Joint Watermarking and Compression for Images in Transform Domain

Gamal Fahmy
Electrical Engineering Dept., Assiut University, Egypt,

Abstract: Image watermarking, authentication and encryption have gained an increased importance during the last decade. This is due to the widespread use of visual media over the Internet and in several digital media applications. Several watermarking techniques have been proposed, some in spatial domain, and more recently in the transform/frequency domain and have been reported to be robust against different attacks, namely compression. It is also well known the importance and effectiveness of compression techniques to store transmit and retrieve visual information. However, the creation or development of a joint watermarking and compression framework for images has yet to be explored, where watermarking and compression could be pursued jointly on a trade-off manner. In other words, watermarking embedding/extraction can be performed on compressed domain data, while compression parameters could be used as watermarking keys. The primary focus of this paper is to explore this novel/unique idea. We propose a joint watermarking and compression (JWC) technique in the transform domain. This transform domain is based on the Natural Preserve Transform and can be utilized to achieve a balance between watermarking and compression for visual information. Watermarking performance is evaluated blindly for different compressed domain data scenarios, while compression performance is analyzed for other watermarking cases. Extensive simulation results that demonstrate the efficiency of the proposed joint watermarking and compression technique are presented.

Keywords: Image Watermarking, Natural Preserve Transform, Image Compression; Hartley Transform

I. Introduction

The rapid growth of visual media based applications necessitates sophisticated compression techniques in order to store, transmit and retrieve audio-visual information. The recent MPEG 4 and JPEG 2000 standards address the need for content based coding and manipulation of visual media. With the widespread use of the Internet and the rapid and massive development of multimedia, there is an impending need for efficient and powerfully effective copyright protection techniques [1-3]. Digital watermarking schemes are typically classified into three categories. (1) Private watermarking which requires the prior knowledge of the original information and secret keys, at the receiver, (2) Semi-private or semi-blind watermarking where the watermark information and secret keys may be available at the receiver, and (3) public or blind watermarking where the receiver must only know the secret keys [4]. The robustness of private watermarking schemes is high to endure signal processing attacks. While private watermarking is suitable for high security applications such as financial or defense data, it is not feasible in real applications, such as DVD copy protection where the original information may not be available for watermark detection. On the other hand, semi-blind and blind watermarking schemes are more feasible in that situation [5], but they have lower robustness than the private watermarking schemes [6]. Hence, while private watermarking is mainly utilized for authentication and verification, blind or public watermarking is for copy protection applications. In general, the requirements of a watermarking system fall into three categories: robustness, visibility, and capacity [7]

A variety of image watermarking methods have been proposed mostly based on transform domain [7-9]. In spite of the successful performance of most watermarking techniques reported in the literature, they still suffer from being semi-fragile due to the energy concentration of their transform domains (DCT and Wavelets), which makes them discard much of the mid and high frequency watermarked data in compression [10-13]. Watermarking compressed domain data will obviate the need for it to be decompressed for watermark extraction, while compressing watermarks would store and transmit visual data efficiently. Hence, there is an impending need for sophisticated joint watermarking and compression techniques that could compress, protect and watermark data simultaneously. While compression aims at concentrating data in the least possible information, watermarking aims at distributing and hiding logos and parameters. Hence, compression and watermarking are inversely related and they have to be treated on a trade-off manner. The amount of extracted/retrieved watermarked data is affected by the compression degree of the host data, while the efficiency of compression is affected by the amount of data that needs to be embedded and extracted.

In this paper we propose a transform domain based technique for data watermarking that has been previously reported in [14], and [15]. This transform domain is based upon the Natural Preserve Transform (NPT) originally reported in [16]. We utilized this transform domain to present our main contribution in this paper, which is to develop a joint compression and watermarking system based on the NPT and wavelet domains for visual data. We try to achieve a framework/equation that includes both compression and watermarking jointly in our proposed system. The organization of this paper is as follows. Section 2 contains necessary mathematical background about the NPT based watermarking approach. Section 3 briefly explains the watermarking embedding and extraction process in the NPT domain. Section 4 shows the robustness of the watermarking technique against several attacks. Section 5 shows our proposed joint
watermarking and compression framework, analysis and results. Discussion is in section 6, followed by conclusions in section 7.

