Journal of VLSI Signal Processing 27, 35–53, 2001

An Integrated Approach to Image Watermarking and JPEG-2000 Compression

PO-CHYI SU, HOUNG-JYH MIKE WANG* AND C.-C. JAY KUO
Department of Electrical Engineering-Systems, University of Southern California, Los Angeles, CA 90089, USA

Received August 2, 1999; Revised January 17, 2000

Abstract. A scheme which integrates image compression and image watermarking in an effective way is proposed in this research. The image compression scheme under consideration is EBCOT (Embedded Block Coding with Optimized Truncation) which has been adopted in the verification model (VM) of the emerging JPEG-2000 image compression standard. The watermark is embedded during the process when the compressed bit-stream is formed, and can be detected on the fly in image decoding. Thus, watermark embedding and retrieval can be done very efficiently in comparison with other existing watermarking schemes. In addition to efficiency, the proposed scheme has many interesting features. The embedded watermark is robust against various signal processing attacks such as coding and filtering while the watermarked image maintains good perceptual quality. The watermark retrieval procedure does not require the knowledge of the original image. Furthermore, the watermark can be detected progressively and region of interest (ROI) watermarking can be accomplished easily.

Keywords: JPEG-2000, EBCOT, digital watermark, progressive watermark detection, ROI

1. Introduction

The need to facilitate transmission, storage and archiving of multimedia data has led to great research interests in the development of efficient coding schemes in the last two decades. With the advance of compression technologies, high quality digital media can be compacted into a small data stream and distributed widely over the network in a fast speed. When people start to enjoy listening to network audio, watching on-line video, reading web newspapers, magazines, or other electronic publications, content-providers are concerned with the problem of copyright infringement. Unlike traditional analog copying with which the quality of the duplicated content is degraded, powerful digital facilities can produce a large amount of perfect copies in a short period of time. Therefore, to develop an effective way to deter users from illegally reproducing or misusing digital media becomes an urgent issue. Recently, researchers have considered embedding invisible or inaudible information into digital data for copyright/ownership verification and authentication. The hidden information is known as the digital watermark.

To unambiguously identify the content source or destination for successful copyright protection for digital media, a digital watermark has several requirements. First of all, a digital watermark should be robust against intentional or unintentional attacks including compression, filtering, and format conversion, etc. Besides, the watermark must be imperceptible to human beings and able to convey enough information for different purposes. The watermark has to be secure enough to resist attempted attacks by knowledgeable persons. Moreover, watermarking schemes should have a low complexity so that they can be applied to real-time applications. It is also important that the probability of watermark false detection should be kept as low as possible. Therefore, a lot of design tradeoffs must be taken into

*Present Address: Media Fair, Inc., Monterey Park, CA 91754, USA.

account to develop a sound watermarking scheme. The overview of watermarking techniques in various types of media can be found in [1–3].

In image watermarking, we classify watermarking schemes into two categories depending on the domain of watermark insertion and retrieval, i.e. the luminance intensity in the spatial domain [4–7] and the transform coefficient magnitude in the frequency domain [8–12]. Spatial-domain watermarking is to embed information by modifying the value of image pixels directly, e.g. replacing the least significant bit (LSB) of image pixels with a binary pseudo-random sequence as watermark information. The basic idea of frequency-domain watermarking is to modify frequency coefficients after a proper transform such as the Discrete Wavelet Transform (DWT), the Discrete Cosine Transform (DCT), or the Discrete Fourier Transform (DFT) is applied. Frequency-domain watermarking methods can be further divided into two categories: visual-model based and energy based watermarking. The visual-model based watermarking decides the location and the amount of the cast watermark by exploiting the human visual system model. The energy based watermarking is done by examining coefficients with a larger energy amount and modifying them slightly. Because frequency-domain watermarking schemes tend to achieve both perceptual transparency and robustness better, a lot of related algorithms have been developed.

Most of frequency-domain watermarking schemes are based on the additive spread-spectrum method, which is inspired by the spread-spectrum modulation technique in the digital communication system. This technique provides more security and resistance to channel noise for digital communication. Similarly, the spread-spectrum watermarking scheme can resist more serious content distortion. The watermark is usually represented by a pseudo-random signal with a low amplitude. The pseudo-random signal is either added or subtracted from the host data and then detected later by using a correlation receiver or matched filter. An early spread-spectrum frequency-domain watermarking method is proposed by Cox et al. [9]. Watermark sequence with length N is added onto the largest N coefficients (except the DC coefficient) after the global DCT transform is applied to the image. The watermark is retrieved by subtracting the original coefficients from the watermarked coefficients and then a correlation detector is used to calculate the similarity between the original watermark sequence and the extracted one. Piva et al. [8] examined another global DCT-based method but no original image is required for watermark detection. This is usually called *blind* watermark detection. The global DCT coefficients are reordered by using a zig-zag scan. Fixed DCT coefficients (e.g. 16000th to 25000th coefficients for an image with size larger than 256 by 256) are selected for watermark embedding and retrieval. The above two watermarking methods share one common major drawback. That is, the watermarking process is very slow due to the high computational complexity in calculating global DCT coefficients. Xia et al. [10] considered a multi-resolution watermarking method in the wavelet domain which requires the original image in watermark retrieval. Wang et al. [12] investigated a blind wavelet-based watermarking scheme, in which the inserted watermark signal is adaptively scaled by different threshold values to maintain perceptual integrity of the watermarked image. These two wavelet-based watermarking methods are more robust against wavelet-based coding in comparison with DCT-based watermarking schemes as given in [8, 9].

It is worthwhile to point out that image compression and frequency-domain watermarking share some common characteristics. In image compression, we encode significant frequency coefficients first because these coefficients convey more fundamental visual information about the image. In watermarking, we choose significant coefficients for watermark casting to enhance its robustness since these coefficients often remain stable after the attack. If they do change substantially, the reconstructed image will be perceptually different from the original one, and the value of protecting the intellectual property right of such a seriously degraded image becomes low. With this similarity, efficiency can be achieved by integrating frequency-domain watermarking procedures with compression processes, since the most expensive computation related to the image transform has been already computed as one part of compression and decompression algorithms.

In this research, we investigate an integrated approach to image compression and watermarking. The image coding scheme under our consideration is EBCOT (Embedded Block Coding with Optimized Truncation) [13, 14], which has been accepted in JPEG-2000 VM (Verification Model) and will be the backbone of JPEG-2000 coding scheme. EBCOT has several distinct advantages, including efficient rate control, low computational complexity, low memory requirement, good error resilience and excellent coding efficiency. Besides, EBCOT supports region of interest

(ROI) coding, which allows users to select parts of an image to achieve higher fidelity. By integrating the watermarking scheme with JPEG-2000, the proposed watermark embedding and retrieval are more efficient in comparison with existing watermarking schemes. The watermark is embedded in the discretized host image coefficients by examining bit-planes. A binary or bi-polar watermark sequence is used, and the resulting watermarked image coefficients also take only discrete values. Therefore, both watermark embedding and detection occur directly in the compressed domain. The integrated scheme eliminates both the need to compress the host image after watermark embedding and the need to decompress the watermarked image before watermark detection. In addition to efficiency, the proposed scheme has quite a few interesting features. The embedded watermark is robust against various signal processing attacks including compression and filtering while the resulting watermarked image maintains good perceptual quality. The progressive characteristic is essential for Internet applications since users can get a coarse-resolution image after a small portion of the bit-stream is received. For the same reason, it is desirable that the embedded watermark can be detected progressively so that an operation, which is enabled via watermark detection such as “never copy”, can be enforced earlier without waiting for the whole image to be downloaded. Furthermore, ROI watermarking can be easily coupled with ROI coding in the proposed scheme. In this case, when we receive ROI without the background, the watermark can still be detected without ambiguity. The embedded watermark can be detected without the knowledge of the original image so that it is a blind watermarking scheme. Experimental results show that the proposed integrated JPEG-2000 watermarking performs very well and supports all above claims.

This paper is organized as follows. A brief overview of JPEG-2000 compression scheme is provided in Section 2. The integrated watermark embedding and detection procedures are presented in Section 3. The decision and analysis of the threshold for watermark detection are discussed in Section 4. Experimental results are illustrated in Section 5. Finally, concluding remarks are given in Section 6.

2. Brief Review of JPEG-2000

The current JPEG-2000 VM (Verification Model) [13, 14] is based on the Embedded Block Coding with Optimized Truncation (EBCOT) scheme proposed by Dr. Taubman. Basically, EBCOT can be viewed as a block-based bit-plane coder. By the block-based coder, we mean that the basic coding unit is a block instead of the whole image as used in coding schemes such as SPIHT [15] and EZW [16]. A bi-orthogonal wavelet transform is first applied to the image, and each subband of wavelet coefficients is divided into blocks of samples with the same dimension, except at image boundaries where some blocks may have smaller dimensions. Therefore, blocks in lower resolution subbands span a larger spatial region in the original image. Each block is then encoded independently by using the same algorithm. That is, for each block, a separate bit-stream is generated without resorting to any information from other blocks. The bit-stream can be truncated to a variety of discrete lengths with respect to different distortion measures. Once the entire image has been compressed, a post-processing operation passes over all compressed blocks, and determines the extent to which each block’s embedded bit-stream should be truncated to achieve the target bit-rate. The final bit-stream is formed by concatenating the truncated bitstreams of all blocks together.

EBCOT is a bit-plane coding, i.e. the most significant bits for all samples in the code block are sent first, then the next most significant bits and so on until all bit planes are sent. Previously encoded information about the current sample and neighboring samples are exploited for efficient block coding. For each bit-plane, the coding proceeds in a number of distinct passes. EBCOT provides many features, including random access, Signal to Noise Ratio (SNR) progressive, SNR parsable, resolution progressive, resolution parsable and component parsable. The rich bit-stream syntax makes EBCOT more attractive than other wavelet-based coders. Region of interest (ROI) is one interesting feature that can be easily supported by EBCOT. ROI coding makes it possible to encode regions in which users are more interested with better quality than the rest of the image. For the extreme case, the specified ROI can be encoded losslessly while the remaining parts of the image are encoded with low bit-rates. When ROI is small compared with the whole image, the transmission time and the storage space can be greatly saved.

