'(l,i,j) \quad E8$$

$$L(l,i,j)=I33(1+\lfloor i/2^{3-l}\rfloor,1+\lfloor j/2^{3-l}\rfloor)/256 \quad E9$$

$$\Xi(l,i,j)=\sum k=03−116−k\sum\theta=02\sum x,y=01[Ik+l\theta(y+i/2k,x+j/2k)]2\cdot Var\{I33(1+y+i/2^{3-l},1+x+j/2^{3-l})\}x=0,1y=0,1 \quad E10$$

The texture activity around a pixel is composed by the product of two contributions; the first is the local mean square value of the DWT coefficients in all detail subbands and the second is the local variance of the 4th level approximation image. Both are computed in a small

2×2 neighborhood corresponding to the location (i, j) of the pixel. The first contribution is the distance from the edges, and the second one is the texture. This local variance estimation is computed with a low resolution.

Detection is made using the correlation between the marked DWT coefficients and the watermarking sequence to be tested for presence (the original image is not needed):

$$\rho(l)=4l\sum_{\theta=0}^{2}\sum_{i=0}^{M/2l-1}\sum_{j=0}^{N/2l-1}\tilde{I}^{l}\theta(i,j)x^{l}\theta(i,j)/(3MN) \quad E11$$

The correlation is compared to a threshold $T_{\rho}(l)$, computed to grant a given probability of false positive detection, using the Neyman-Pearson criterion. For example, for $Pf\leq10^{-8}$, the threshold is $T\rho(l)=3.972\sigma\rho(l)2$, with $\sigma_{\rho(l)}^{2}$ the variance of the wavelet coefficients, if the image was watermarked with a code Y other than X,

$$\sigma\rho(l)2\approx(4l/(3MN))2\sum_{\theta=0}^{2}\sum_{i=0}^{M/2l-1}\sum_{j=0}^{N/2l-1}(\tilde{I}^{l}\theta(i,j))2. \quad E12$$

Barni's method is quite robust against common signal processing techniques like filtering, compression, cropping and so on. However, because embedding is made only in the last resolution level, the watermark information can be easily erased by an attacker. Nafornita, 2008 proposed a pixel-wise mask allowing insertion of the watermark in lower resolution levels. The third factor of the texture is estimated using the local standard deviation of the original image computed on a rectangular moving window $W(i,j)$ of $W_S \times W_S$ pixels, centered on each pixel $I(i,j)$. This criterion of segmentation finds its contours, textures and regions with high homogeneity. The local mean is:

$$\mu^{\wedge}(i,j)=WS-2\sum I(m,n)\in W(i,j)I(m,n) \quad E13$$

The local variance is given by:

$$\sigma^{\wedge}2(i,j)=WS-2\sum I(m,n)\in W(i,j)(I(m,n)-\mu^{\wedge}(i,j))2 \quad E14$$

The local standard deviation is the square root of this local variance. The texture for a considered DWT coefficient is proportional with the local standard deviation of the corresponding pixel from the host image. We denote this local standard deviation image with S, and the local mean image with U. Embedding is made in the subband s, level l; the size of the texture matrix must agree with the size of the subband. Hence, the approximation image at the lth decomposition level is used. This compression can be realized exploiting the separation properties of the DWT. To generate the mask required for the embedding into the detail sub images corresponding to the lth decomposition level, the DWT of the local standard deviation image is computed (making l+1 iterations). The required mask will be the approximation subimage from level l, denoted S_{l}^{3}, normalized to the local mean, also compressed in the wavelet domain, U_{l}^{3}. This is illustrated in Fig. 3. One difference between the watermarking method proposed by Nafornita, 2008 and the one proposed by Barni et al., 2001, is given by the computation of the local variance – the second term – in (10). To obtain the new values of the texture, the local variance of the image to be watermarked is computed, using the relations (13) and (14). The local standard deviation image is decomposed using one iteration wavelet transform, and only the approximation image is kept. Relation (10) is then replaced with:

$$\Xi(l,i,j)=\sum_{k=0}^{3}-116-k\sum_{\theta=0}^{2}\sum_{x,y=0}^{1}[I_{k+l}\theta(y+i/2k,x+j/2k)]2\cdot S_{l}3(i,j)/U_{l}3(i,j) \quad E15$$
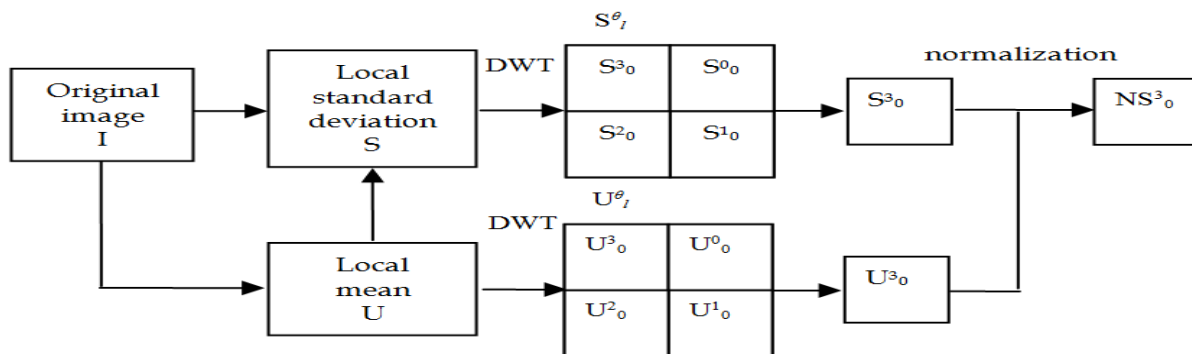

Figure 3.

Watermark embedding. The watermark is embedded using a secret or public key, making invisible changes to the cover work.

The second difference is that the luminance mask is computed on the approximation image from level l, where the watermark is embedded. The DWT of the original image using l decomposition levels was computed and the approximation subimage corresponding at level l was separated, obtaining the image $I_{l}3$. The luminance content is computed using:

$$L(l,i,j)=I_{l}3(i,j)/256 \quad E16$$

Since both factors are more dependent on the resolution level in the method proposed by Barni, the noise sensitivity function becomes:

$$\Theta(l,\theta)=\{2,\theta=11,\text{otherwise}\}\{1.00l\in\{0,1\}0.66l=2\} \quad E17$$

.

It was considered the ratio between the correlation $\rho(l)$ in Eq. (11) and the image dependent threshold $T_{\rho}(l)$, hence the detector was viewed as a nonlinear function with a fixed threshold. In Nafornita, 2007a, three detectors are used, to take advantage of the wavelet hierarchical decomposition. The watermark presence is detected,

from all resolution levels, "all_levels", separately from each resolution level, considering the maximum detector response from each level, "max_level", separately from each subband, considering the maximum detector response from each subband, "max_subband".