2. Mathematical Background for NPT based Watermarking

The NPT was first used as a new orthogonal transform that holds some unusual properties that can be used for encoding and reconstructing lost data from images. The NPT transform of an image \( S \) of size \( N \times N \) is given by:

\[
S_{tr} = \psi(\alpha)S\psi(\alpha)
\]

As \( \psi(\alpha) \) is the transformation kernel defined as in [17-18].

\[
\psi(\alpha) = \alpha I_N + (1 - \alpha) H_N
\]

\( I_N \) is \( N^th \) order identity matrix, \( 0 \leq \alpha \leq 1 \), and \( H_N \) is any orthogonal transform, like Hadamard, DCT, Hartley, etc. Throughout this paper, we use the 2-D Hartley transform, defined by

\[
H_N(k, j) = \frac{1}{\sqrt{N}} \left( \cos \left( \frac{2(k-1)\pi}{N} \right) + \sin \left( \frac{2(j-1)\pi}{N} \right) \right)
\]

We note here that the Hartley transform was utilized due to its circular symmetry performance, as it evenly distributes the energy of the original image in the 4 corners of the orthogonally projected transform image, Fig. 1(a). Hence the Hartley transform achieves a trade-off point between the energy concentration feature (which is crucial for any transform domain for compression purposes) and the even distribution and spreading feature (which is crucial for watermarking and data hiding applications).

After the transformation kernel \( \psi \) is calculated in eq. 2, it is multiplied by the input image as a separable 2-D kernel, eq.1. The value of \( \alpha \) in eq. 2, gives a balance between the original domain (that would be multiplied by the identity matrix) and the transform domain (that would be multiplied by the Hartley basis). Clearly, when \( \alpha = 1 \), the transformed image is the original image, whereas when \( \alpha = 0 \), it is its orthogonal projection (which is the Hartley transform as in this paper). Hence the NPT transform is capable of concentrating energy of the image while still preserving its original sample values on a trade-off basis. This makes the NPT transform domain image has both almost original pixel values (that can not be visually distinguished from the original image) and a capability feature of retrieving the logo watermark image from a small part of the transformed image (provided that this small part has enough energy concentration in it).

The original image can be retrieved from the transformed image \( S_{tr} \), using

\[
S = \psi^{-1}(\alpha)S_{tr}\psi^{-1}(\alpha)
\]

If \( H \) is symmetric, as in Hartley matrices, the matrix \( \psi^{-1}(\alpha) \) can be computed as follows:

\[
\psi^{-1}(\alpha) = \phi = \frac{1}{\alpha} \left[ I - \frac{1 - \alpha}{\alpha} H + \left( \frac{1 - \alpha}{\alpha} H \right)^2 - \left( \frac{1 - \alpha}{\alpha} H \right)^3 + \ldots \right]
\]

Fig. 1(b-c) shows the Lena image and its NPT transformed image. \( \alpha \) is adjusted to a value of 0.994, which yields a nominal PSNR of around 45 dB. The high similarity between the original and transformed images, suggests that NPT is very convenient for watermarking and data hiding.
3.1 Watermark Embedding

Let the host image \( S \), (size \( N \times N \)) be watermarked by a watermarking logo (image) \( w \), of size (\( m \times n \)). In the bottom embedding technique [14-15], the logo is embedded to \( S \) as the last \( r \) bottom lines. Hence, the logo matrix is reshaped to be a matrix \( w_1 \) (of size \( r \times N, r = \frac{mn}{N} \)). Then, the last \( r \) rows of \( S \) are replaced by the reshaped logo \( w_1 \), as in Fig. 1(d). This would yield a watermarked image \( S_{wm} \),

\[
S_{wm} = \begin{bmatrix} S_1 \\ w_1 \end{bmatrix}, \quad S_1 = S(1 : N - r,:) .
\]