The implementation of EBCOT is a pipeline structure, which attempts to minimize the internal memory size. Thus, EBCOT can be implemented by hardware conveniently. Two kernels are used in EBCOT. One is reversible kernel for lossless compression, and the other is non-reversible kernel for lossy compression. Since the two kernels use different wavelet filters and normalization strategies, encoding and decoding must adopt the same kernel. For lossy compression, the original I-bit image samples are level shifted to a nominal range of -2^{I-1} to 2^{I-1} and then shifted up by $P-I-G$ bits to fit within the P-bit implementation precision. G is the number of guard bits, which is included to avoid the occurrence of overflow so that the frequency coefficients can be represented with the fixed-point precision. The wavelet transform kernels are then normalized so that the low-pass analysis filters always have a unit DC gain and the high-pass analysis filters always have a unit Nyquist gain. This means that the nominal range of subband coefficients will be in the range of -2^{P-G-1} to 2^{P-G-1}. The normalization of coefficients is a very important step in the EBCOT implementation, which turns out to facilitate the proposed watermarking process as described later.

3. Watermark Embedding and Retrival

3.1. *Framework for Watermarking*

Before presenting the implementation of the proposed watermarking scheme, we briefly describe the basic framework of the watermarking method to be adopted. Similar to most robust watermarking schemes given in Section 1, the additive spread-spectrum watermarking method is chosen due to its decent characteristics in robustness, unobtrusiveness and security to watermarking applications. After a proper transform (the wavelet transform in our scheme) is applied to the image, the watermark is added onto the selected frequency coefficient by

$$I'(x, y) = I(x, y) + \alpha(x, y) \times W(x, y), \qquad (1)$$

where $I'(x, y)$ is the watermarked coefficient and $I(x, y)$ is the original coefficient with the coordinate (x,y) in the spatial position. $I(x, y)$ is chosen based on its magnitude, i.e. the coefficient with the large magnitude is selected for watermark embedding. $W(x, y)$ is the corresponding watermark symbol, which can be a real number or only take values, 1 and -1. The weighting factor $\alpha(x, y)$ is a positive number used to adjust the amount of added watermark energy. The value of α is usually adjusted according to the magnitude of the frequency coefficients or the different subband characteristics so that the balance between robustness and fidelity of the resulting watermarked image can be achieved. The inverse transform is then applied to form the watermarked image.

In watermark detection, a correlation detector is used to determine if the watermark exists in the tested image. It is based on the fact that if the coefficients and the watermark sequence are independent, the inner product of the watermark and the coefficient sequences will be close to 0. If the target watermark sequence is added to the coefficient sequence, we will get a peak response from the inner product. We show this basic idea as follows; $I^*(x, y)$ is the wavelet coefficient of the suspected image. We make use of the correlation detector to determine if the wavelet coefficients are embedded with a specific watermark sequence $W^*(x, y)$. The correlation response ρ of the watermark detector can be expressed as

$$\rho = \sum_{(x,y)} (I^*(x, y) \times W^*(x, y)) \qquad (2)$$

By assuming that $I^*(x, y)$ is formed by casting watermark symbol $W(x, y)$ onto the original coefficient $I(x, y)$ without any modification, then we can express ρ as

$$\rho = \sum_{(x,y)} ((I(x, y) + \alpha(x, y) \times W(x, y)) \times W^*(x, y)) \qquad (3)$$

$$= \sum_{(x,y)} (I(x, y) \times W^*(x, y)) + \sum_{(x,y)} (\alpha(x, y) \times W(x, y) \times W^*(x, y)) \qquad (4)$$

After calculating the expected value of both sides, we get

$$\mathcal{E}[\rho] = \mathcal{E}\left[\sum_{(x,y)} (I(x, y) \times W^*(x, y))\right] + \mathcal{E}\left[\sum_{(x,y)} (\alpha(x, y) \times W(x, y) \times W^*(x, y))\right], \qquad (5)$$

where $\mathcal{E}[\cdot]$ is the expected value. The first term on the right-hand side of (5) is zero if the tested watermark sequence $W^*(x, y)$ and the coefficients $I(x, y)$ are independent. Similarly, the second term is also zero if $W(x, y)$ and $W^*(x, y)$ are independent or $W(x, y)$

does not exist. If the image is embedded with $W^*(x, y)$, i.e. $W(x, y) = W^*(x, y)$, then the expected value of the correlation response $\mathcal{E}[\rho]$ will be close to

$$\mathcal{E}[\rho] = \mathcal{E}\left[\sum_{(x,y)} \alpha(x, y) \times W^{*^2}(x, y)\right], \qquad (6)$$

which is much larger than zero. Therefore, we can simply examine the peak response and compare it with a threshold value to determine the existence of watermark without any difficulty.

3.2. *Implementation of the Integrated Watermarking Scheme*

In the proposed system, the watermark is embedded after coefficients are quantized so that the watermark can be easily embedded into the bitstream. Watermark detection is done before the dequantization stage. We choose the non-reversible kernel for watermark embedding and detection in the following discussion since lossy compression offers a broader application scope than the lossless one. The same idea can however be applied to the reversible kernel without modification.

3.2.1. Watermark Embedding. To make the embedded watermark robust against attacks, significant coefficients are chosen for watermark casting. Significant coefficients are those with a larger magnitude. Because coefficients in each subband have been normalized to have unit gain in EBCOT implementation, the significant coefficients in each subband tend to have their highest non-zero bit in the same bit-plane. Therefore, we can apply the same watermark embedding rule in each subband. EBCOT divides the subband into blocks which is the basic coding unit so that we also use the coding block as the basic unit for watermarking.

In EBCOT implementation, the Most Significant Bit (MSB) of the coefficient indicates the sign value and the remaining $P - 1$ bits represent the absolute magnitude of the coefficient. This simplifies the case when the magnitude is required only, because we can avoid the calculation of the absolute value. We select significant coefficients by examining the highest non-zero bit (not including the sign bit) that is higher than a certain bit-plane with index q. That is, coefficient $I_{b_s}(x, y)$ in the block b_s of subband s with the coordinate (x, y) will be chosen for watermark embedding if

$$\|I_{b_s}(x, y)\| \geq 2^q, \qquad (7)$$

where we define that the Least Significant Bit (LSB) of coefficients form the bit-plane with index “0”. The strategy to select coefficients matches the bit-plane coding well since coefficients to be coded earlier will be cast with the watermark first. The watermark in our scheme is a random number sequence taking two values 1 and -1. First, a seed, which can be viewed as a user ID number, is used to generate the watermark sequence with the length equal to the number of coefficients in a coding block. The sequence forms a watermark map with a dimension equal to that of a block. For a block of size $\gamma \times \gamma$, the watermark map is $W_{b_s}(x, y)$, where $x, y \in [0, \gamma)$, and the coefficient $I_{b_s}(x, y)$ that satisfies (7) is modified to $I'_{b_s}(x, y)$ by

$$I'_{b_s}(x, y) = I_{b_s}(x, y) + \left(W_{b_s}(x, y) \times 2^{\delta_{bs}}\right) \qquad (8)$$

where $W_{b_s}(x, y) = \pm 1$ is the watermark element in the position (x, y) on the watermark map associated with block b_s and δ_{b_s} is the number of bit-shift that depends on the implementation precision P and the watermark energy. In general, the shifted number is chosen to be

$$\delta_{b_s} = P - I - G + \alpha_{b_s}. \qquad (9)$$

As mentioned earlier, P, G and I are the implementation precision, the guard bit, and the image sample precision, respectively, and α_{b_s} is the watermark scaling factor. We may increase the embedded watermark energy by shifting the watermark a few bits to the left. It should be noted that α_{b_s} can vary in different subbands or blocks so that we can adjust it according to different subband or block characteristics. Generally, only bitplanes around $P - I - G + \alpha_{b_s}$ will be affected by watermark embedding so the bitplane-based watermark embedding method does not affect the coding efficiency much. Besides, by experiments, the setting of δ_{b_s} achieves a pretty good balance between image quality and robustness of the watermark. Special care must be taken that we do not cast the watermark in blocks of the DC band since it may lead to serious fidelity degradation in the watermarked image.

3.2.2. Watermark Detection. As done in the embedding procedure, we only pick coefficients that satisfy (7) for watermark detection. We use the same bit-plane as a reference so that only the coefficients that are possibly embedded with watermark are taken into consideration. A similar objective might be achieved if we embed and detect the watermark in all of the wavelet coefficients. However, the watermarking process will be less efficient because the computational load will increase significantly especially when we have to test a lot of watermark sequences to see which one is embedded in the image.

However, we have to take the significance of different subbands into account during watermark detection. A value called "extra LSB" and denoted by β_{b_s} is determined along with the EBCOT normalization process and can be interpreted as the number of insignificant bit-planes in the coding block b_s. β_{b_s} is smaller in subbands that need better precision and larger in high-frequency subbands. Thus, the calculation of correlation response is done as

$$\rho = \frac{\sum\limits_{s}\sum\limits_{b_s}\sum\limits_{\substack{(x,y)\\(\|I^*_{b_s}(x,y)\|\geq 2^q).}} \left(I^*_{b_s}(x,y) \times 2^{-\beta_{b_s}}\right) \times \left(W_{b_s}(x,y) \times 2^{(\delta_{b_s}-\beta_{b_s})}\right)}{\sum\limits_{s}\sum\limits_{b_s}\sum\limits_{\substack{(x,y)\\(\|I^*_{b_s}(x,y)\|\geq 2^q)}} 2^{(2\delta_{b_s}-2\beta_{b_s})}}, \tag{10}$$

where δ_{b_s} is defined in (9). $I^*_{b_s}$ is the coefficient of the investigated image. Note that there is a difference between (2) and (10). In (10), we normalize the correlation response by the sum of squares of selected watermark symbols. Since the watermark symbol takes value 1 or -1, $W^2_{b_s}(x,y)$ is equal to 1 and omitted in the denominator. There are a couple of reasons that we decide to normalize the correlation response. First of all, the value of the response will not be affected by the number of selected coefficients. Consequently, the same correlation response can be used in different scenarios, e.g. normal watermark detection and progressive watermark detection, which will be discussed in Section 3.3. Second, this normalization process will help in explaining the high value of the correlation response of the watermarked image in our scheme. That is, the value of (2) in a watermarked image will be even larger than (6). This phenomenon will be discussed in Section 4.