Evaluating the correlations separately per resolution level or subband can be sometimes advantageous. In the case of cropping, the watermark will be damaged more likely in the lower frequency than in the higher frequency, while lowpass filtering affects more the higher frequency than lower ones. Layers or subbands with lower detector response are discarded. This type of embedding combined with new detectors is more attack resilient to a possible erasure of the three subbands watermark. The detector "all_levels" evaluates the watermark's presence on all resolution levels:

$$d1=\rho d1/Td1 \quad E18$$

where the correlation $\rho d1$ is given by:

$$\rho d1=\sum_{l=0}^{2}\sum_{\theta=0}^{2}\sum_{i=0}^{M/2l-1}\sum_{j=0}^{N/2l-1}\tilde{I}^{l}\theta(i,j)x^{l}\theta(i,j)/(3MN\sum_{l=0}^{2}4-l) \quad E19$$

The threshold for $P_{f}\leq10^{-8}$ is $Td1=3.97\sigma\rho d12$, with:

$$\sigma\rho d12\approx\sum_{l=0}^{2}\sum_{\theta=0}^{2}\sum_{i=0}^{M/2l-1}\sum_{j=0}^{N/2l-1}(\tilde{I}^{l}\theta(i,j))2/(3MN\sum_{l=0}^{2}4-l)2 \quad E20$$

The second detector "max_levels" considers the responses from different levels, as $d(l)=\rho(l)/T(l)$, with $l\in\{0, 1, 2\}$, and discards the detector responses with lower values:

$d_2 = \max_l \{d(l)\}$ E21

The third detector considers the responses from different subbands and levels, as $d(l,\theta)$ the ratio $\rho(l,\theta)/T(l,\theta)$, with $l,\theta \in \{0, 1, 2\}$, and discards the detector responses with lower values,

$d_3 = \max_{l,\theta}\{d(l,\theta)\}$ E22

The correlation and threshold are computed with the same rationale on one subband, indicated by its orientation and level.

3.2. Complex wavelet transform methods

The discrete wavelet transform is useful to embed the watermark because the visual quality of the images is very good. However, it has three main disadvantages (Kingsbury, 2001): lack of shift invariance, lack of symmetry of the mother wavelets and poor directional selectivity. Caused by the lack of shift invariance of the DWT, small shifts in the input signal can produce important changes in the energy distribution of the wavelet coefficients. Due to the poor directional selectivity for diagonal features of the DWT the watermarking capacity is small. The most important parameters of a watermarking system are robustness and capacity. These parameters must be maximized. These disadvantages can be diminished using a complex wavelet transform (Kingsbury, 2000, 2001).

A very simple implementation of the Hyperanalytic Wavelet Transform, (HWT), recently proposed (Adam et al., 2007) has a high shift-invariance degree versus other quasi-shift-invariant wavelet transforms (WT) at same redundancy. It has also an enhanced directional selectivity. All the WTs have two parameters: the mother wavelets (MW) and the primary resolution (PR), (number of iterations). The importance of their selection is highlighted in Nason, 2002. Another appealing particularity of those transforms, coming from their multiresolution capability, is the interscale dependency of the wavelet coefficients.

We present in the next paragraphs a new implementation of HWT (Adam et al., 2007) and its application to watermarking (Nafornita et al., 2008). The watermark capacity was studied in Moulin & Mihcak, 2002, where an information-theoretic model for image watermarking and data hiding is presented. Models for geometric attacks and distortion measures that are invariant to such attacks are also considered. The lack of shift invariance of the DWT and its poor directional selectivity are reasons to embed the watermark in the field of another WT. To maximize the robustness and the capacity, the role of the redundancy of the transform used must be highlighted first. An example of redundant WT is represented by the tight frame decomposition. In Hua & Fowler, 2002 are analyzed the watermarking systems based on tight frame decompositions. The analysis indicates that a tight frame offers no inherent performance advantage over an orthonormal transform (DWT) in the watermark detection process despite the well known ability of redundant transforms to accommodate greater amounts of added noise for a given distortion. The overcompleteness of the expansion, which aids the watermark insertion by accommodating greater watermark energy for a given distortion, actually hinders the correlation operator in watermark detection. As a result, the tight-frame expansion does not inherently offer greater spread-spectrum watermarking performance. This analytical observation should be tempered with the fact that spread-spectrum watermarking is often deployed in conjunction with an image-adaptive weighting mask to take into account the human visual model (HVM) and to improve perceptual performance. Another redundant WT, the DTCWT, was already used for watermarking (Loo & Kingsbury, 2000). The authors of this paper prove that the capacity of a watermarking system based on a complex wavelet transform is higher than the capacity of a similar system that embeds the watermark in the DWT domain. Many authors (e.g. Daugman, 1980) have suggested that the processing of visual data inside our visual cortex resembles filtering by an array of Gabor filters of different orientations and scales. The proposed implementation of HWT is efficient, has only a modest amount of redundancy, provides approximate shift invariance, has better directional selectivity than the 2D DWT and it can be observed that the corresponding basis functions closely approximate the Gabor functions. So, the spread spectrum watermarking based on the use of an image adaptive weighting mask applied in the HWT domain is potentially a robust solution that increases the capacity.

3.2.1. A new implementation of the Hyperanalytic Wavelet Transform

The hypercomplex mother wavelet associated to a real mother wavelet $\psi(x,y)$ is:

$\psi_a(x,y) = \psi(x,y) + i\mathcal{H}_x\{\psi(x,y)\} + j\mathcal{H}_y\{\psi(x,y)\} + k\mathcal{H}_x\{\mathcal{H}_y\{\psi(x,y)\}\}$ E23

where $i^2 = j^2 = -k^2 = -1$, and $ij = ji = k$ (Davenport, 2008). The HWT of the image $f(x,y)$ is:

$HWT\{f(x,y)\} = \langle f(x,y), \psi_a(x,y) \rangle.$ E24

The 2D-HWT of the image $f(x,y)$ can be computed using the 2D-DWT of its associated hypercomplex image:

$HWT\{f(x,y)\} = DWT\{f(x,y)\} + iDWT\{\mathcal{H}_x\{f(x,y)\}\} + jDWT\{\mathcal{H}_y\{f(x,y)\}\} + kDWT\{\mathcal{H}_y\{\mathcal{H}_x\{f(x,y)\}\}\} = \langle f_a(x,y), \psi(x,y) \rangle = DWT\{f_a(x,y)\}.$ E25

HWT uses four trees, each implemented by 2D-DWT, being adequate to a multi-wavelet environment (Firoiu et al., 2009). H_x is the Hilbert transform computed across lines and H_y across columns (Fig. 4). The HWT coefficients are organized in two sequences of complex coefficients separated by the sign of their preferential orientation, with 6 subbands, 3 of positive orientations and 3 of negative orientations $\pm\text{atan}(1/2)$, $\pm\pi/4$ and $\pm\text{atan}(2)$:

$z_\pm = z_{\pm r} + jz_{\pm i} = (Df_{1,2,3} \mp D\mathcal{H}_y\{\mathcal{H}_x\{f\}\}_{1,2,3}) + j(D\mathcal{H}_x_{1,2,3} \pm D\mathcal{H}_y_{1,2,3}).$ E26
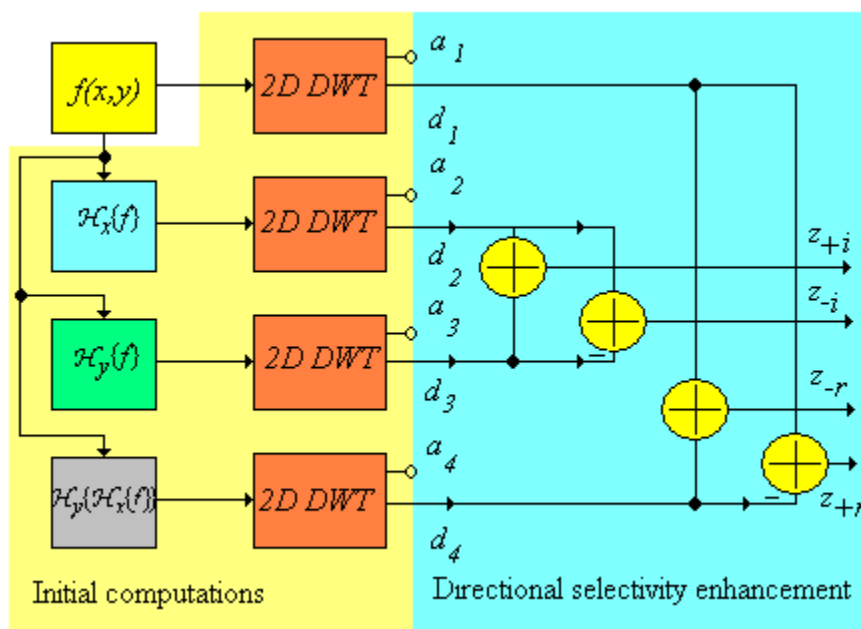
Figure 4.

The new HWT implementation architecture.

3.2.2. Watermarking using the Hyperanalytic Wavelet Transform

Adapting the strategy already described in the previous paragraph to the case of HWT, a new method was proposed in Nafornita et al., 2008. The first three wavelet decomposition levels are used and the watermark is embedded into the real coefficients with positive and negative orientations, $z+r$ and $z-r$, respectively. In this case the relations already described in the previous paragraph were used independently for each of these two images. The same message was embedded in both images, using the mask from Nafornita, 2007a. The difference is that the orientations or preferential directions are in this case: $\text{atan}(1/2)$, $\pi/4$, $\text{atan}(2)$ (respectively for $\theta = 0, 1, 2$), for the image $z+r$ and $-\text{atan}(1/2)$, $-\pi/4$, $-\text{atan}(2)$, ($\theta=0, 1, 2$) for the image $z-r$. At the detection side, we consider the pair of images ($z+r, z-r$), thus having twice as much coefficients than the standard approach, and θ takes all the possible values, $\pm\text{atan}(1/2)$, $\pm\pi/4$, $\pm\text{atan}(2)$.

3.3. Results and comparisons

We will compare in the following watermarking systems based on DWT with the ones based on complex WTs, namely the HWT.

3.3.1. Results for methods based on the discrete wavelet transform

In Nafornita et al., 2006a, the system proposed by Barni et al. was modified, using the texture mask in (15). The image Barbara is watermarked with various values of the embedding strength α. The binary watermark is embedded in all the detail wavelet coefficients of the first resolution level. Watermarked Barbara for $\alpha=1.5$ is shown in Fig. 5.

Figure 5.
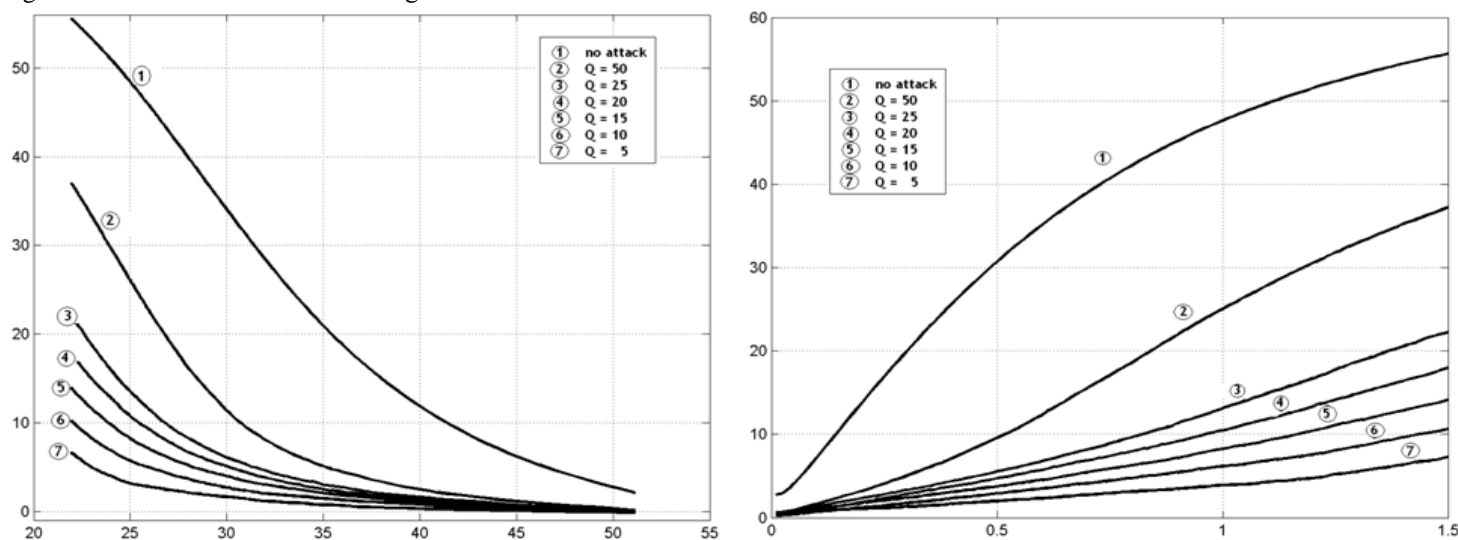Original and watermarked Barbara images with α = 1.5.

Figure 6.
Left: The ratio ρ/T as a function of the PSNR between the marked and the original images, for different quality factors, JPEG compression. Right: Ratio ρ/T as a function of embedding strength, for different quality factors, JPEG compression. P_f is set to 10^{-8}.