Then the NPT of \( S_{wm} \) is obtained as:

\[
A_w = \psi(\alpha) S_{wm} \psi'(\alpha) = \begin{bmatrix} A_{0w} \\ z \end{bmatrix} \uparrow (N - r) \downarrow r \quad \leftarrow N \rightarrow
\]

This step in eq. 6, would register the watermark (distribute its energy) over the entire host image. In order to make the watermarking logo invisible, we replace the last \( r \) rows \( z \) of \( A_w \) with the last \( r \) of the original image \( S \), Fig 1(e).

\[
A_{wm} = \begin{bmatrix} A_{0w} \\ S(N - r + 1 : N,:) \end{bmatrix}
\]

3.2 Watermark Extraction

The watermarking extraction process is divided into a non-blind case, and a blind case. In the non blind case the original host image is known at the receiver side and we only try to extract the logo from the watermarked image. In the blind case the host image is not known at the receiver side, and we try to extract both the host and logo images from the watermark image, \( A_{wm} \).

3.2.1 The Non Blind Case

Assuming that the original image \( S \), the parameter \( \alpha \) of eq. 1 and the type of the orthogonal transformation \( H_N \), are known at the receiver, the extraction of the watermark from the received \( A_{wm} \) proceeds as follows:
1. Since the size of the watermark \( m \times n \) is known at the receiver side, as well as the number of rows of \( w \). Form

\[
Y = A_{wm} \phi = \begin{bmatrix} Y_1 \\ Y_2 \end{bmatrix} = \psi S_{wm} = \psi \begin{bmatrix} S_1 \\ w_1 \end{bmatrix}.
\]

(8)

2. Partition

\[
\psi = \begin{bmatrix} \psi_{11} & \psi_{12} \\ \psi_{21} & \psi_{22} \end{bmatrix} \uparrow (N - r) \updownarrow r \]

(9)

Then, as long as \( N - r \geq r \), the watermark \( w \) is the least squares solution of the system

\[
Y_1 - \psi_{11} S_1 = \psi_{12} w_1
\]

(10)

The quality of extraction is judged by computing the normalized correlation \( NCORR \) between the original and extracted logo, i.e.

\[
NCORR = \frac{\sum_{i=1}^{m} \sum_{j=1}^{n} w_{ij} w_{exij}}{\| w \| \| w_{ex} \|}.
\]

\( w_{ex} \) is the extracted watermark. The non-blind extracted logo, in our experiments achieved a \( NCORR = 1 \) performance factor.

### 3.2.2 The Quasi Blind Case

When the prior knowledge of the host image \( S \) is not available, the following quasi blind technique is proposed for watermarking extraction of an NPT-based watermarked image. The proposed technique can be described as follows:

1. Partition

\[
\psi = \begin{bmatrix} \psi_{11} & \psi_{12} \\ \psi_{21} & \psi_{22} \end{bmatrix} \uparrow (N - r) \updownarrow r
\]

(12)

As \( A_{wm} \phi = \psi S_{wm} \) from eq. (6, 7, and 8), we can show that

\[
\begin{bmatrix} A_{0w} \\ S(N - r + 1 : N,:) \end{bmatrix} \phi = \begin{bmatrix} \psi_{11} & \psi_{12} \\ \psi_{21} & \psi_{22} \end{bmatrix} \begin{bmatrix} S_1 \\ w_1 \end{bmatrix}
\]

i.e. \( A_{0w} \phi = \psi_{11} S_1 + \psi_{12} W_1 \)

(13)