3.3. *Progressive Watermark Detection*

Progressive watermark detection is one of the most attractive features for watermarking in JPEG-2000 compressed images. When a large image is being decompressed, it is not efficient to detect the watermark after the whole image is formed. This is especially true for Internet applications. A fully-embedded compression scheme lets the user truncate the image at any time to get his or her "best" image. Thus, it is desirable that the watermark can also be detected progressively. EBCOT is a bit-plane coder which can support the fully-embedded feature. Significant coefficients, which have been embedded with the watermark in our scheme, will be encoded and decoded first so that progressive watermark detection can be achieved easily. However, we should set a threshold value η to indicate the minimum number of coefficients needed for watermark detection. If the correlation response is higher than the current threshold, which is used to decide the existence of watermark, but the selected coefficients are less than η, the detection process should continue in other blocks to avoid possible false alarm. The derivation of the threshold in the proposed watermarking scheme will be discussed in Section 4.

3.4. *Region of Interest Watermark*

There are two types of ROI functionality. The first one is "ROI during encoding", in which ROI is specified when the image is compressed. The other one is "ROI during decoding" that supports interactive browsing. In JPEG-2000 VM, the "ROI during encoding" mode is implemented. In the encoder part, coefficients that belong to ROI remain unchanged while other coefficients which do not belong to ROI are scaled down by a few bits. The encoding process is done as usual while the coordinates of ROI and scaling values are put in the bitstream header for transmission. When the SNR progressive mode is used, ROI will be sent before the background. The decoder can detect ROI by examining the magnitude of received coefficients since all ROI coefficients are larger than other coefficients outside ROI. The decoder may have to upshift the received coefficients when necessary.

Under this scenario, we do not have to change the proposed algorithm because only coefficients in ROI with a larger magnitude will be embedded with the watermark. All coefficients outside ROI will be downshifted so that they will not satisfy the criterion in (7) for watermark embedding and retrieval. To conclude, our scheme can support ROI watermarking automatically.

4. Threshold Decision and Analysis

It is essential to determine a threshold value so that the existence of a watermark sequence can be detected by comparing the value of the correlation response with the selected threshold value. There are two main parts in this section. First of all, we determine the threshold value to decrease the possibility of false positive detection. False positive detection occurs when the watermark is falsely detected in an image that contains no watermark or the wrong watermark ID is detected. Since the usage of the image will be limited once a certain watermark is found, false positive detection will bring much more inconvenience to the legitimate users. Therefore, the threshold value should be decided carefully. Second, we examine the peak correlation response of the watermarked image and show that the existence of the watermark can generate a large correlation response.

In watermark detection, we compute the sum of multiplications of the shifted coefficients with the corresponding watermark symbol in the watermark map, and then divide it by a weighting factor, i.e. the weighted norm of the watermark sequence as indicated in (10). Here, we assume that the correlation response ρ follows the Gaussian distribution due to the Central Limit Theorem.

The variable ρ in (10) has a mean equal to zero if the watermark does not exist. The variance of ρ can be estimated by

$$\sigma_\rho^2 \simeq \frac{\displaystyle\sum_{s}\sum_{b_s}\sum_{\substack{(x,y)\\(\|I^*_{b_s}(x,y)\|\geq 2^q)}} I^{*^2}_{b_s}(x,y)\times 2^{(2\delta_{b_s}-4\beta_{b_s})}}{\left\{\displaystyle\sum_{s}\sum_{b_s}\sum_{\substack{(x,y)\\(\|I^*_{b_s}(x,y)\|\geq 2^q)}} 2^{(2\delta_{b_s}-2\beta_{b_s})}\right\}^2}, \qquad (11)$$

where all entities in above are the same as those in (10).

By definition, the Gaussian Integral Function [17] (or simply the Q function) can be written as

$$Q(z) = \int_z^\infty \frac{1}{\sqrt{2\pi}}\, e^{\frac{-x^2}{2}}\, dx. \qquad (12)$$

If random variable $Y(u)$ follows the Gaussian distribution with mean m and variance σ^2, the probability that $Y(u) > a$ can be expressed as

$$Pr\{Y(u) > a\} = Q\left(\frac{a-m}{\sigma}\right). \qquad (13)$$

We should set up the threshold value according to the Q function so that the false alarm rate is lower than a given probability. As a result, the threshold value is actually a function of the variance of ρ. Here, we simply define the threshold as

$$T = \tau \times \sigma, \qquad (14)$$

where τ is a scaling parameter. On one hand, we can lower the false alarm rate by raising the τ value. On the other hand, we can reduce the τ value so that detection of the embedded watermark can be more easily achieved even under very serious attacks at the expense of a higher false alarm rate. For example, if the desired false alarm rate is around 10^{-12}, we should choose the threshold value as $T = 7\sigma$ since

$$Pr\{Y(u) > T\} = Q\left(\frac{T}{\sigma}\right) = Q(7) = 1.28 \times 10^{-12}. \qquad (15)$$

In progressive watermark detection, the probability of false alarm can be larger because the number of the selected coefficients may not be large enough. We choose a larger τ to get a higher threshold to lower the probability of false alarm as much as possible. It is also possible to adjust the τ value to adapt to different detection situations.

After setting up the threshold, we would like to analyze the peak value of the correlation response when a certain watermark is found to exist in an image. To simplify the analysis, it is assumed that the extra LSB β_{b_s} and the bit-shift number δ_{b_s} are both equal to δ in all blocks. If the watermark exists, (10) can be modified as

$$\begin{aligned}\rho &= \frac{\sum\{(I_\mathrm{d} + W_\mathrm{d} \times 2^\delta) \times 2^{-\delta} \times W_\mathrm{d}\}}{\sum(W_\mathrm{d} \times W_\mathrm{d})}\\ &= \frac{\sum(I_\mathrm{d} \times W_\mathrm{d})}{\sum(W_\mathrm{d} \times W_\mathrm{d})} \times 2^{-\delta} + 1, \end{aligned} \qquad (16)$$

where W_d and I_d are the watermark symbol and the original coefficient selected by the watermark detector. To be more precise, we calculate the expected value on both sides as

$$\mathcal{E}[\rho] = \mathcal{E}\left[\frac{\sum(I_\mathrm{d} \times W_\mathrm{d})}{\sum(W_\mathrm{d} \times W_\mathrm{d})}\right] \times 2^{-\delta} + 1. \qquad (17)$$

As discussed in Section 3.1, one may think that the first term on the right-hand side of (17) is zero so that the expected value of the maximal correlation peak is unity. However, the peak can be substantially larger than 1 if a certain watermark exists in the image as argued below.

Let I_e denote the original coefficient selected by the watermark embedder, i.e. the coefficient satisfies (7), and W_e be its respective watermark symbol, i.e. the watermark symbol to be cast on the selected coefficient. First, we calculate the expected cumulative sum of $I_\mathrm{e} \times W_\mathrm{e}$:

$$\mathcal{E}[R_\mathrm{e}] = \mathcal{E}\Big[\sum (I_\mathrm{e} \times W_\mathrm{e})\Big]. \tag{18}$$

Note that $\mathcal{E}[R_\mathrm{e}] = 0$ because I_e and W_e are independent. Let us divide $\mathcal{E}[R_\mathrm{e}]$ into two parts, i.e.

$$\begin{aligned}\mathcal{E}[R_\mathrm{e}] &= \mathcal{E}[R_{\mathrm{e}_1}] + \mathcal{E}[R_{\mathrm{e}_2}] \\ &= \mathcal{E}\Big[\sum (I_{\mathrm{e}_1} \times W_{\mathrm{e}_1})\Big] + \mathcal{E}\Big[\sum (I_{\mathrm{e}_2} \times W_{\mathrm{e}_2})\Big].\end{aligned} \tag{19}$$

I_{e_2} is the coefficient satisfying both of the following conditions:

$$2^q \leq \|I_{\mathrm{e}_2}\| < 2^q + 2^\delta, \quad q > \delta, \tag{20}$$

and

$$I_{\mathrm{e}_2} \times W_{\mathrm{e}_2} < 0, \tag{21}$$

where W_{e_2} is the respective watermark symbol of I_{e_2}. Obviously, $\mathcal{E}[R_{\mathrm{e}_2}]$ is a negative number so that $\mathcal{E}[R_{\mathrm{e}_1}]$ has to be positive to make $\mathcal{E}[R_\mathrm{e}]$ equal to 0. However, owing to the process of watermark detection, coefficients I_{e_2} in R_{e_2} will not be picked by the detection process in watermark retrieval since its highest nonzero bit is $q-1$, which is lower than q. Therefore, the expected value of the correlation response calculated in the detection process is equal to

$$\begin{aligned}\mathcal{E}[\rho] &= \frac{\mathcal{E}[R_\mathrm{e}] - \mathcal{E}[R_{\mathrm{e}_2}]}{\mathcal{E}\left[\sum W_{\mathrm{e}_2}^2\right]} \times 2^{-\delta} + 1 \\ &= \frac{\mathcal{E}[R_{\mathrm{e}_1}]}{\mathcal{E}\left[\sum W_{\mathrm{e}_2}^2\right]} \times 2^{-\delta} + 1 > 1\end{aligned} \tag{22}$$

