Available at www.ComputerScienceWeb.com
POWERED BY SCIENCE DIRECT®

ELSEVIER

Information Sciences 151 (2003) 93–105

INFORMATION SCIENCES
AN INTERNATIONAL JOURNAL

www.elsevier.com/locate/ins

A comparative study of digital watermarking in JPEG and JPEG 2000 environments

M.A. Suhail [a], M.S. Obaidat [b,*], S.S. Ipson [b], B. Sadoun [c]

[a] *Monmouth University, UK*
[b] *University of Bradford, UK*
[c] *Al-Balqa' Applied University (BAU), Jordan*

Received 1 June 2001; accepted 27 April 2002

Abstract

JPEG 2000 is a new compression technology that achieves very high compression rate and maintains visual quality. Digital watermarking techniques have been developed to protect the copyright of media signals. The goal of this paper is to put into perspective joint photographic experts group (JPEG) and JPEG 2000 concepts a long with watermarking principle. It provides evaluation of the compatibility aspects of JPEG 2000 versus JPEG standard with watermarking. Various experiments have been conducted to compare the performance of both standards under various conditions. An outlook on the future of digital image watermarking within JPEG 2000 is introduced.

Keywords: JPEG; JPEG 2000; Watermarking; Image processing; DCT; DWT; Image compression

1. Introduction

Many watermarking schemes have been suggested for images and some for audio and video streams. A large number of these schemes address the problems

* Corresponding author. Address: Department of Computer Science, Monmouth University, W. Long Branch, NJ 07764, USA. Tel.: +1-732-571-4482; fax: +1-732-263-5202.
E-mail address: obaidat@monmouth.edu (M.S. Obaidat).

0020-0255/02/$ - see front matter
doi:10.1016/S0020-0255(02)00291-8

of implementing invisible watermarks. Basic watermarking concepts are discussed in [1,2]. Researchers define a digital watermark as identification code carrying information (an author's signature, a company's log, etc.) about the copyright owner, the creator of the work, the authorized consumer and so on. It is permanently embedded into digital data for copyright protection and may be used for checking whether the data have been modified. Visible and invisible watermarking are the two categories of digital watermarking. The concept of the visible watermarking is very simple; it is analogous to stamping a mark on a paper. The data is said to be digitally stamped. An example of visible watermarking is seen in television channels when the station's logo is visibly superimposed in the corner of the screen. Invisible watermarking, on the other hand, is a far more complex concept. It is most often used to identify copyright data, like author, distributor, etc.

On the other hand, image compression of digital images is the process of reducing the size of an image while retaining the highest possible visual quality. JPEG is the very well known ISO/ITU-T standard for image compression. Several modes are defined in JPEG [3]. It is released in late 1980s. JPEG 2000 is a new compression technology that achieves very high compression rate and maintains visual quality. The JPEG 2000 is issued now to become an International Standard (IS) [3,4].

This paper will give an answer to a common question about the robustness performance of the watermarking techniques against attacks of JPEG and JPEG 2000. An outlook on the future of digital image watermarking within JPEG 2000 will be given. Section 2 introduces an overview of watermarking concept. Section 3 provides a background about JPEG and JPEG 2000. Also, it compares both standards in terms of technology, performance, and applications. Section 4 presents the experimental work and the results. Section 5 provides a look into the future of image coding and data security. Section 4 concludes this paper.

2. Watermarking concept and techniques

2.1. Watermarking applications and properties

The two major applications for watermarking are protecting copyrights and authenticating photographs. The main reason for protecting copyrights is to prevent image piracy when the provider distributes the image on the Internet [2]. One method used to authenticate digital images is to embed a digital watermark that breaks or changes as the image is tampered with. This informs the authenticator that the image has been manipulated.

Watermarking techniques that are intended to be widely used must satisfy several requirements. The type of application decides which watermarking

technique to be used. However, three requirements have been found to be common to most practical applications. These are robustness, invisibility and delectability. Some of watermarking requirements competes with each other. Also other requirements [1,2] may be significant.