2. To cancel the effect of \( S_1 \) in eq. 13, construct an \( (N-r) \times r \) square matrix \( V \) such that \( V^t \psi_{12} = 0 \). This matrix can be easily constructed by expressing its \( k \)th vector \( V_k \) as follows:

\[
V_k = I_{N-r,k} - \sum_{j=1}^{r} \alpha_j \psi_{12}(; j), \quad \text{and} \quad I_{N-r,k} \equiv I_{N-r}(; k), \quad 1 \leq k \leq N - r
\]

(14)

The \( \alpha_j \) are obtained by solving a set of \( r \) linear equations satisfying the following condition:

Since \( \psi_{12} \) is an \( (N-r) \times r \) matrix,

\[
V_k^t \psi_{12}(; j) = 0 \quad 1 \leq j \leq r
\]

then its maximum rank is \( r \). Consequently, the rank of the matrix \( V \) is \( (N-r) \), [19].

3. Pre-multiply Equation (13) by \( V^t \) to yield

\[
V^t A_{0w} \phi = V^t \psi_{11} S_1
\]

(15)

As the rank of \( \psi_{11} \) is \( (N-r) \), the rank of \( V^t \psi_{11} \) is \( (N-r) \). So, to have a unique solution of eq.15, \( r \) arbitrary parameters of every column of \( S_1 \) have to be known at the receiver/extractor. This can be achieved if in the watermarked image \( A_w \), we choose the matrix \( z \) (eq. 6), to be \( S(N-2r+1:N,:) \) instead of \( S(N-r+1:N,:) \). (it basically means replicating the \( r \) last rows of the image as in Fig. 2 (a)).
Having obtained \(S_f\) as the unique solution of eq.15, \(w_f\) (the logo) is extracted as in the non-blind case, and subsequently reshaped to regain the original watermark \(w\). We used the terminology quasi blind, as a minor amount of information has to be known (\(r\) parameters of every column) at the receiver side. We note here that having \(r\) rows of the host image known at the receiver side as a mandatory condition for our blind technique is a slight draw back. However if we replicate the \(r\) rows of our host image, \(S(N-2r+1:N-r,;\), as the last \(r\) rows, our host image would be like fig.4(a) with negligible effect for this replication process, especially if the host image has a large size compared to \(r\), as \(N>>r\).

**4. Robustness against attacks (compression, noise and cropping)**

The proposed watermarking techniques has been reported to be robust against compression (which is mainly shown in the next section), cropping and noise attacks [14-15]. Although this paper is primarily aimed at introducing a joint compression and watermarking system, we report here the performance against different attacks and compare it with other literature performances.

Regarding the cropping attack [14], if we crop the host watermarked image up to 50% of its original size, full extraction of the watermarked logo is shown to be possible, as in the non blind case, provided that the remaining watermarked size is at least the logo size. This ratio outperforms most of the other watermarking techniques against this kind of attack.

Regarding the noise attack, as reported in [15], we mixed the watermarked image with different amounts of noise such as the salt and pepper noise and the AWGN noise, so that the PSNR value of the original image went as low as 22-25 dB. The watermarking logo was correctly extracted with a correlation rate higher than 90%, which is very competitive with the recent literature [8].

We note here that studying the compression attack’s impact on the proposed watermarking scheme is thoroughly examined in the next section, as it is part of the proposed joint compression and watermarking system, but we briefly state that the proposed watermarking approach can fully extract the hidden logo (more than 90% NCORR value) with up 1.0 bpp compression using the SPIHT compression approach.

**5. NPT based joint watermarking and Compression**

In our proposed system, we watermark our host image with a logo image to obtain a watermarked image. Then we compress the watermarked image through any transform based image compression standard. In our case we selected the SPIHT wavelet based image codec [20], to compress and then decompress (at the receiver side) the watermarked image, and then the extraction process takes place for the host and logo images. In our system we measure the compression performance by the PSNR quality of the reconstructed image (with respect to the original image) for a specific bit rate, while we measure the watermarking performance by the PSNR quality of the extracted image (host and logo) for a specific bit rate with a specific logo size. It can also be easily proven that the target compression bit rate would significantly affect the watermarking extraction quality, as shown next.