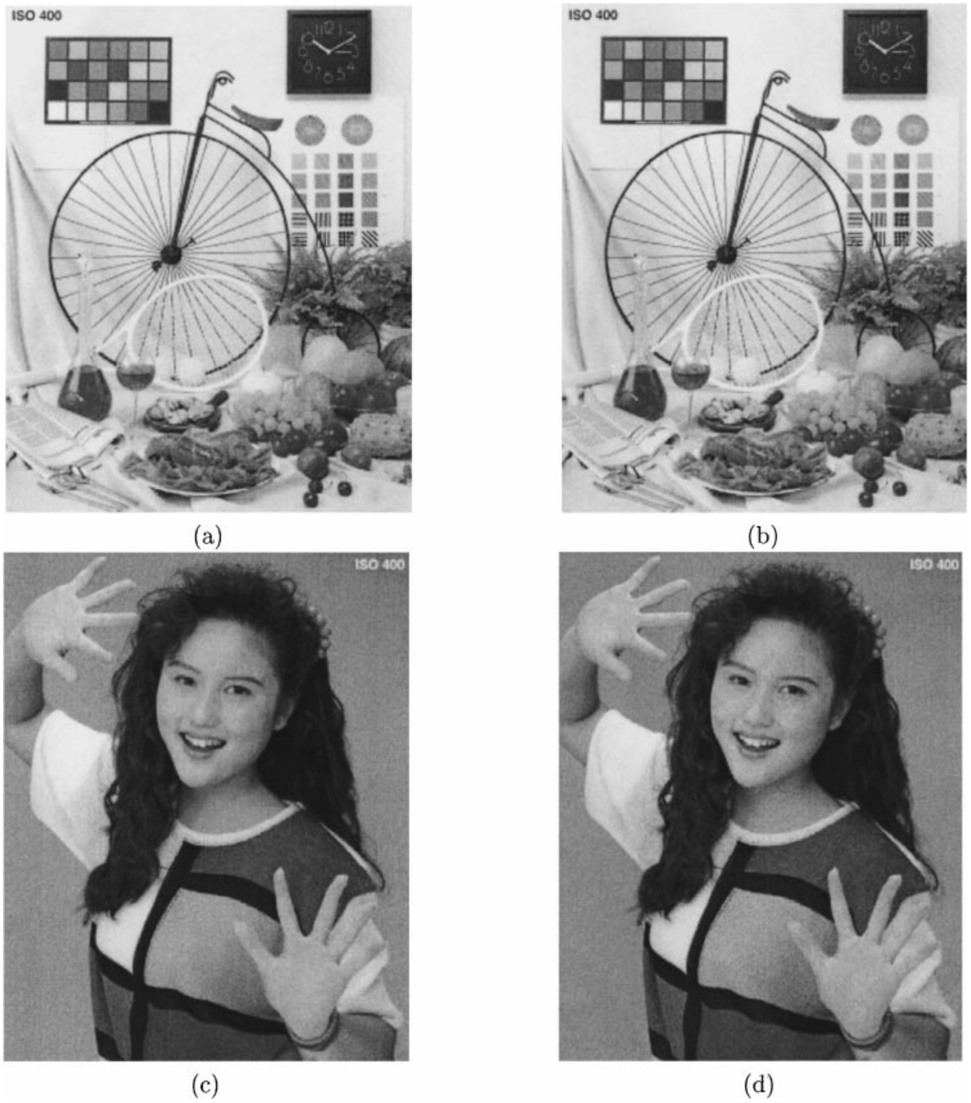
The number of coefficients I_{e_2} is quite large so that the first term of the right-hand side in (22) can be larger than 1 to generate a peak value ρ that could be even equal to 2 when the watermark exists in the image. Therefore, the first term of the right-hand side in (17) is positive and does make a contribution to the peak correlation response when a watermark is embedded.

One main concern of the correlation-based watermark detection is the efficiency issue. To determine which watermark ID number is embedded, we may have to check all possible ID numbers. By assuming the total number of users is 2^{32}, it is not practical to try from ID number 0 to $2^{32} - 1$ to determine the exactly embedded watermark ID number. Thanks to the block coding of EBCOT, we can simplify the detection structure. We first divide all coding blocks into n subset S_i, $i = 1, \ldots, n$. We can embed k bits in each of the subset S_i. Therefore, the total number of bits that can be embedded in the image is $k \times n$. In watermark detection, we only need to check 2^k different watermark candidates in each subset to decide the k-bit value. $k \times n$ bits can be decoded correctly after n subsets are processed. If we also consider the sign of the correlation response, we can check only 2^{k-1} watermark candidates in each block. For larger images, we are able to have more divided subsets to allow a larger watermark capacity. However, because spread-spectrum watermarking is adopted in the system, a spreading gain must be maintained to reliably embed and retrieve the watermark. Therefore, there exists a tradeoff between robustness and capacity.

5. Experimental Results

In this section, we show some experimental results to demonstrate the robustness of the proposed watermarking scheme. The embedded watermark has an ID number 500, which is actually the seed to generate the random watermark sequence. The watermark is embedded when the image is compressed. It can be detected when the EBCOT bit-stream is expanded. We test 1000 watermark ID numbers to see if the correct one is detected without ambiguity. A threshold value calculated with (14) is used to determine if there exists a certain watermark in the image.

First of all, we examine the parameters to be used in the experiments. In EBCOT implementation, the coefficient precision P can be either 32 or 16. We choose 32 since it is commonly used in software or hardware designs today. The guard bit G is chosen as 2, which has been shown a reasonable number to avoid the overflow problem. Therefore, the nominal range of subband coefficients will be in $(-2^{29}, 2^{29})$. The image sample precision I is equal to 8 for gray-level images. In the experiments, we let q in (7) be equal to 24 so that if a coefficient that has the nonzero bit higher than or equal to 24 will be viewed as a significant coefficient for watermark embedding or retrieval. The watermark sequence W_{b_s}, which takes value 1 or -1, is left-shifted by $22 + \alpha_{b_s}$ bits and then added to the selected coefficients to form watermarked



(a) (b) (c) (d)

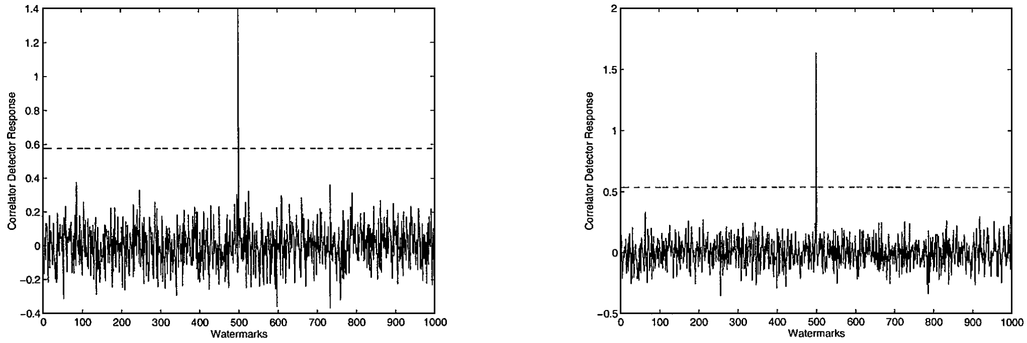
Figure 1. Original images v.s. compressed/watermarked images: (a) original "Bike", (b) watermarked "Bike" (PSNR:32.49 dB), (c) original "Woman" and (d) watermarked "Woman" (PSNR:33.09 dB). Both images are with size 2048 × 2560 and are compressed with 0.5 bpp.

coefficients as indicated in (9). The value of "extra LSB", which indicates the number of insignificant bit-planes in a coding block, is determined by EBCOT. We do not make any change on it. In watermark detection, our algorithm tends to generate a very high correlation response if the watermark exists. This allows us to set a higher threshold value to avoid any possibility of false alarm. The threshold scaling parameter τ in (14) is set to 7. If the progressive watermark detection is used, we choose τ to be 8.5. As mentioned in Section 3.3, we should define the minimum number η of the selected coefficients to claim the existence of watermark. In the experiment, η is chosen to be 500.

Two JPEG-2000 test images, "Bike" and "Woman", with size 2048 by 2560, as shown in Fig. 1(a) and (c), respectively, are used to demonstrate the invisibility of the embedded watermark. Because of the large size of the images, we encode them with a lower bit rate equal to 0.5 bpp so that they can be stored and transmitted efficiently. The SNR progressive mode is enabled to demonstrate the fully-embedded feature and progressive watermark detection. When the watermark function is disabled, the peak signal to noise ratio (PSNR) between the original and the compressed images of "Bike" and "Woman" are 33.54 dB and 33.70 dB, respectively. The PSNR values between the original and watermarked/compressed images are 32.49 dB and 33.09 dB, respectively. It is clear that the quality degradation resulting from watermark insertion is very little. The watermarked images are shown in Fig. 1(b) and (d).

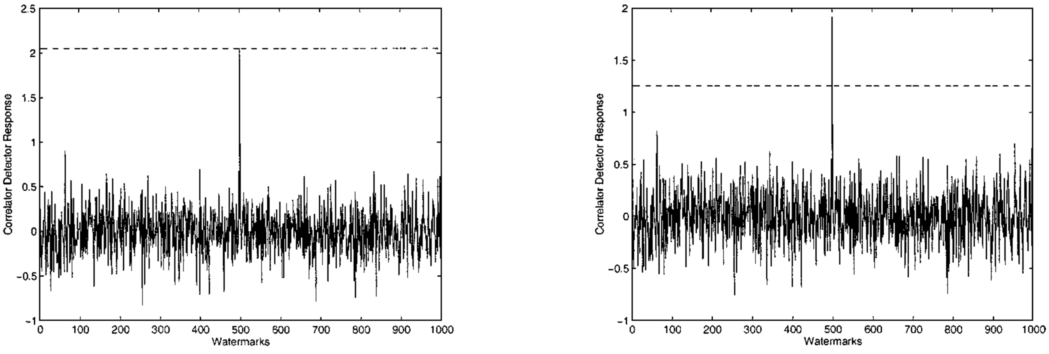
Next, we demonstrate the correlation response in the watermark detection process. Detection results are shown in Fig. 2. We can see clearly that there exists a peak with the watermark ID number 500 in both cases. The peak value of the correlation response is much larger than the threshold value T, which is shown as the break line in the figures. The responses of other watermarks are much lower than T. The target watermark can thus be determined unambiguously.