2.2. Digital watermarking approaches

There are two main generations of watermarking: first generation watermarking and second generation watermarking [5]. Both approaches can be achieved via spatial or transform techniques such as discrete cosine transform (DCT) and discrete wavelet transform (DWT). First generation watermarking (1GW) methods have been mainly focused on applying the watermarking on the entire image/video domain. However, this approach is not compatible with novel approaches for still image and video compression. JPEG 2000 and MPEG4/7 standards are the new techniques for image and video compression. They are region- or object-based, as can be seen in the compression process. By contrast, second generation watermarking (2GW) was developed in order to increase the robustness and invisibility and to overcome the 1GW weakness. The 2GW takes into account region, boundary and object characteristics. They give additional advantages in terms of detection and recovery from geometric attacks as compared to the 1GW [5]. This can be achieved by exploiting salient region or object features and characteristics of the image. Such watermarking methods may present additional advantages in terms of detection and recovery from geometric attacks [6]. They may be designed so that selective robustness to different classes of attacks is obtained. This will improve the watermark flexibility.

3. Joint photographic experts group standards

This section will introduce some discussion about JPEG and JPEG 2000 standards. JPEG is the most widely used standard. However, JPEG 2000 is a new standard, which will appear in various applications in the near future. It represents the state-of-the-art in image coding. This section will give an explanation of the principles behind the algorithms used in both standards.

3.1. JPEG standard

JPEG is the very well known ISO/ITU-T standard. Several modes are defined in JPEG. Baseline and lossless modes are the most popular ones [7,8]. It was released in late 1980s.

The baseline mode supports lossy coding. The lossless mode is created for lossless coding only. In the baseline mode, the image is subdivided into pixels of size 8×8 (64 pixels). Then, each pixel of this subimage is level shifted by

subtracting the quantity $2^{(n-1)}$. The DCT of each block is then computed. After that, the block is quantized and reordered using zig-zag pattern to form 1-D sequence. The AC coefficients of this 1-D sequence are coded using a variable-length code. The DC coefficient is coded relative to the DC coefficient of the previous subimage. An excellent background and examples of this are given in [8]. The transformation and normalization process produces a large number of zero-valued coefficients. These coefficients that remain after the normalization process will be discarded. Then, entropy coded with Huffman coding is performed. The quantization step size for each of the 64 DCT coefficients is specified in a quantization table, which remains the same for all blocks. To decompress a JPEG compressed subimage, the decoder must first recreate the normalized transform coefficients that led to the compressed bit stream. Because a Huffman coded binary sequence is instantaneous and uniquely decodable, this step is easily accomplished using a lookup table. Any difference between the original and reconstructed subimage is the result of the lossy nature of the JPEG compression and decompression processes [3,8].

Fig. 1 shows a JPEG block diagram for lossy compression. However, the lossless mode is based on a completely different algorithm. It relies on a predictive scheme which is based on the nearest three causal neighbors and seven different predictors are defined (the same one is used for all samples). The prediction error is entropy coded with Huffman coding. The other modes defined in JPEG provide variants of the previous two basic modes. This is like progressive bit streams and arithmetic entropy coding [8,9].

3.2. JPEG 2000 standard

JPEG 2000 was also developed by the International Standards Organization (ISO). It is the new image compression standard. The JPEG 2000 code handles both lossy and lossless compression using the same transform-based framework [4]. It is based on the DWT. The latter provides a number of benefits over

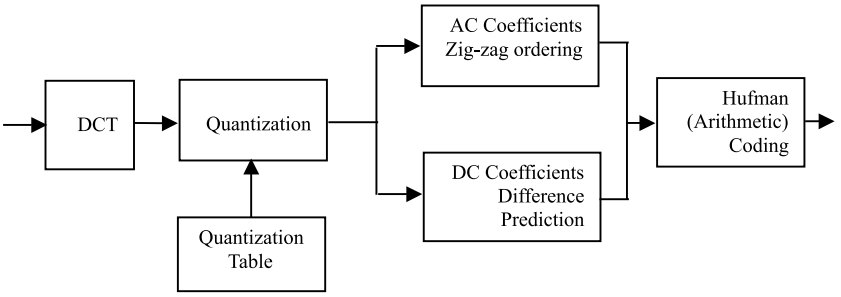

Fig. 1. Block diagram of JPEG algorithm (lossy mode encoder).

the previous JPEG compression techniques that are based on DCT. DWT encodes the image in a continuous stream. So, this will avoid the tendency toward visible artifacts that sometimes result from DCT's division of an image into discrete compression blocks [3,4]. Also, its model relies on scalar quantization, context modeling, and arithmetic coding and post-compression rate allocation. The DWT used in JPEG 2000 is dyadic. It can be performed with a reversible filter (Le Gall (5,3) taps filter 9) [9], which provides for lossless coding. Also, a non-reversible filters (Daubechies (9,7) taps BI-orthogonal one 10) can be used for higher compression to do lossy compression but not lossless. The quantizer follows an embedded dead-zone scalar approach. It is independent for each subband. Each subband is divided into block (64×64). These subbands are entropy coded using context modeling and bit-plane arithmetic coding. The coded data is organized in layers. They are quality levels, using the post-compression rate allocation and output to the code-stream in packets [3]. The basic scheme of JPEG 2000 can be seen in Fig. 2. The above is part 1 description of JPEG 2000 standard, which defines the core system. Part 2 is still in preparation [9].