We also watermark compressed domain data, by watermarking the LL band image in the wavelet transform of any compression process, Fig. 2(b). It can also be shown that the amount of watermarked data (with its target extraction quality) would significantly affect the compression reconstruction performance; it is also dependent on which wavelet level (number of layers) its LL band is being watermarked as also shown in the next section. We note here that the higher the LL band (more layers) that is being watermarked, the less the quality of the reconstructed image from wavelet based compression theories. This is due to the fact that more data would be concentrated in LL band of the highest layer; therefore any manipulation to the band coefficients, as what happens by NPT, would more deteriorate the reconstructed image, also as a larger number of high band frequencies are dependent on it as in SPIHT or EBCOT [20-21]. We note here that if the there is no watermark, zero number of embedded bottom lines, then increasing the number of wavelet layers would definitely enhance the PSNR of reconstructed image from enhanced resolution, but if there is a watermark, even if it is small (5 rows), it will affect (negatively) the reconstructed host image, and hence increasing the number of wavelet decomposition layers would further deteriorate the PSNR of the reconstructed host image. Increasing the number of wavelet layers would also
double the number of rows in the bottom embedding process, as the logo (watermark) has a fixed size and the last LL band would be half the number of rows and columns of the previous case for every decomposition level. This would provide us with one more justification for the deteriorated PSNR reconstruction quality of the host image for increasing the number of wavelet layers from this joint watermarking and compression process.

For a watermarking system that is based on section 3, Fig.3 shows the PSNR values of the watermarked image for different values of alpha ($\alpha$), along with the corresponding NCORR values of the extracted image, when the watermarked image is compressed using SPIHT with bpp (bits per pixel) = 2.5, and no wavelet decomposition layers. It can be seen in the figure, that the smaller the value of alpha, the less contribution of the original image in eq.2, and the lower the PSNR, but the more contribution of the Hartley basis, which means more energy distribution, which will yield better extraction, better NCORR, and vice versa. A value of alpha in the range 0.985-0.99, is the optimal trade-off point between the 2 curves for this watermarking case, as in Fig. 3.

Fig. 4, shows a block diagram for our proposed joint watermarking and compression system. There are primarily three parameters that can significantly affect the performance of both watermarking and compression. The alpha parameter ($\alpha$) as in eq.2, the number of wavelet layers and the target bit-rate in compression in the adopted SPIHT.

While it can be easily proven that the higher the bit-rate, the better is the PSNR of the extracted image (both host and logo) and the lower is the compression performance from basic rate-distortion theories [20-22]. The higher the value of $\alpha$ the more weight of the original image would be in eq.2, which would imply less contribution of the Hartley basis, which means lower amount of energy distribution, which means less watermarking performance. On the other hand, more wavelet decomposition layers, which would imply more resolutions levels, and would lead to better compression performance as well known from successful wavelet based coders [20, 21]. Since in our system we watermark the LL band in the last wavelet layer, increasing the number of layers would deteriorate the compression reconstruction quality of watermarking extracted images, as higher band frequencies are added to it in reconstruction, as in Fig. 6. Therefore increasing the number of wavelet layers in our system would imply less PSNR for the reconstructed image (that has been watermarked and extracted). Hence, while increasing the bit rate would enhance the reconstruction quality of watermarking an extracted image, increasing the number of wavelet decomposition layers would deteriorate it in our joint watermarking and compression system, and the lower the value of alpha, the better the watermarking extraction as the NCORR curve in Fig. 3. Since the number of wavelet decomposition layers and the bit rate are two compression parameters and they have an inverse impact on the watermarking performance, they could be jointly combined in a single variable $C$, according to this relation, $C=K_1 \times \text{bpp} + (1/K_2 \times \text{No. of wavelet layers})$.
From all above, we can identify the two variables of alpha and C as the parameters that affect the performance of our proposed joint watermarking and compression system. As shown above, each of them can significantly affect the performance of both watermarking and compression (JWC) on an inverse manner. Hence these two parameters can be combined into a single equation with a Lagrange multiplier as in eq. 16. The Lagrange multiplier can be adjusted to control both alpha () and C on a trade-off manner. JWC stand for performance of our joint system.