It usually takes a while to decode such large images completely from the entire bit-stream. Furthermore, watermark detection may involve a lot of coefficients so that the watermarking process is also time-consuming. We take the "Woman" image for example. There are over 400K coefficients selected for watermark detection. Actually, the number of the selected coefficients necessary for watermark detection can be reduced. We use progressive watermark detection by taking advantage of the fully-embedded feature of JPEG-2000 to speed up the watermarking process. There are two ways to demonstrate this property. The first one is to adopt progressive watermark detection. During the decoding process, whenever the correlation response is larger than the threshold T and the number of the selected coefficients is larger than η, we stop watermark detection and claim the existence of watermark. We test "Woman" image in progressive watermark detection. The result is shown in Fig. 3(a). The number of selected coefficients is 32,611. The value is still large because we set up a conservative threshold to avoid false alarm. In the second approach, we



(a) (b)

Figure 2. Watermark detection results for (a) "Bike" and (b) "Woman" with 1000 watermark sequences tested.



(a) (b)

Figure 3. Progressive watermark detection: (a) watermark detection by using the progressive mode and (b) watermark detection of the image decoded at a bit rate of 0.01 bpp.

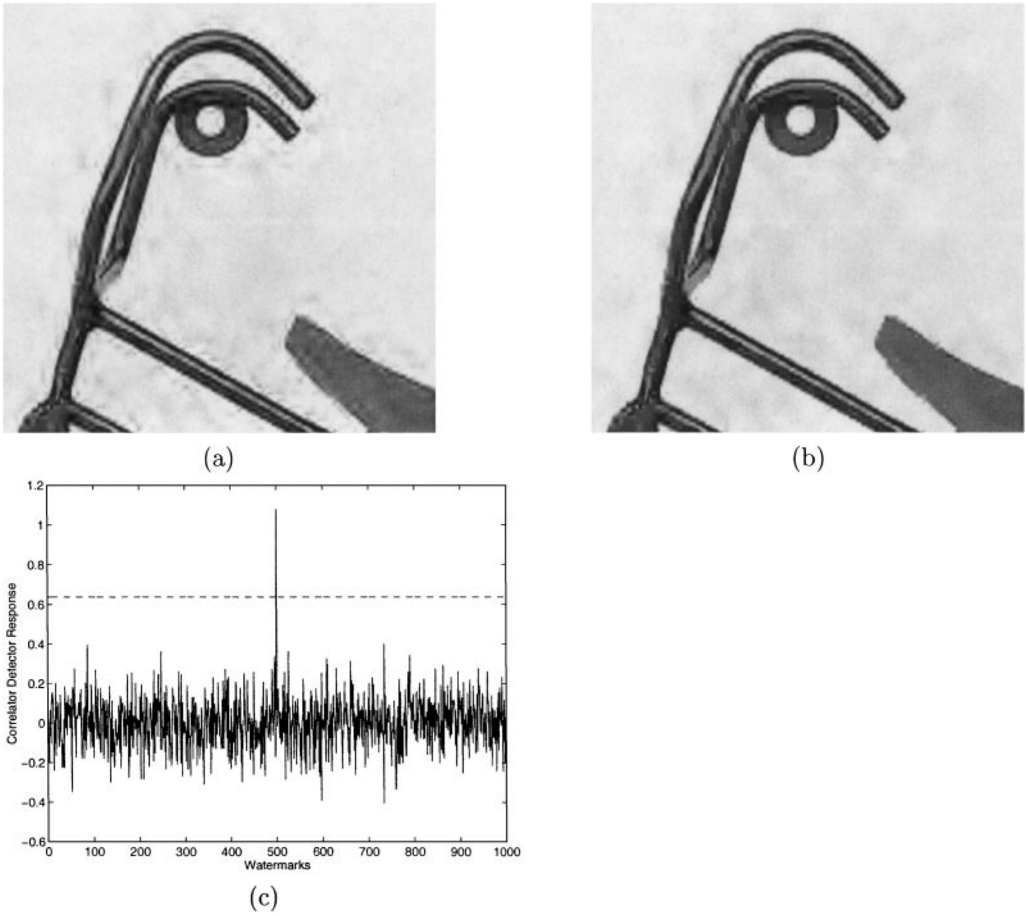


Figure 4. Postprocessing: (a) part of the “Bike” image before postprocessing, (b) part of the “Bike” image after postprocessing and (c) the watermark detection result.

do not use progressive detection but specify the decoding rate of the image. Fig. 3(b) shows the detection result when the image is decoded at a bit rate equal to 0.01 bpp. In this case, the number of selected coefficients is 6,511. The existence of watermark with ID number 500 is detected in both cases, yet the speed of watermark detection is greatly improved.

Although wavelet-based coding schemes have the advantages over the block DCT-based coding method in terms of the rate-distortion tradeoff performance, reconstructed images still suffer from various coding artifacts such as ringing effect, graininess, and blotchiness, etc. In JPEG-2000 VM, a postprocessing technique is used to reduce these artifacts so that the overall visual quality of decoded images can be improved substantially. Therefore, we apply the JPEG-2000 postprocessing technique [14, 18] to the decoded image and then test the performance of watermark detection. We decode the “Bike” image with 0.125 bpp and then feed it to the postprocessing stage with three iterations. The effect of the postprocessing can be understood by comparing the two images, before and after postprocessing. Fig. 4(a) and (b) show only part of the “Bike” image. The ringing artifact around the bike handler in Fig. 4(a) is greatly reduced in Fig. 4(b) so that the visual quality is improved. The watermark detection result demonstrated in Fig. 4(c) indicates that our watermarking scheme can be coupled very well with JPEG-2000 including the postprocessing procedure.

The next example is ROI watermarking. ROI coding is especially useful for large images. We use the other JPEG-2000 test image, “Aerial2” (2048 × 2048), as an example because application of ROI is important for aerophotography. We assign two rectangular regions which cover two constructions in image “Aerial2” as the desired ROI. We then enable the SNR progressive

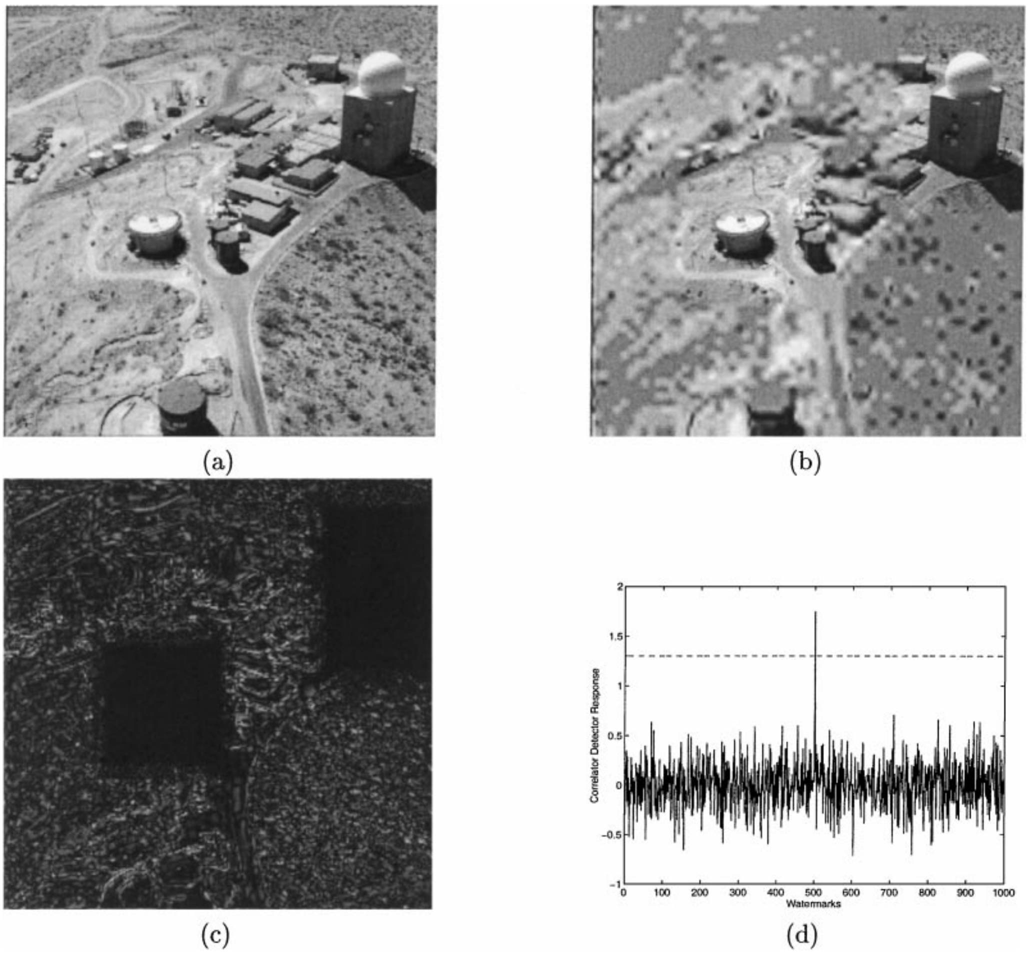


Figure 5. ROI watermarking: (a) the fully reconstructed image from ROI coding bitstream, (b) the decoded image with a bit rate of 0.4 bpp, (c) the spatial difference of these two images (the lighter the pixel is, the larger the difference and the two black rectangles are the assigned ROI) and (d) the watermark detection result.

mode to encode the image, and then decode it with a lower bit rate. We see that the two regions are well reconstructed while other parts of the image remain blurred. The ROI coding can be verified by the spatial difference of the transmitted image and the roughly decoded image as shown in Fig. 5(c) where the lighter the pixel is, the larger the difference between the two images. The detection result shown in Fig. 5(d) indicates that the proposed watermarking scheme matches the ROI feature of EBCOT, and the embedded watermark can be detected without any difficulty. Besides, with ROI watermarking, it is also possible to embed different watermark ID numbers into different objects in the same image. In this case, the watermark can be viewed as a function of data labeling, which may benefit content-based retrieval in the management of multimedia databases [19].