Fig. 6 shows results for JPEG compression, for different quality factors: the ratio ρ/T is plotted as a function of the peak signal-to-noise ratio (PSNR) between the marked (un-attacked) image and the original one, and respectively as a function of α. The probability of false positive detection is set to 10^{-8}. If this ratio is greater than 1 then the watermark is positively detected. Generally, for a PSNR higher than 30 dB, the original image and watermarked one are considered indistinguishable. For compression quality factors higher or equal than 25 the distortion introduced by JPEG compression is tolerable. For PSNR in the range of 30-35 dB, of practical interest, the watermark is detected for all significant compression quality factors. Increasing the embedding strength, the PSNR of the watermarked image decreases, and the ratio ρ/T increases. The watermark is still detectable even for very small values of α. For the quality factor Q=5 (or a compression ratio CR=32), the watermark is still detectable even for α=0.5. Fig. 7 shows the detection of a true watermark for various quality factors, in the case of α=1.5; the threshold is well below the detector response. In Table 1 we give a comparison between the two methods, for the Lena image, α=1.5 in the case of JPEG compression with a quality factor of 5 (compression ratio of 46).
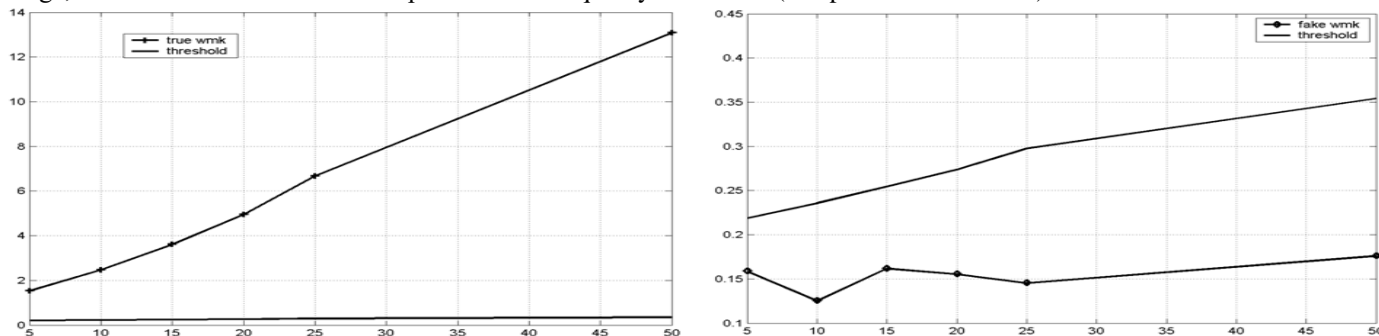

Figure 7.
Left: Detector response ρ, threshold T, as a function of different quality factors (JPEG compression). The watermark is successfully detected. P_f is set to 10^{-8}. Right: Highest detector response, $ρ_2$, corresponding to a fake watermark and threshold T. The threshold is above the detector response.

	Nafornita et al., 2006a	Barni et al., 2001
	0.3199	0.038
T	0.0844	0.036
2	0.0516	0.010

Table 1.

A comparison for JPEG compression with a compression ratio CR = 46.

The detector response for the original embedded watermark ρ, the detection threshold T, and the second highest detector response ρ_2 are given. P_f was set to 10^{-8} and 1000 marks were tested. The detector response is higher than in Barni's case.

Figure 8.

Original image Lena; mask from Nafornita et al., 2006b and Barni's mask for level l=0. The masks are the complementary of the real ones.

In Nafornita et al., 2006b, Barni's method is modified, using the texture mask in (15), as well as the luminance factor in (16). The masks obtained are shown in Fig. 8. The improvement is clearly visible around edges and contours. The method is applied in two cases, when the watermark is inserted in level 0 only and when it's inserted in level 1 only. JPEG compression is again considered. The image Lena is watermarked at level l=0 and respectively at level l=1 with α ranging from 1.5 to 5. The binary watermark is embedded in all the detail wavelet coefficients of the resolution level, l as previously described. For α=1.5, the watermarked images, in level 0 and level 1, as well as the image watermarked using Barni's mask, are shown in Fig. 9. Obviously the quality of the watermarked images are preserved using the new pixel-wise mask. The PSNR values are 38 dB (level 0) and 43 dB (level 1), compared to Barni's method, with a PSNR of 20 dB.

Figure 9.

Watermarked images, α =1.5, for Nafornita et al., 2006b, level 0 (PSNR = 38 dB); level 1 (43 dB); for Barni et al., 2001, level 0 (20 dB).
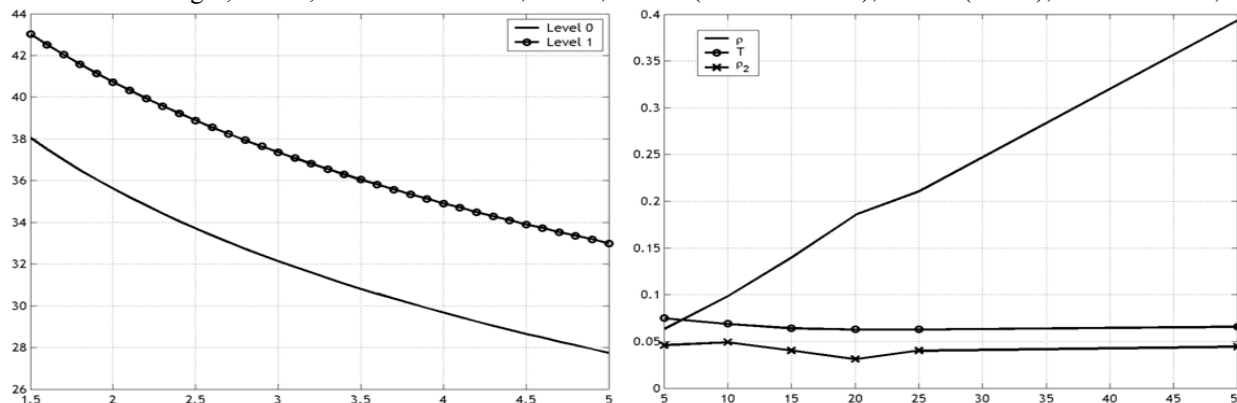

Figure 10.

Left: PSNR as a function of α. Embedding is made either in level 0 or in level 1.Right: Detector response ρ, threshold T, highest detector response, ρ_2, corresponding to a fake watermark, as a function of different quality factors (JPEG compression). The watermark is successfully detected. P_f is set to 10^{-8}. Embedding was made in level 0.

PSNR values are shown in Fig. 10(left) as a function of the embedding strength. The watermark is still invisible, even for high values of α. Fig. 11 gives the results for JPEG compression. In all experiments, the probability of false positive detection is set to 10^{-8}. The watermark is successfully detected for a large interval of compression quality factors. For PSNR values higher than 30 dB, the watermarking is invisible. For quality factors Q≥10, the distortion introduced by JPEG compression is tolerable. For all values of α, the watermark is detected for all the significant quality factors (Q≥10). Increasing the embedding strength, the PSNR of the watermarked image decreases, and ρ/T increases. For the quality factor Q = 10 (or a compression ratio CR = 32), the watermark is still detectable even for low values of α.

Fig. 10(right) shows the detection of a true watermark from level 0 for various quality factors, for α=1.5; the threshold is below the detector response. The selectivity of the watermark detector is also illustrated, when a number of 999 fake watermarks were tested: the second highest detector response is shown, for each quality factor. False positives are rejected.