3.2.1. JPEG 2000 functionality and features

JPEG 2000 includes many-advanced features and supports a number of functionalities. Many of these functionalities are inherent from the algorithm itself [4,9,10]. These feature and functionalities are:

- High compression ratio.
- Lossy and lossless compression.
- Progressive recovery by fidelity or resolution.
- Visual (fixed and progressive) coding.
- Good error resilience.
- Arbitrarily shaped region of interest coding.
- Random access to specific regions in an image.
- Security
- Multiple component images
- Palletized images
- It also can support images in width and height from 1 up to $2^{32}-1$.

3.2.2. JPEG 2000 applications

The following are examples of potential application that will benefit directly from JPEG 2000; see Table 1.

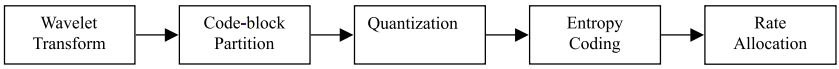

Fig. 2. Basic encoding scheme of JPEG 2000.

Table 1
Examples of potential applications of JPEG 2000

Document imaging	Digital photography
Scanning	Color facsimile
Medical imaging	Internet
Web browsing	E-Commerce
Image archiving	Remote sensing
Digital library	Mobile

3.3. Comparison between JPEG and JPEG 2000

In this section, we will present some comparative experimental results to show the difference between JPEG and JPEG 2000. A boat image is compressed at very low bit rates using JPEG, at the same time, the image is compressed to the same degree using JPEG 2000, see Figs. 3–5. The compression ratio is 30:1. The images compressed using JPEG degrades significantly. Also, the images compressed using the JPEG 2000 algorithms and at the same compression rates do not suffer from the same degree of degradation as JPEG images. The noise artifacts, such as blockiness, that are clearly evident with JPEG are reduced with JPEG 2000. At very high compression rates the image content is easily recognizable with JPEG 2000 but not with JPEG. This shows that JPEG 2000 outperforms JPEG at higher compression ratios. Table 2 shows the main difference between the JPEG and JPEG 2000.

Fig. 3. Original boat image.

Fig. 4. Compressed image using JPEG standard.

Fig. 5. Compressed image using JPEG 2000 with same compression ratio as in Fig. 4.

4. Experimental work

4.1. DCT-based watermarking algorithms

The two-dimensional forward DCT kernel is used here. It is defined as

Table 2
Major differences between JPEG and JPEG 2000

Standard	Technologies and features	Applications
JPEG by ISO/IEC	DCT	Internet imaging
	Perceptual quantization	Digital photography
	Zig-zag reordering	Image and video editing
	Huffman coding	
	Arithmetic coding	
JPEG 2000 by ISO/IEC	DWT	Digital libraries
	New functionalities	E-Commerce
	Reversible integer-to-integer and nonreversible real-to-real DWT	Internet
	ROI	Digital photography
	Error resilience	Image and video editing
	Progression orders	Printing
	Lossy to lossless in one system	Medical imaging
	Better compression at low bit-rates	Mobile
	Better at compound images and graphics (palletized)	Color facsimile
		Satellite imaging
		Scanning
		Remote sensing

$$g(x,y,0,0) = \frac{1}{N}, \tag{4a}$$

$$g(x,y,u,v) = \frac{1}{2N^3}[\cos(2x+1)u\pi][\cos(2y+1)v\pi] \tag{4b}$$

for $x,\ y = 0,1,\ldots,N-1$, and $u,v = 1,2,\ldots,N-1$ [8]. The DCT scheme relies on some of the ideas proposed by Cox et al. [11]. They propose a watermark that consists of a sequence of randomly generated real numbers. These numbers have a normal distribution with zero mean and unity variance:

$$W = \{w_1, w_2, \ldots, w_N\}. \tag{5}$$

Then, the DCT of the whole image is computed. The DCT coefficients are chosen to be watermarked. After that, the watermark is added by modifying the DCT coefficients:

$$C = \{c_1, c_2, \ldots, c_N\}. \tag{6}$$

According to

$$c_i' = c_i + \alpha c_i w_i, \tag{7}$$

where $i = 1,2,\ldots,N$, and $\alpha = 0.1$. If we denote the original image by I_0 and the watermarked possibly distorted image I_w^*, then, a possibly corrupted watermark W^* can be extracted. Reversing the embedding procedure can do this extracting. This is done using the inverse DCT.