We then apply a series of attacks to show the robustness of the proposed watermarking schemes. First, we consider compression attacks, i.e. to compress the image with other schemes at low bit rates. The well-known DCT-based codec, JPEG, and the wavelet-based codec, SPIHT, are the two compression attacks under test. The attacked image is encoded into the EBCOT bitstream for watermark detection. Since perceptual loss caused by compression varies in different images, some images can be compressed with a higher compression ratio yet preserving good image quality. To verify that the watermark is robust against JPEG and SPIHT attacks, we choose to compress the image with

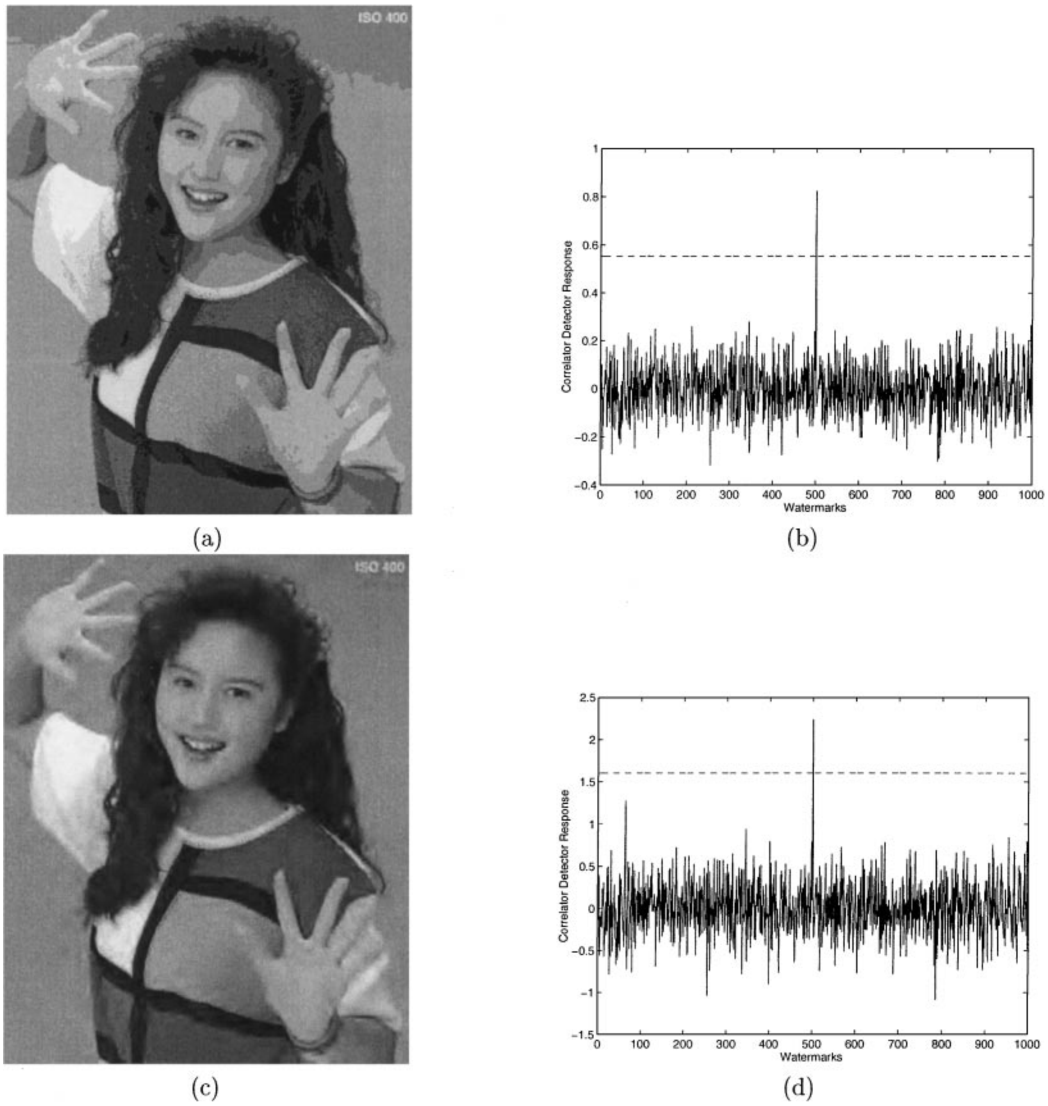
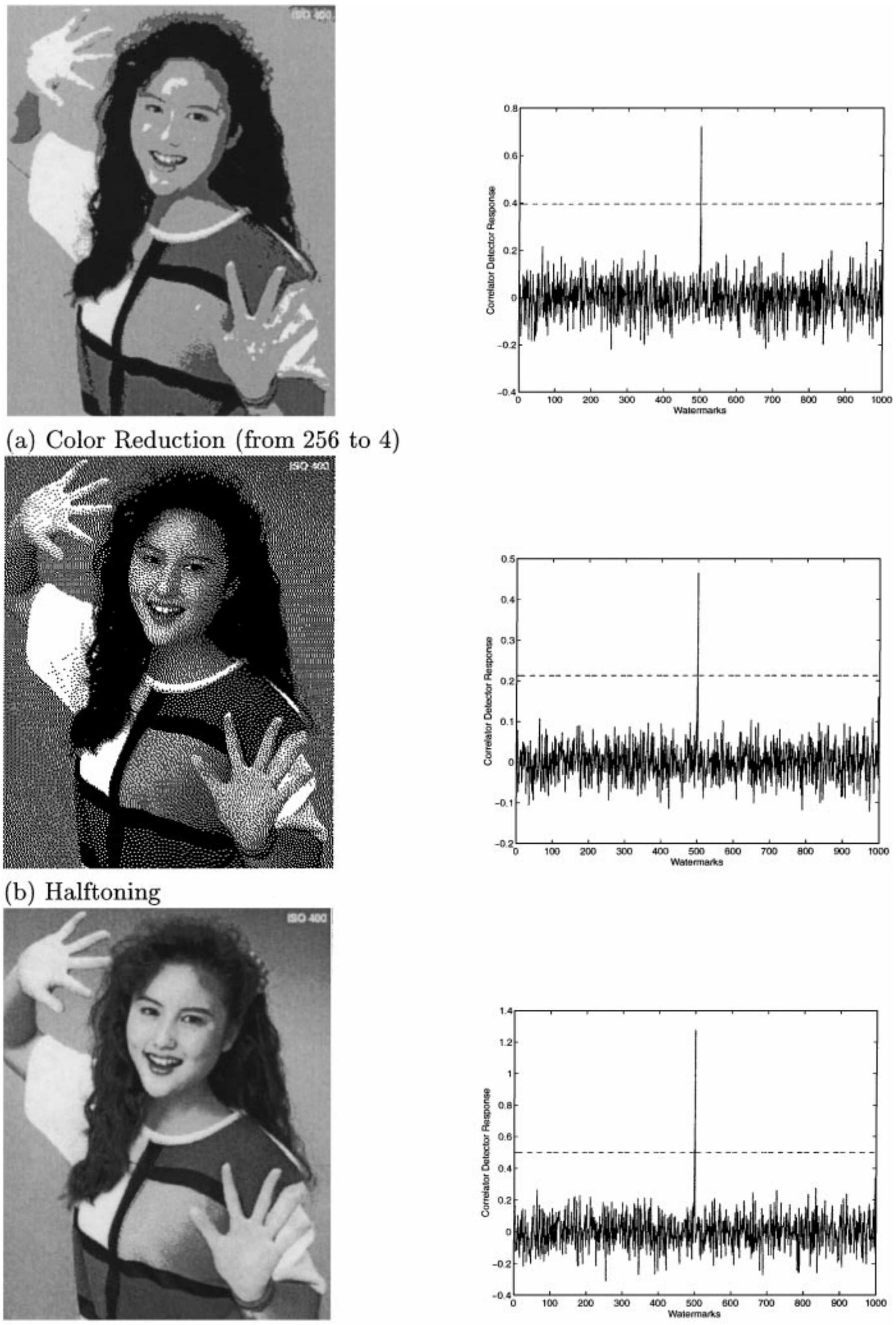


Figure 6. Compression attacks: (a) the watermarked “Woman” image compressed by JPEG with quality factor equal to 1 (PSNR: 22.61 dB), (b) the watermark detection result of the JPEG-attacked image, (c) the watermarked “Woman” image compressed with SPIHT at a bit rate of 0.005 bpp (PSNR: 22.50 dB) and (d) the watermark detection result of the SPIHT-attacked image.

extremely low bit rates. That is, the “Woman” image is compressed by JPEG with quality factor equal to 1 and by SPIHT with a bit rate of 0.005 bpp. The resulting images and detection results are shown in Fig. 6. In the JPEG-attacked image as shown in Fig. 6(a), a very serious blocking artifact appears since JPEG encodes an image block by block. The SPIHT-attacked image, as shown in Fig. 6(c), is blurred very much since only a few coefficients are used to reconstruct the whole image. The PSNR values of the JPEG- and SPIHT-attacked images are 22.61 dB and 22.50 dB, respectively. Although the two images are compressed to an unacceptable degree, the embedded watermark still survives well as shown in Fig. 6(b) and (d).