In Table 2 a comparison between Nafornita et al., 2006b and Barni et al., 2001, can be seen for JPEG compression with Q=10 (compression ratio of 32). The detector response for the original watermark ρ, the detection threshold T, and the second highest detector response $ρ_2$, when the watermark was inserted in level 0 are given. The detector response is higher than for Barni et al.
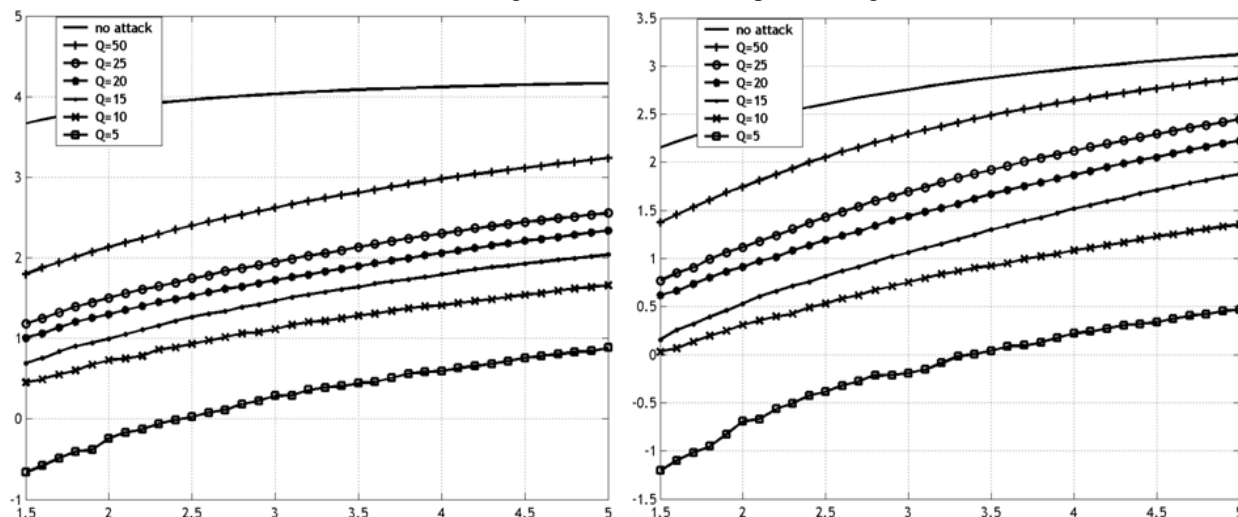

Figure 11.

Ratio ρ/T as a function of the embedding strength α. The watermarked image is JPEG compressed with different quality factors Q. P_f is set to 10^{-8}. Embedding was made in level 0 (left), and in level 1 (right).

	Nafornita et al., 2006b	Barni et al., 2001
ρ	0.0750	0.062
T	0.0636	0.036
$ρ_2$	0.0461	0.011

Table 2.

A comparison for JPEG compression with a compression ratio CR = 32. The method in Nafornita, 2007a allows embedding of the watermark in all resolution levels, except the last one (low resolution). Three types of detectors are used, as described in paragraph 3.1. Various images of size 512x512, have been watermarked at levels l∈{0, 1, 2} using the new mask. The embedding strength is α=1.5. Based on human observation and the peak-signal-to-noise ratio, PSNR, the images are indistinguishable from the original ones. For Barni et al. method, a watermark is embedded in all the detail wavelet coefficients of the first resolution level, l=0, for α=0.2, that results in a similar image quality (see Fig.12). This has been concluded in Nafornita, 2007b, where by limiting the watermark strength such that the PSNR is 35 dB and in average the percentage of affected pixels is less than 25%, the quality of the images is greatly improved. Girod's model has been used for determining the location and number of affected pixels (Girod, 1989). For instance, in Barni's case, the watermarked image with α=0.2 has a PSNR of 36.39 dB, 11.84% affected pixels, compared to the one watermarked with α=1.5 has a PSNR of 20 dB, and all pixels are affected. What is kept constant for comparison are the 2D watermarks embedded in the first level, and the image quality. The method Nafornita, 2007a cannot be compared with the one in Barni et al., 2001 when the watermark is embedded in all resolution levels, simply because their mask isn't suited for embedding in other levels than the highest resolution level. Results for some of the standard images from the USC SIPI Image Database are given.

Figure 12.

left) Original image Lena, (middle) Watermarked images for Nafornita, 2007a, α=1.5, PSNR=36.86 dB, (right) Barni et al., 2001, α=0.2, PSNR=36.39 dB.

Table 3 includes PSNR values for the two cases. For the first detector, an estimate of the false positive probability is shown for the image Lena, before and after JPEG compression attack, with quality factor Q=10, as a function of the detection thresholds, $T_{\rho1}$. The threshold values have been computed using as estimate the variance of the ρ_1 obtained from experiments.

The mean PSNR for the twelve images is 34.16 dB for the proposed method (Nafornita, 2007a) and 34.06 dB for Barni's method.

Detector response vs. attack	Nafornita, 2007a			Barni's method
	1-All levels	2-Max level	3-Max subband	
JPEG compression, Q=10	2.38	1.98	1.44	1.75
Median filtering, M=5	1.32	1.12	1.46	0.25
Scaling, 50%	4.06	5.21	5.76	1.85
Cropping, 512x512 -"/> 32x32	0.68	0.98	1.73	1.48
Gamma correction, =2	20.32	29.19	28.06	32.54
Motion blur, L=31, θ=11	1.98	5.48	8.04	6.14

Table 3.