The watermark is embedded in subimages of the image. Therefore, the $N \times M$ image I is subdivided into pixels of size 16×16 (256 pixels). The DCT of the block is then computed. After that, the DCT coefficients are reordered into a zig-zag scan. This reordering is similar to the JPEG compression algorithm [8]. Then the coefficients in the zig-zag ordering of the DCT spectrum are selected. These selected coefficients are modified, according to (6), where c_i is the original DCT coefficient, w_i is the watermark coefficient and c_i, w is the modified coefficient. To tune the watermark energy, the term α is used. The higher the α value, the more robust and visible the watermark. Finally, we need to reverse the above procedure to get our watermarked image. The modified DCT coefficients are reinserted in the zig-zag scan. Then, the inverse DCT is applied. Finally, the blocks are merged to obtain the watermarked image I_w.

4.2. DWT-based watermarking algorithms

A DWT-based approach is used. The image (I) and watermark (W) are transformed into the DWT. The host image is transformed into three levels ($L = 3$) of DWT. Each of these levels (l:1 to 3) will produce a sequence of three levels detail images ($j = 1, 2, 3$). Also, a gross approximation of the image at the coarsest resolution level will be generated at level three ($l = 3$ and $j = 4$) [12]. The resulting coefficients are then watermarked according to

$$Iw_{j,l}(x, y) = I_{j,l}(x, y) + \beta(f_1, f_2) W_{j,1}(x, y),$$

where $I(x, y)$ is the DWT of the host image, $Iw(x, y)$ is the watermarked image, W is the watermark, l is the DWT resolution level and j is the DWT frequency orientation. The watermarking algorithm is adaptive by making use of human visual system (HVS) characteristics, which increase robustness and invisibility at the same time. The HVS $[\beta(f_1, f_2)]$ can be represented by [13,14]:

$$\beta(f_1, f_2) = 5.05 e^{-0.178(f_1+f_2)} \left(e^{0.1(f_1+f_2)} - 1\right),$$

where, f_1 andf_2 are the spatial frequencies (cycles/visual angle). However, the watermark will be spatially localized at high-resolution levels of the host image. By this, the watermark will be more robust. At the end, the inverse DWT is applied to form the watermarked image. Fig. 3 shows the block diagram of the proposed method.

4.3. Watermarking detection

The embedding watermark function makes small modifications to I_{orig}. For example, if $W = (w1, w2, \ldots) = (1, 0, 1, 1, 0, \ldots)$, the embedding operation may involve adding or subtracting a small quantity a from each pixel or sample of I_{orig} when w_i is 1 or 0, respectively. During the second stage of the watermarking system, the detecting function D uses knowledge of W, and possibly I_{orig}, to extract a sequence W^* from the signal R undergoing testing:

$$D(R, I_{\text{orig}}) = W^*.$$

The signal R may be the watermarked signal I_w. It may be a distorted version of I_w resulting from attempts to remove the watermark, or it may be an unrelated signal. The extracted sequence W^* is compared with the watermark W to determine whether R is watermarked. The comparison is usually based on a correlation measure ρ, and a threshold γ_0 used to make the binary decision (Z) on whether the signal is watermarked or not. To check the similarity between W (the embedded watermark), and W^* (the extracted watermark), the correlation measure between them can be found using

$$\rho(W, W^*) = \frac{W \cdot W^*}{\sqrt{W^* \cdot W^*}},$$

where $W \cdot W^*$ is the scalar product between these two vectors. However the decision function is

$$Z(W^*, W) = \begin{cases} 1, & c \geqslant \gamma_0 \\ 0 & \text{otherwise,} \end{cases}$$

where c is the value of the correlation and γ_0 is a threshold. A '1' indicates a watermark has been detected, while a '0' indicates that a watermark has not been detected. In other words, if W and W^* are sufficiently correlated (greater than some threshold γ_0), the signal R has been verified to contain the watermark, which confirms the author's ownership rights to the signal. Otherwise, the owner of the watermark W has no rights over the signal R. The detection threshold γ_0 is considered empirically to be 0.1 in our experiments. This was decided based on the examination of the correlation of random sequences.