GIF is a popular file format for graphics. Unlike JPEG, the maximum number of colors that can be used for a picture is 256. For some images, annoying visual degradation may not be generated when they are converted to the GIF format. Thus, color reduction is another important type of attack that a watermark must resist. We have tested three kinds of color-related attacks. The first one is to reduce the number of colors from 256 to 4 for a gray-level image. The second one is image halftoning that is used quite often in FAX, newspapers, or other publications. The third one is histogram equalization which tends to stretch the dynamic range of the gray-level distribution of an image. Detection results of these attacks and attacked images are shown in Fig. 7. The distinctive peak of the correlation response indicates the survival of the watermark even though the attacked image is visually different from the original one.



(a) Color Reduction (from 256 to 4)

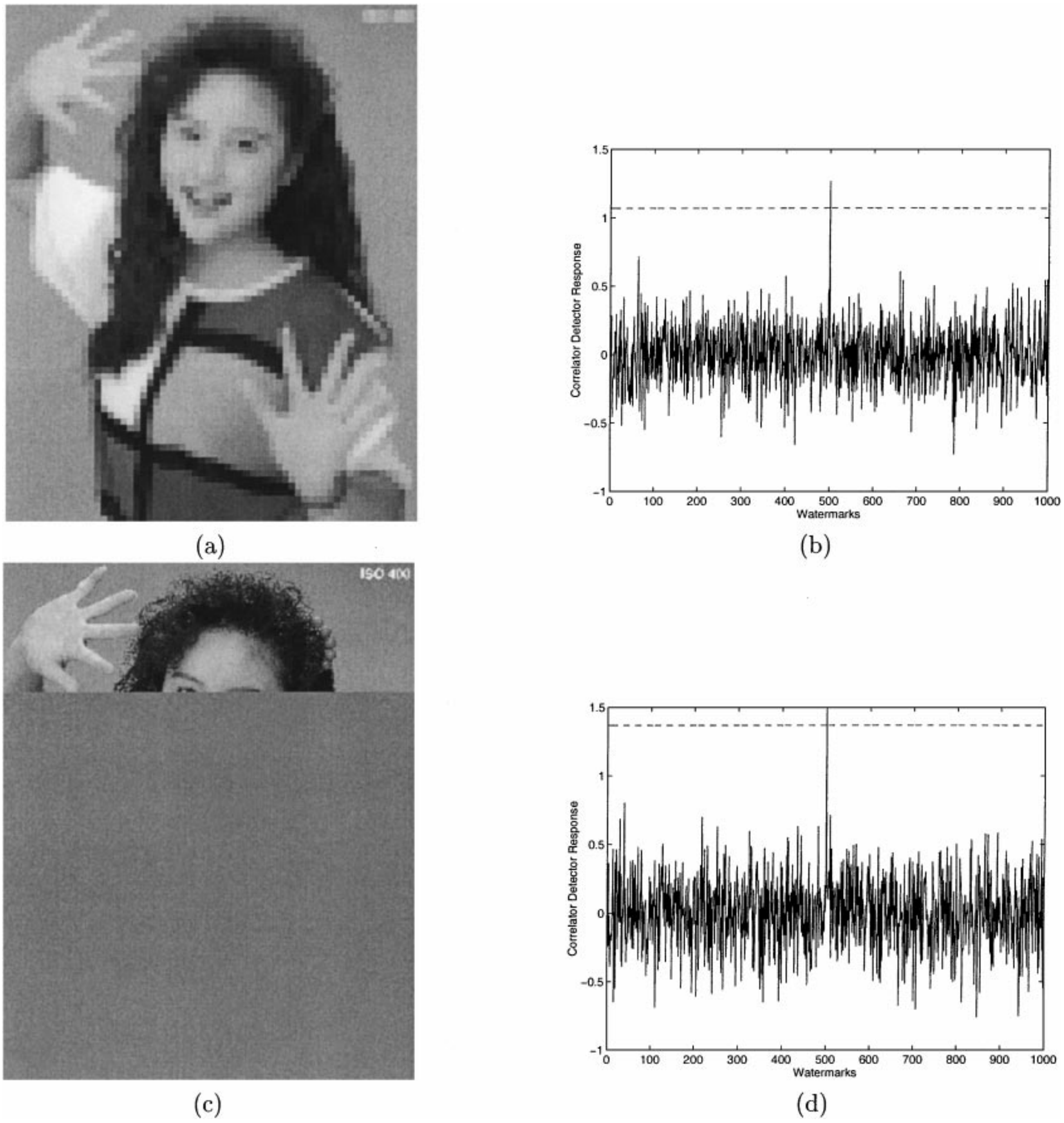
(b) Halftoning

(c) Histogram Equalization

Figure 7. Color-based attacks.

We then test the performance of our watermarking scheme when the protected image is resized or cropped. We reduce the watermarked “Woman” image from a size of 2048 × 2560 to a size of 256 × 320 and then interpolate it back to the original size, as shown in Fig. 8(a). The finer detail of the image is lost due to the resizing process. The detection result is shown in Fig. 8(b), which indicates the watermark survives after the resizing operation. We also crop the lower 3/4 of the image and fill it with a constant gray level of 128 as shown in Fig. 8(c) for the watermark robustness test. The result is shown in Fig. 8(d). Again, the watermark can be easily detected. However, the pre-registration process must be done before detecting watermark from these two attacked images so some information of the original image is required.

With the advances of graphical tools, users may edit an image with some artwork. Thus, it is interesting to test the robustness of the proposed watermarking scheme by using a popular editing tool, e.g. the



(a)

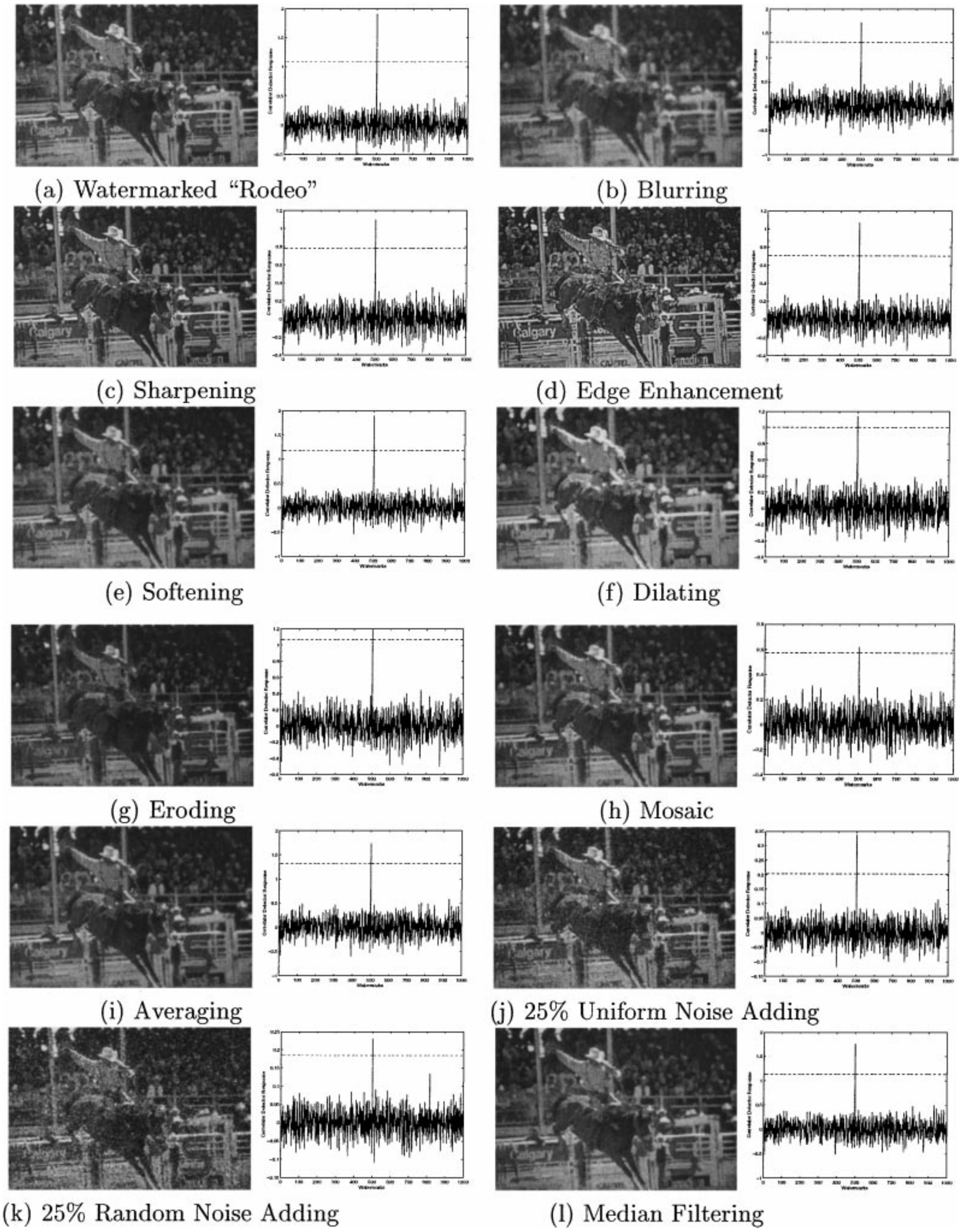
(b)

(c)

(d)

Figure 8. Robustness test against cropping and resizing attacks: (a) resizing “Woman” from 2048 × 2560 to 256 × 320 and then interpolating it back to 2048 × 2560, (b) the watermark detection result of the resized image, (c) cropping the lower 3/4 of the watermarked image and filling it with gray level 128, and (d) the watermark detection result of the cropped image.

Paint Shop Pro. In order to demonstrate the attack effects, we choose a smaller image, "Rodeo" provided by Corel Corporation. The image has size 768 by 512 and is compressed with bit-rate equal to 0.75 bpp. The PSNR between the original image and compressed/watermarked image is 39.83 dB. The attacks tested include blurring, sharpening, edge enhancement, eroding, dilating, median filtering, averaging, 25% random noise adding, 25% uniform noise adding, softening, and mosaic. The attacked images and detection results are shown in Fig. 9. We can see that the watermark is very robust under these attacks


(a) Watermarked "Rodeo"

(b) Blurring

(c) Sharpening

(d) Edge Enhancement

(e) Softening

(f) Dilating

(g) Eroding

(h) Mosaic

(i) Averaging

(j) 25% Uniform Noise Adding

(k) 25% Random Noise Adding

(l) Median Filtering

Figure 9. Extensive watermark testing on the watermarked "Rodeo" (768 × 512).

because the watermark is embedded in significant coefficients that usually remain stable after most image processing operations.