Resistance to different attacks, for Nafornita, 2007a method. The detector response is a mean value of different responses.Tests were made for JPEG compression, median filtering, cropping, resizing, gamma correction and blurring. Table 3 shows the mean values of the detector responses for each attack. A particular attack parameter is chosen where the watermark is still detectable by at least one detector. For compression, the method in Nafornita, 2007a successfully detects the watermark at Q=10. The 1st detector is better in all cases. This new method has better results than Barni's technique. The watermark of both methods survived in all images for median filtering with kernel sizes up to 3. For kernel size 5, the watermark of Nafornita, 2007a using the first and third detector is detectable; Barni's method fails to detect the watermark. In the case of scaling to 50%, the watermark was successfully detectable in both cases, with better results for Nafornita, 2007a. The third detector has the best performance in detecting the mark. The watermark of Nafornita, 2007a was successfully detected in the cropped image of 32x32, only with the third detector, which proves its efficiency. Barni's method detects the watermark with similar detector responses as in the case of the third detector. As expected for normalized correlation detection, both methods are practically insensitive to gamma correction adjustment. For the motion blur attack, both methods have successfully detected the watermark in all cases. Detector 3 has slightly better results than the others.
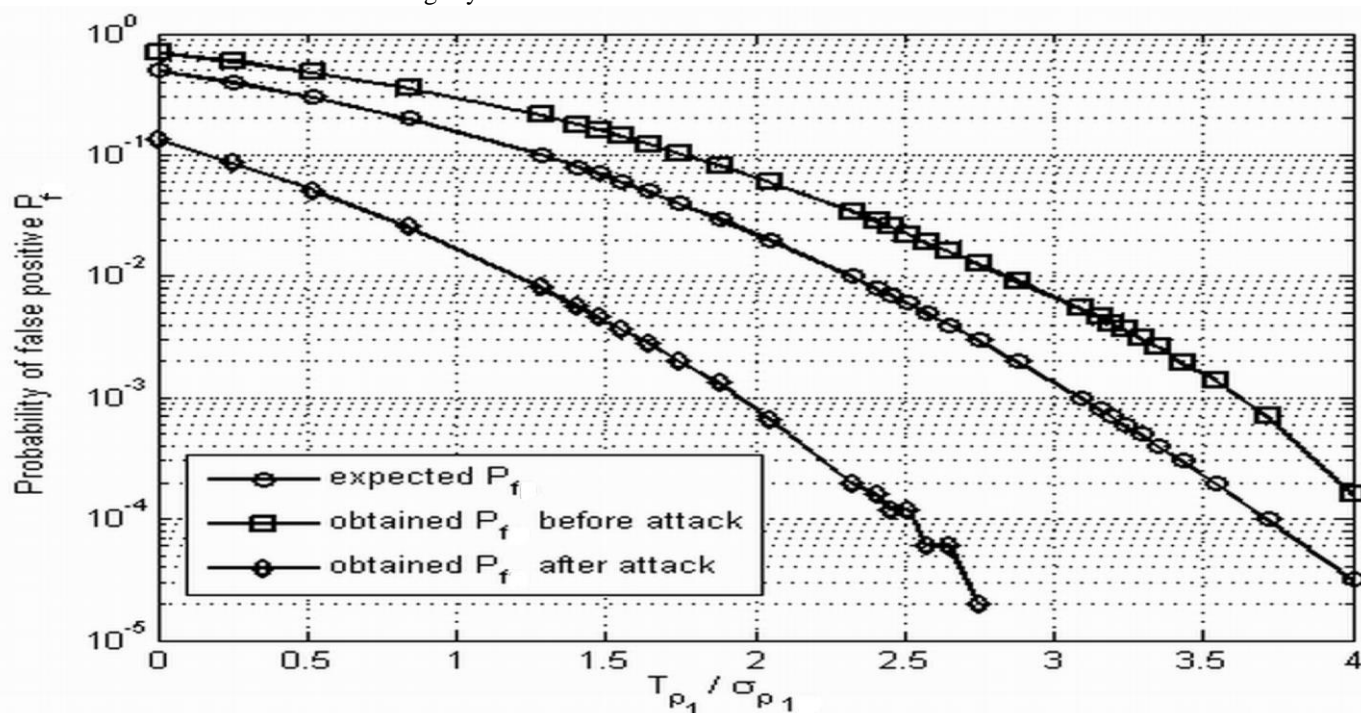

Figure 13.

Experimentally evaluated probability of false positive P_f vs. $T_{\rho1}/\sigma_{\rho1}$, the ratio between the detection threshold and standard deviation of the correlations in the case where an incorrect watermark was embedded. The theoretical trend is also shown ('o' marker). Tests were made on Lena, before and after JPEG compression with quality factor 10, using 5×10^4 different watermarks.

For the first detector, the probability of false positive was estimated by searching many different watermarks into one watermarked image, Lena. Each threshold $T_{\rho1}$ was set in such a way to grant a given value of P_f. The trial was repeated for values of P_f ranging from 10^{-1} through 10^{-4}. In total $5x10^4$ watermarks per image have been tested. The estimation has been done before any type of manipulation and after JPEG compression, with quality factor 10. The estimated P_f is plotted in Fig. 13 versus the ratio $T_{\rho1}/\sigma_{\rho1}$ between the detection thresholds and standard deviations of correlations for the case corresponding to certain estimates of this probability of false positive. This case corresponds to the situation where the image is watermarked with a code Y other than X.

Surprisingly, the estimated false alarm P_f, is lower in the case of compression than in the case of no attack, for the same detection threshold. This can be explained by the fact that before compression, the empirical pdf of the correlations in the case for an incorrect watermark is embedded, was not Gaussian. Although the two empirical pdf's are closer after the attack, they are still very good separated and the empirical pdf for an incorrect watermark has the mean below zero, compared to the equivalent one before – which is centered on zero. Thus

setting a particular threshold can indeed result in a lower false alarm after attack. Similar results were obtained for Barbara, and for the same attack.

For the first detector, the obtained probability of false positive is close to the expected one. The assumption that the wavelet coefficients from different levels and subbands are i.i.d. is thus reasonable and the detector has a good performance.

3.3.2. Results for methods based on the Hyperanalytic Wavelet transform

In Nafornita et al., 2008 the watermark is embedded in the HWT domain, in all levels (0, 1 and 2) and all orientations (positive and negative). The test image is Lena, of size 512x512. For $\alpha=1.5$, the watermarked image has a PSNR of 35.63 dB. The original image, the corresponding watermarked image and the difference image are presented in Fig. 14.
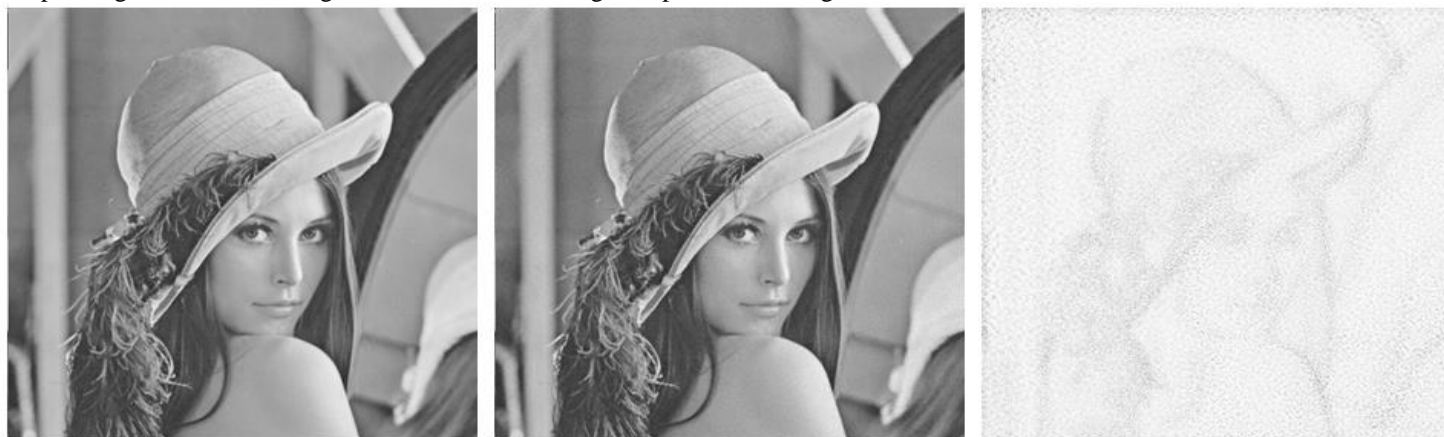

Figure 14.

Original and watermarked images with method (Nafornita et al., 2008), for $\alpha=1.5$, PSNR=35.63 dB; Difference image, amplified 8 times.

The watermarked images have been exposed at some common attacks: JPEG compression with different quality factors (Q), shifting, median filtering with different window sizes M, resizing with different scale factors, cropping with different areas remaining, gamma correction with different values of γ, blurring with a specified point spread function (PSF) and perturbation with AWGN with different variances.