\[ JWC = \alpha + \lambda \cdot C \]  

(16)

Fig. 4 shows a block diagram of the proposed joint watermarking and compression system with a Lagrange multiplier as an adjustor that controls the trade-off between both. Fig. 5 shows the PSNR and the NCORR values for different alpha values on the same curve, it can be shown that an alpha value of 0.985 is optimal on that curve’s trade-off. Fig. 6 shows the reconstructed PSNR quality of host images from watermarking the LL band for different number of layers, with an alpha () value of 0.985 and 2.5 target bpp. Fig. 7 shows the reconstructed PSNR quality of host images for different bit rates from one wavelet decomposition layer with an alpha value of 0.985.
We note here the variables of $K_1$, $K_2$ and $\lambda$ are image dependent, and can be adjusted according to the needed point on the compression and watermarking trade-off.

Fig. 8 shows the PSNR of the reconstructed and extracted host image with a bpp 2.5 with different numbers of bottom embedding rows, which imply different logo sizes. It is obvious that the increased number of bottom rows of the logo image, would deteriorate the PSNR of the reconstructed host image.

Fig. 9 shows the compression performance (PSNR reconstruction quality of watermarked host image) and the watermarking performance (NCORR correlation of the extracted logo), both against different alpha ($\alpha$) values as well as different $C$ values, a higher $C$ value would imply high bit rate and less number of wavelet decomposition layers. It can be shown that the compression and watermarking performances are inversely affected by changing the value of either alpha or $C$; hence they have to be treated on a trade-off manner.

5. Discussion

In this paper we presented a joint watermarking and compression system that can both compress and watermark a host image on a trade-off manner. We note here that our primary objective was to present the idea of joint compression and watermarking, rather than a regular single watermarking or compression technique like the recent literature, or our work in [14-15].

![Joint graph for NCORR and PSNR values across different alpha values](image-url)
Fig. 6 PSNR reconstructed quality of host for different number of wavelet layers

Fig. 7 PSNR reconstructed quality for different bpp for one wavelet decomposition layer
Fig. 8 PSNR reconstructed quality for host for different logo sizes

Fig. 9 Joint watermarking and Compression for different bits per pixels for Lena and Cameraman images
When treating compression and watermarking jointly, compression parameters can be treated as security keys, while watermarking data or keys can be considered as compression indices. Our proposed simulation results showed that there were three variables that could significantly affect the performance of both watermarking and compression. Bit rate, number of wavelet decomposition layers and the alpha value, which controls the balance between energy concentration (compression) and energy distribution (watermarking). The number of wavelet decomposition layers and the bit rate are two compression parameters that are typically defined in any wavelet-based compression process and they were combined in a single compression parameter C. Since both the alpha value and the C compression parameter had inverse impact on the performance of both compression and watermarking, a Lagrange multiplier equation was introduced that controls the balance between alpha and C on a trade-off manner. We note here the Lagrange multiplier value would depend on both the image class/type/content in addition to the desired point between compression and watermarking performances.

7. Conclusions

Our proposed system can be utilized in joint watermarking and compression applications that exploits compression parameters as watermarking variables, while compression indices could be used as watermarking actuators/adjustors. Our illustrated simulation results support our hypotheses and analogies in joint watermarking and compression, that they are inversely related and there is a trade-off relation between them, hence they should be treated jointly to achieve the optimal point of them. This work is funded by the ministry of Communication and Information Technology, Egypt, ITIDA. It has also been funded partly by the Alexander von Humboldt foundation, Germany.

References