Finally, we would like to measure the false positive rate of the proposed system. As mentioned in Section 4, there are two cases in false positive detection: (1) the watermark is detected in an un-watermarked image and (2) the wrong watermark ID is detected. In the first case, i.e. the watermark is found in an un-watermarked image, the best method to measure the probability of false positive detection is to detect watermarks in numerous clear (un-watermarked) images by using the proposed watermarking scheme. This part is difficult to achieve due to the shortage of content sources. However, we believe that the Gaussian assumption should hold in this case so that the false positive rate should be covered by our analysis. The major concern of the accuracy of the Gaussian assumption comes from the second case, i.e. a wrong watermark is detected from a watermarked image with different ID. At this point, we would like to verify it by experimental data. To do so, we generated 100000 watermark sequences, constructed the watermarked image by embedding one of the watermark sequences and used 100000 watermarks (one correct watermark and the other 99999 incorrect watermarks) for detection. We counted the number of tested watermarks with a correlation response higher than the threshold value set according to the allowable false positive rate. We tested the false positive rate from 5×10^{-3} to 10^{-5}. We measured more points around 10^{-4} to 10^{-5} because these measurements may be more correct and important. The results are shown in Table 1. We see that the number of false detection matches pretty well with the predicted false detection based on the Gaussian assumption. Table 1 verifies the suitability of our analysis. By following this trend, we expect that the false positive analysis will work when a higher threshold value (with lower false positive rate) is set.

Table 1. The number of false positive detections measured from 100000 tested watermark sequences v.s. estimated number of false positive detections based on Gaussian assumption.

Error rate	Number of wrong watermark detected	Expected number of false detection
5×10^{-3}	525	500
10^{-3}	99	100
5×10^{-4}	55	50
10^{-4}	12	10
8×10^{-5}	10	8
5×10^{-5}	7	5
3×10^{-5}	3	3
10^{-5}	1	1

6. Conclusion

We presented an integrated approach to image compression and watermarking in this paper. EBCOT, which is the basis of JPEG-2000 VM, provides various features for different applications and the proposed watermarking method can be coupled with EBCOT to provide a way to assert copyright information for JPEG-2000 compressed images. The watermark sequence is embedded on significant wavelet coefficients so that it is robust against general signal processing attacks. The detection process does not resort to the help from the original image. Progressive watermark detection can be supported so that the watermark retrieval process can be done faster. ROI watermarking can also be achieved easily under the same framework. One may view this integrated scheme as a base-line watermarking scheme for copyright protection. Other variants can be easily derived based on this basic scheme. Future work will be to build an anti-geometric watermarking scheme upon this basic scheme to make the watermarking system more robust.

References

1. M.D. Swanson, M. Kobayashi, and A.H. Tewfik, "Multimedia Data Embedding and Watermarking Technologies," *Proceeding of IEEE*, vol. 86, no. 6, 1998, pp. 1064–1087.
2. F. Hartung and M. Kutter, "Multimedia Watermarking Techniques," *Proceeding of IEEE*, vol. 87, no. 7, 1999, pp. 1079–1107.
3. R.B. Wolfgang, C.I. Podilchuk, and E.J. Delp, "Perceptual Watermarking for Digital Images and Video," *Proceeding of IEEE*, vol. 87, no. 7, 1999, pp. 1108–1126.
4. G. Caronni, "Assuring Ownership Rights for Digital Images," in *Proc. VIS 95*, *Session Reliable IT Systems*, Vieweg, Germany, 1995, pp. 251–263.
5. K. Tanaka, Y. Nakamura, and K. Matsui,"Embedding Secret Information into a Dithered Multi-Level Image," in *Proc. 1990 IEEE Military Communications Conference*, Monterey, CA, 1990, pp. 216–220.
6. R.G. van Schyndel, A.Z. Tirkel, and C.F. Osborne, "A Digital Watermark," in *Proc. 1994 IEEE Int. Conf. on Image Processing(ICIP)*, Austin, TX, 1994, vol. 2, pp. 86–90.
7. W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for Data Hiding," in *IBM Syst. Journal*, 1996, vol. 35, no. 3/4, pp. 313–316.

8. A. Piva, M. Barni, F. Bartolini, and V. Cappellini, "DCT-Based Watermark Recovering Without Resorting to the Uncorrupted Original Image," in *Proc. 1997 IEEE Int. Conf. on Image Processing(ICIP)*, Santa Barbara, CA, 1997, vol. 1, pp. 520–523.
9. I.J. Cox, F.T. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Images, Audio and Video," in *Proc. 1996 IEEE Int. Conf. on Image Processing(ICIP)*, Lausanne, Switzerland, 1996, pp. 243–246.
10. X.G. Xia, C.G. Boncelet, and G.R. Arce, "A Multisolution Watermark for Digital Images," in *Proc. 1997 IEEE Int. Cont. on Image Processing(ICIP)*, Santa Barbara, CA, vol. 1, 1997, pp. 548–551.
11. C.I. Podilchuk and W. Zeng, "Image-Adaptive Watermarking Using Visual Models," in *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 4, 1998, pp. 525–539.
12. H.-J. Wang, P.-C. Su, and C.-C.J. Kuo, "Wavelet Based Blind Watermark Retrieval Technique," in *1998 SPIE Photonics East - Symposium on Voice, Video, and Data Communications*, Boston, MA, 1998.
13. C. Chrysafis, D. Taubman, and A. Drukarev, "Overview of JPEG2000," in *Proc. 1999 PICS 52nd Annual Conference*, Savannah, GA, 1999, pp. 333–338.
14. JPEG 2000 Document, "JPEG 2000 Verification Model 5.0 (Technical description)," ISO/IEC JTC1/SC29/WG1 N1409, July 1999.
15. A. Said and W.A. Pearlman, "A New, Fast, and Efficient Image Codec Based on Set Partitioning in Hierarchical Trees," in *IEEE Trans. on Circuits and Systems for Video Technology*, vol. 6, 1996, pp. 243–250 .
16. J. Shapiro, "Embedded Image Coding Using Zerotrees of Wavelet Coefficients," in *IEEE Trans. on Signal Processing*, vol. 4, 1993, pp. 3445–3462.
17. H. Stark and J.W. Woods, *Probability, Random Processes and Estimation Theory for Engineers*, Englewood Cliffs, NJ: Prentice Hall, 1994.
18. M.-Y. Shen and C.-C.J. Kuo, "Artifact Reduction in Low Bit Rate Wavelet Coding with Robust Nonlinear Filtering," in *Proc. 1998 IEEE Second Workshop on Multimedia Signal Processing*, Redondo Beach, CA, 1998, pp. 480–485.
19. P.-C. Su, H.-J.M. Wang, and C.-C.J. Kuo, "Digital Image Watermarking in Regions of Interest," in *Proc. 1999 PICS 52nd Annual Conference*, Savannah, GA, 1999, pp. 295–300.

Mr. Po-Chyi Su was born in Taipei, Taiwan in 1973. He received the B.S. degree from the National Taiwan University, Taipei, Taiwan, in 1995 and M.S. degree from the University of Southern California, Los Angeles, in 1997, both in Electrical Engineering. He is currently pursuing the Ph.D. degree at the Signal and Image Processing Institute, University of Southern California. His research interests include digital watermarking, data compression and detection theory.
pochyisu@sipi.usc.edu

Dr. Houng-Jyh Mike Wang received the M.S. and Ph.D. degrees from the University of Southern California, Los Angeles, in 1994 and 1998 respectively, all in Electrical Engineering. He has authored more than 20 technical publications in international conferences and journals. Dr. Wang's research interests include multimedia compression, digital watermarking, cryptography, and signal detection.

Dr. Wang worked at the Chung-Shan Institute of Science and Technology (CSIST), a research institute of the Department of National Defense in Taiwan, from 1988 to 1993, where he obtained the Award of Excellent Staff of CSIST. He is the National Honorary Civilian of Taiwan.

He is a member of the Institute of Electrical and Electronics Engineering (IEEE), the International Society for Optical Engineering (SPIE) and the International Standard Organization-Joint Picture Expert Group (ISO-JPEG). He is the vice president and the chief of technology office in Media Fair, Inc., USA and working on the Internet multimedia researches and applications.
mikewang@mediafair.com

Dr. C.-C. Jay Kuo received the B.S. degree from the National Taiwan University, Taipei, in 1980 and the M.S. and

Ph.D. degrees from the Massachusetts Institute of Technology, Cambridge, in 1985 and 1987, respectively, all in Electrical Engineering.

Dr. Kuo was Computational and Applied Mathematics (CAM) Research Assistant Professor in the Department of Mathematics at the University of California, Los Angeles, from October 1987 to December 1988. Since January 1989, he has been with the Department of Electrical Engineering-Systems and the Signal and Image Processing Insitute at the University of Southern California, where he currently has a joint appointment as Professor of Electrical Engineering and Mathematics. His research interests are in the areas of digital signal and image processing, audio and video coding, wavelet theory and applications, multimedia technologies and large-scale scientific computing. He has authored around 400 technical publications in international conferences and journals.

Dr. Kuo is a member of SIAM, ACM, a Fellow of IEEE and SPIE. He is the Editor-in-Chief for the journal of Visual Communication and Image Representation, and served as Associate Editor for IEEE Transaction on Image Processing in 1995–98 and IEEE Transaction on Circuits and Systems for Video Technology in 1995–1997. Dr. Kuo received the National Science Foundation Young Investigator Award (NYI) and Presidential Faculty Fellow (PFF) Award in 1992 and 1993, respectively.
cckuo@sipi.usc.edu