Resistance to unintentional attacks, for watermarked image Lena, can be compared to the results obtained using the watermarking methods in Barni et al., 2001 and Nafornita, 2007a analyzing Table 4. For the method in Nafornita, 2007a, the same watermark strength, 1.5 is used and the watermark is embedded in all three wavelet decomposition levels, resulting in a PSNR of 36.86 dB. For the method in Barni et al., 2001, the watermark strength 0.2 is used and the embedding is made only in the first resolution level, resulting in a similar quality of the images (PSNR=36.39 dB).

Attacks vs. detector response	DWT-Nafornita, 2007a			DWT-Barni et al., 2001	HWT-Nafornita et al., 2008		
	all levels	max level	max subband		all levels	max level	max subband
Before attack	21.57	39.12	33.60	**44.31**	24.78	43.18	26.30
JPEG, Q=50	5.45	6.76	5.02	6.22	6.25	**7.87**	4.85
JPEG, Q=25	3.02	3.67	2.60	3.03	3.23	**4.19**	2.62
JPEG, Q=20	2.55	3.08	2.09	2.38	2.72	**3.58**	2.33
Shift, *li*=128, *co*=128	21.57	39.12	33.59	**44.31**	24.78	43.18	26.30
Median filter, M=3	4.29	4.58	4.87	1.57	4.59	**5.42**	4.37
Median filter, M=5	**1.66**	1.24	2.27	0.59	1.61	1.64	1.49
Resizing, 0.75	9.53	15.86	15.64	14.09	10.93	**19.34**	14.67
Resizing, 0.50	4.21	5.72	5.75	2.31	4.56	6.14	**8.71**
Cropping, 256x256	7.40	12.14	17.10	**18.08**	8.68	15.20	13.82
Cropping, 128x128	3.11	4.66	**8.31**	8.01	3.53	6.04	6.86
Cropping, 64x64	1.10	1.72	**4.45**	3.92	1.32	2.47	3.71
Gamma correction, =1.5	22.18	39.76	33.74	43.04	25.31	**43.61**	26.45
Gamma correction, =2	22.59	39.70	32.98	42.43	25.62	**43.24**	25.88
Blur, L=31, β=11	2.69	7.81	**9.56**	9.05	3.05	9.18	7.55

Table 4.

Resistance to different attacks, for HWT based method compared to DWT based methods. Special attention was paid to the shifting attack. First the watermarked image was circularly shifted with *li* lines and *co* columns, obtained the attacked image(Ĩt). Supposing that the numbers *li* and *co* are known, the messages at level *l* are circularly shifted with $li/2^l$ lines and $co/2^l$ columns obtaining the new messages(xt)lθ. Next the watermark was detected using the image (Ĩt) and the messages(xt)lθ. The values obtained for *li*=128 and *co*=128 are presented in Table 4.

From the results, it is clear that embedding in the real parts of the HWT transform yields in a higher capacity at the same visual impact and robustness. In fact the results obtained in Nafornita et al., 2008 are slightly better than the results obtained with the DWT-based methods in Nafornita et al., 2008 and Barni et al., 2001 for JPEG compression, median filtering with window size M=3, resizing and gamma correction. For the other attacks the results obtained are similar with the results of the watermarking methods based on DWT. The case of the shifting attack is very interesting. In this case the robustness of the watermarking method is given by two properties: the shift invariance degree of the WT used and the masking ability. All the methods compared in Table 4 are very robust against the shifting attack. The values of the ratios between the correlations and the image dependent thresholds obtained before and after the shifting attack are equal for all the methods compared in Table 4. So, the ability of masking seems to be more important than the shift invariance degree of the WT used for the

conception of counter-measures against the shifting attack, when the numbers of lines and columns used for the attack are already known. Of course, the detection of these numbers must also be realized, for the implementation of a strategy against the shifting attack.

4. Conclusion

In a watermarking system, robustness evaluation should be made if invisibility criteria are satisfied. For this purpose, perceptual watermarks are being used to overcome the issue of robustness against invisibility. In the literature, there was proposed a blind spread spectrum technique that uses a perceptual mask in the wavelet domain, taking into account the noise sensitivity, texture and the luminance content of all image subbands. We described new techniques proposed by the authors, based on the modifications of this perceptual mask, in order to increase robustness, while still maintaining imperceptibility. Moreover, using the new mask, information is successfully hidden in the lower frequency levels, thus increasing the capacity and making the watermark more robust to common attacks that affect both high frequencies and low frequencies of the image. A good balance between robustness and invisibility of the watermark is achieved when embedding is made in all detail subbands for all resolution levels, except the coarsest level; this can be particularly useful against erasure of high frequency subbands containing the watermark in Barni's system.

A nonlinear detector with fixed threshold – as ratio between correlation and the image dependent ratio – has been used; three watermark detectors were proposed in Nafornita, 2007a that take advantage of the hierarchical wavelet decomposition: 1) from all resolution levels, 2) separately from each level, considering the maximum detector response for each level and 3) separately from each subband, considering the maximum detector response for each subband. This has been advantageous for cropping, scaling and median filtering where the 3rd detector shows improved performance. We tested our methods against different attacks, and found out that it is better than Barni's method. The behavior of our methods can be explained by the fact that we have used a better estimate of the mask and we took advantage of the diversity of the wavelet decomposition. The effectiveness of the new perceptual mask is appreciated by comparison with Barni's method. Simulation results show the superiority of the proposed methods (Nafornita et al., 2006a, b, Nafornita, 2007a).

The HWT is a very modern WT as it has been formalized only two years ago. A very simple implementation of this transform has been used, which permits the exploitation of the mathematical results and of the algorithms previously obtained in the evolution of wavelets theory. It does not require the construction of any special wavelet filter. It has a very flexible structure, as we can use any orthogonal or bi-orthogonal real mother wavelets for the computation of the HWT. The presented implementation leads to both a high degree of shift-invariance and to an enhanced directional selectivity in the 2D case. An ideal Hilbert transformer was considered. A new type of pixel-wise masking for robust image watermarking in the HWT domain has been presented (Nafornita et al., 2008). Modifications were made to two existing watermarking technique proposed in Barni et al., 2001 and Nafornita, 2007a, based on DWT. These techniques were selected for their good robustness against the usual attacks. The method is based on the method in Barni et al., 2001, with some modifications. The first modification is in computing the estimate of the variance, which gives a better measure of the texture activity. An improvement is also owed to the use of a better luminance mask. The third improvement is to embed the watermark in the detail coefficients at all resolutions, except the coarsest level, making the watermark more attack resilient. The HWT embedding exploits the coefficients $z+r$ and $z-r$.

The simulation results illustrate the effectiveness of the proposed algorithms. The methods were tested against different attacks (in terms of robustness). The HWT based watermarking method is similar and in some cases outperforms the DWT based methods, but it has a superior capacity than the DWT based methods.

As a future research direction, the statistical properties of the HWT will be used to improve the watermark detection.

References

1. AbdulazizN.GlassA.PangK. K.2002 Embedding Data in Images Using Turbo-Coding, 6th Symposium on DSP for Communication Systems, 2831Jan. 2002, Univ. of Wollongong, Australia.