4.4. Results and discussion

Figs. 6–9 show the experimental results. DCT- and wavelet-based watermarking algorithms described in this paper are implemented in Matlab environment. Different watermarked images are exposed to JPEG and JPEG 2000 for different compression ratios. The results are recorded in Table 3, which shows the correlation coefficients of the watermarking detector after compression using JPEG and JPEG 2000. The compression ratio was varied from 5 to 45. The recorded data is for wavelet and DCT techniques.

Fig. 6 shows a DCT-based watermarking algorithms exposed to both JPEG and JPEG 2000. It is clear from the figure that the robustness of the watermarking algorithm against JPEG is better than JPEG 2000. On the other hand, the wavelet-based watermarking technique is less robust when exposed to JPEG attack than when exposed to JPEG 2000. This is shown in Fig. 7. On another display of the recorded data, Fig. 8 shows the results of JPEG attacks on DCT and wavelet watermarking techniques. The robustness of DCT algorithm compared to wavelet algorithms is better. However, the robustness of wavelet

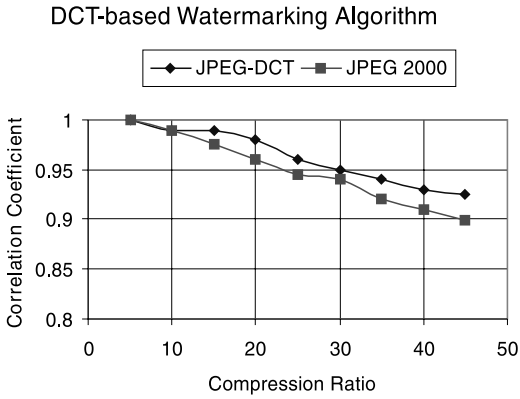

Fig. 6. Comparison between JPEG and JPEG 2000 on a DCT-based watermarking technique.

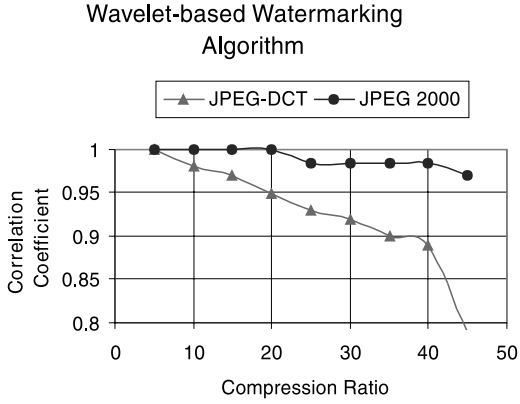

Fig. 7. Comparison between JPEG and JPEG 2000 on a wavelet-based watermarking technique.

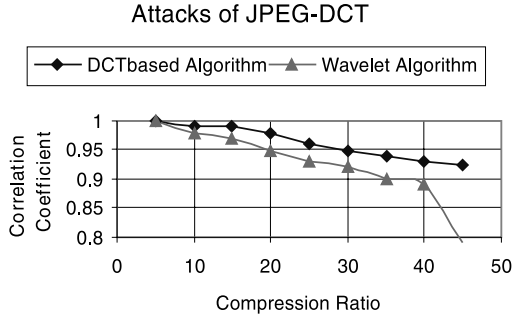

Fig. 8. Results of JPEG-DCT attacks on DCT and wavelet techniques.

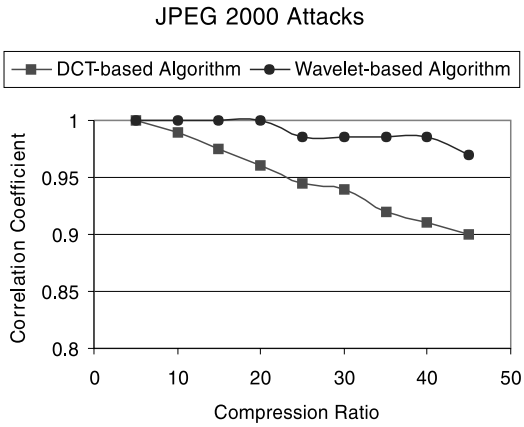

Fig. 9. Results of JPEG 2000 attacks on DCT and wavelet techniques.