2. AdamI.NafornitaC.BoucherJ.-M.IsarA.2007 A New Implementation of the Hyperanalytic Wavelet Transform, Proc. of IEEE Symposium ISSCS 2007, Iasi, Romania, '07401404

3. BaladoF.Perez-GonzalezF.2001 Coding at the Sample Level for Data Hiding: Turbo and Concatenated Codes, SPIE Security and Watermarking of Multimedia Contents, San Jose CA, 22-25 Jan. 2001, San Jose CA, USA, 20014314532543

4.BarniM.BartoliniF.PivaA.2001 Improved wavelet-based watermarking through pixel-wise masking, IEEE Trans. Image Processing, 10, 5, May 2001783791

5.BraudawayG. W.MagerleinK. A.MintzerF.1996 Protecting publicly available images with a visible watermark, Proc. SPIE- Int. Soc.Opt. Eng., 2659126133

6.CoxI.2005 Robust watermarking, ECRYPT Summer School on Multimedia Security, Salzburg, Austria, Sept. 22, 2005

7.CoxI.KillianJ.LeightonT.ShamoonT.1997 Secure Spread Spectrum Watermarking for Multimedia, IEEE Trans. Image Processing, 6, 12, 1997, 1673 EOF87 EOF

8.CoxI.MillerM.BloomJ.2002 Digital Watermarking, Morgan Kaufmann Publishers, 2002

9.DaugmanJ.1980 Two-dimensional spectral analysis of cortical receptive field profiles, Vision Res., 20, '80847856

10.DavenportC.2008 Commutative Hypercomplex Mathematics, Available from: http://home.comcast.net/~cmdaven/hyprcplx.htm.

11.FiroiuI.NafornitaC.BoucherJ.M.IsarA.2009 Image Denoising Using a New Implementation of the Hyperanalytic Wavelet Transform, IEEE Transactions on Instrumentation and Measurements, 588August 2009, 24102416

12.GirodB.1989 The information theoretical significance of spatial and temporal masking in video signals, Proc. SPIE Human Vision, Visual Processing, and Digital Display, 1077178187

13.HuaL.FowlerJ. E.2002 A Performance Analysis of Spread-Spectrum Watermarking Based on Redundant Transforms, Proc. IEEE Int. Conf. on Multimedia and Expo, Lausanne, Switzerland, '02, 2

14.KingsburyN.2001 Complex Wavelets for Shift Invariant Analysis and Filtering of Signals, Applied and Comp. Harm. Anal. 10, '01234253

15.KingsburyN.2000 A Dual-Tree Complex Wavelet Transform with improved orthogonality and symmetry properties, Proc. IEEE Conf. on Image Processing, Vancouver, '00, paper 1429.

16.KundurD.2000 Water-filling for Watermarking?, Proc. IEEE Int. Conf. On Multimedia and Expo, NY, 12871290Aug. 2000.

17.KundurD.HatzinakosD.1998 Digital Watermarking using Multiresolution Wavelet Decomposition, Proc. IEEE Int. Conf. On Acoustics, Speech and Signal Processing, Seattle, Washington, 529692972May 1998.

18. KundurD.HatzinakosD.2001 Diversity and Attack Characterization for Improved Robust Watermarking, IEEE Transactions on Signal Processing, 491023832396

19. LinC. Y.WuM.BloomJ. A.CoxI. J.MillerM. L.LuiY. M.2001 Rotation, Scale, and Translation Resilient Watermarking for Images, IEEE Trans. On Image Processing, 10, 5, May 2001

20. LooP.KingsburyN.2000 Digital Watermarking Using Complex Wavelets, ICIP 2000.

21. MoulinP.MihcakM. K.2002 A Framework for Evaluating the Data-Hiding Capacity of Image Sources, IEEE Trans. Image Processing, 11(9), '0210291042

22. NafornitaC.IsarA.BordaM.2005 Image Watermarking Based on the Discrete Wavelet Transform Statistical Characteristics, Proc. IEEE EUROCON 2005, Serbia & Montenegro, 943946

23. NafornitaC.2008 Contributions to Digital Watermarking of Still Images in the Wavelet Transform, Ph.D. thesis, Feb. 2008, Technical University of Cluj-Napoca, Romania.

24. NafornitaC.IsarA.KovaciM.2009 Increasing Watermarking Robustness using Turbo Codes, IEEE International Symposium on Intelligent Signal Processing WISP 2009, Budapest, Hungary, 2628August 2009.

25. NafornitaC.FiroiuI.BoucherJ.M.IsarA.2008 A New Watermarking Method Based on the Use of the Hyperanalytic Wavelet Transform, Proc. SPIE Europe: Photonics Europe, 7000Optical and Digital Image Processing 70000W, 70000W700001W-12, 978-0-81947-198-7Strasbourg, April, 2008.

26. NafornitaC.2007 A New Pixel-Wise Mask for Watermarking, Proc. of ACM Multimedia and Security Workshop, 2007, Dallas, TX, USA.

27. NafornitaC.IsarA.BordaM.2006 Pixel-wise masking for watermarking using local standard deviation and wavelet compression, Scientific Bulletin of the Politehnica Univ. of Timisoara, Trans. on Electronics and Communications, 51(65), 2, 1461511583-3380

28. NafornitaC.IsarA.BordaM.2006 Improved Pixel-Wise Masking for Image Watermarking, Multimedia Content Representation, Classification and Security, September 11-13, 2006, Istanbul, Turkey, Lecture Notes in Computer Science, Springer-Verlag, 2006, 9097

29. NafornitaC.2007 Robustness Evaluation of Perceptual Watermarks, IEEE Int. Symposium on Signal, Circuits and Systems ISSCS 20071213July 2007, Iasi, Romania.

30. NasonG. P.2002 Choice of wavelet smoothness, primary resolution and threshold in wavelet shrinkage, Statistics and Computing, 12, '02219227

31. NikolaidisN.PitasI.1998 Robust Image Watermarking in the Spatial Domain, Trans. Signal Processing, 663385403

32. Ó RuanaidhJ. J. K.PunT.1998 Rotation, Scale and Translation Invariant Spread Spectrum Digital Image Watermarking, Signal Processing, 66(1998), 303317

33. RuanaidhÓ.J. J. K.DowlingW. J.BolandF. M.1996 Phase watermarking of digital images, Proc. IEEE Int. Conf. Image Processing, 1996, 239242

34. PodilchukC.ZengW.1998 Image-Adaptive Watermarking Using Visual Models, IEEE Journal on Selected Areas in Communications, 16, 4, May 1998525539

35. SelesnickI. W.BaraniukR. G.KingsburyN.2005 The Dual-tree Complex Wavelet Transform- A Coherent Framework for Multiscale Signal and Image Processing, IEEE Signal Processing Magazine, 226123151November 2005.

36. SerdeanC. V.AmbrozeM. A.TomlinsonM.WadeJ. G.2003 DWT based high-capacity blind video watermarking, invariant to geometrical attacks, IEE Proc.-Vis. Image Signal Process., 150, 1, Feb. 2003.

37. XiaX.BonceletC. G.ArceG. R.1998 Wavelet Transform Based Watermark for Digital Images, Optics Express, 312497505