Table 3
Experimental results

Tech	DCT-based		Wavelet-based	
CR	JPEG-DCT	JPEG 2K	JPEG-DCT	JPEG 2K
5	1	1	1	1
10	0.99	0.99	0.98	1
15	0.99	0.975	0.97	1
20	0.98	0.960	0.95	1
25	0.96	0.945	0.93	0.985
30	0.95	0.940	0.92	0.985
35	0.94	0.92	0.90	0.985
40	0.93	0.91	0.89	0.985
45	0.925	0.9	0.79	0.970

algorithm against JPEG 2000 outperform the same attack when applied on DCT algorithm. One can conclude from this that the compatibly issues between the watermarking algorithms and the compression standard may play an important role in the robustness of the watermarking. When the images are compressed at a very high compression ratio, the images compressed using JPEG-DCT degrades significantly. However, the images compressed using the JPEG 2000 algorithms and at the same compression rates do not suffer from the same degree of degradation. Also, the study needs more investigation on wide range of watermarking algorithms either using DCT or wavelet domain to generalize this result.

5. Concluding remarks

The goal of this paper is to evaluate the performance of DCT and wavelet watermarking techniques against JPEG and JPEG 2000 attacks. The paper

shows that there are compatibly issues between the robustness of the watermarking algorithms and the compression standards. More investigation is needed on a wide range of DCT- and wavelet-based watermarking algorithms to investigate the generalization of this conclusion.

There was a discussion about how and whether watermarking should form part of the standard during the standardization process of JPEG 2000. The requirements regarding security have been identified in the framework of JPEG 2000. However, there has been neither in depth clarification nor a harmonized effort to address watermarking issues. The initial drafts of the JPEG 2000 standard did not mention the issue of watermarking. However, there is a plan to examine how watermarking might be best applied within the JPEG 2000. Therefore the potential is that watermarking technology will be used in conjunction with JPEG 2000.

References

[1] Busch, Christopher, Olfgang Funk, Stephen Wolthusen, Digital watermarking: from concepts to real-time video applications, IEEE Computer Graphics and Applications 19 (1) (1999) 25–35.
[2] F. Hartung, M. Kutter, Multimedia watermarking techniques, Proceedings of the IEEE 87 (7) (1999) 1079–1106.
[3] D. Santa-Cruz, T. Ebrahimi, A study of JPEG 2000 still image coding versus other standards, in: Proceeding of the X European Signal Processing Conference (EUSIPCO), Tampere, Finland, September 5–8, vol. 2, 2000, pp. 673–676.
[4] ISO/IEC JTC 1/SC 29/WG 1, ISO/IEC FCD 15444-1: Information technology JPEG 2000 image coding system: core coding system, WG 1 N 1646, pp. 1–205, March 2000. Refer to: http://www.jpeg.org/FCD15444-1.htm.
[5] http://www.tsi.enst.fr/~maitre/tatouage//icip2000.html.
[6] M. Kutter, S.K. Bhattacharjee, T. Ebrahimi, Towards second generation watermarking schemes, in: Proceedings of the International Conference on Image Processing, 1999, ICIP 99, 1 (October) (1999) 320–323.
[7] http://www.jpeg.org/.
[8] R. Gonalez, P. Wintz, Digital Image Processing, second ed., Addison Wesley, Reading, MA, 1987.
[9] D. Santa-Cruz, T. Ebrahimi, J. Askelöf, M. Larsson, C. Christopoulos, JPEG 2000 still image coding versus other standards, in: Proceedings of the SPIE's 45th annual meeting, Applications of Digital Image Processing XXIII, V 4115, San Diego, California, July 30–August 4, 2000, pp. 1–10.
[10] D. Santa-Cruz, T. Ebrahimi, An analytical study of JPEG 2000 functionalities, in: Proceedings of the IEEE International Conference on Image Processing (ICIP), vol. 2, Vancouver, Canada, September 10–13, 2000, pp. 49–52.
[11] Cox, J. Kilian, T. Leighton, T. Shamoon, Secure Spread Spectrum Watermarking for Multimedia. Tech. Rep. 95-10, NEC Research Institute, 1995.
[12] C. Burrus, H. Guo, Introduction to Wavelets and Wavelet Transforms: A Primer, first ed., Prentice-Hall, Englewood Cliffs, NJ, 1998.
[13] M. Levine, Vision in Man and Machine, McGraw-Hill, New York, 1985.
[14] R. Clark, An introduction to JPEG 2000 and Watermarking, IEE Seminar on Secure Images & Image Authentication, 2000, pp. 3/1–3/6 http://ltswww.epfl.ch/~ebrahimi/JPEG2000Seminar.