QUANTIZATION WATERMARKING IN THE JPEG2000 CODING PIPELINE

Peter Meerwald
Department of Scientific Computing, University of Salzburg,
Jakob-Haringer-Str. 2, A-5020 Salzburg, Austria
pmeerw@cosy.sbg.ac.at

Abstract In this paper, we propose a blind watermarking method integrated in the JPEG2000 coding pipeline. Prior to the entropy coding stage, the binary watermark is placed in the independent code-blocks using Quantization Index Modulation (QIM). The quantization strategy allows to embed data in the detail subbands of low resolution as well as in the approximation image. Watermark recovery is performed without reference to the original image during image decompression. The proposed embedding scheme is robust to compression and other image processing attacks. We demonstrate two application scenarios: image authentication and copyright protection.

Keywords: Digital watermarking, quantization, QIM, dither modulation, JPEG2000, robustness, image authentication, data hiding.

1. INTRODUCTION

The watermarking problem is to embed a message into multimedia data in a robust yet imperceptible way. Previous research [1] indicates that significant portions of the host image, e.g. the low-frequency components, have to be modified. This led to the development of transform domain watermarking. Recently, many wavelet-based watermarking schemes have been proposed for applications such as copyright protection [2, 3] or image authentication [4, 5].

Corvi proposed one of the first wavelet-domain watermarking algorithms, simply by applying Cox's additive algorithm [1] to the approximation image of a wavelet decomposition. Another technique manipulating coefficients of the approximation image is Xie's [4] algorithm which quantizes the median coefficient of a 3×1 sliding window. Kim [6] utilizes DWT coefficients of all subbands including the approximation image to equally embed a random Gaussian distributed watermark sequence in the whole image. Perceptually significant coefficients are selected by level-adaptive thresholding to achieve high robustness. The energy of the watermark is depending on the level of the decomposition to avoid perceptible distortion. Kundur [7] embeds a binary watermark by modifying the amplitude relationship of three transform-domain coefficients from distinct detail subbands of the same resolution level of the host image. Selected coefficient tuples are sorted and the middle coefficient is quantized to encode either a zero or a one bit.

An early attempt to integrate wavelet-based image coding and watermarking has been made by Wang [8] and Su [9]. While the first approach was based on the "Multi-Threshold Wavelet Codec" (MTWC) [10], the later proposal builds on "Embedded Block Coding with Optimized Truncation" (EBCOT) [11] which is also the basis for the upcoming JPEG2000 image compression standard. Both watermarking algorithms add a pseudo-random Gaussian noise sequence to the significant coefficients of selected detail subbands.

In this paper, we present a blind watermarking technique integrated in the JPEG2000 coding pipeline. The watermark embedding and recovery process is performed on-the-fly during image compression and decompression. The computational cost to derive the transform domain a second time for watermarking purposes can therefore be saved. Our design builds on the results of the previously proposed wavelet-domain watermarking algorithms mentioned above. However, in order to fit the JPEG2000 coding process, our watermarking system has to obey the independent processing of the code-blocks. Algorithms which depend on the inter-subband [7] or the hierarchical multi-resolution [5] relationship can not be used directly in JPEG2000 coding. Due to the limited number of coefficients in a JPEG2000 code-block, correlation-based methods [3, 8] fail to reliably detect watermark information in a single independent block. Obviously, watermarking methods that require access to the original image or reference data for watermark extraction are not suited as well – this precludes all the non-blind schemes [2, 6].

In sections 2 and 3, we will review quantization watermarking and briefly discuss the JPEG2000 coding model. Our JPEG2000-integrated watermarking algorithm is proposed in section 4. Experimental results demonstrating two application scenarios are presented in section 5.

2. QUANTIZATION WATERMARKING

Blind watermarking is the communication of information via multimedia data where the unmodified host data is not available to the watermark receiver (see figure 1). The watermark w (encoding the message m) is

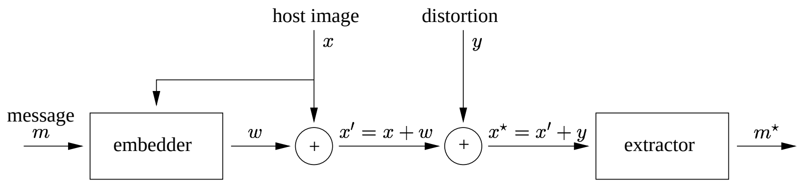


Figure 1 Blind watermark communication model.

added to the host image x. The resulting watermarked image denoted by x' has to be perceptual identical (or at least similar) to the original image. This limits the amount of modification the host image can undergo in the embedding process. Ramkumar [12] points out that for blind watermark communication, the host data x has to be seen as noise (called "self-noise"), much like the distortion y that can result from image processing or watermark attacks. However, contrary to the distortion y, the host image x is known to the watermark embedder.

Many previously proposed watermarking techniques add a spread-spectrum signal to the host image. Because the unmodified host image can not be subtracted from the received signal $x^\star$, the performance of these blind additive watermarking schemes suffers from host-signal interference when correlating the watermark with the received data.

However, watermark embedding based on Costa's result [13] has been proposed by Chen [14] and further analyzed by Eggers [15]. The technique called "quantization index modulation" (QIM) uses the watermark message as an index to select a particular quantizer from an set of possible quantizers. The selected quantizer is applied to the host data to encode the watermark message.

For the watermarking method proposed in this work, the watermark message is a sequence of N binary values, $m_n \in \{0, 1\}$. We use Chen's [14] dither modulation system with two pseudo-random dither vectors d_l of length L. The embedding rule to place one bit of watermark information into a host image vector x of length L is given by

$$s(x_i; m) = Q_\Delta(x_i + d_i(m)) - d_i(m),$$

where $Q_\Delta(\cdot)$ denotes scalar uniform quantization with step size Δ. For watermark extraction, the minimum distance between the received data $x^\star$ and its closest reconstruction point, belonging to either $m = 0$ or $m = 1$, is calculated,

$$m^\star = \arg_m \min \left\| x^\star - s(x^\star; m) \right\| .$$

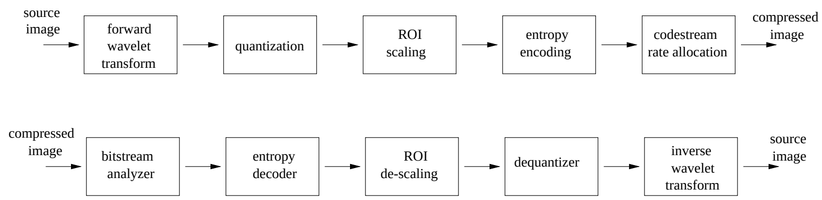


Figure 2 The JPEG2000 coding pipeline.

We have chosen the dither modulation system for embedding mainly because of its simplicity – the performance of our watermarking system might be further improved using more efficient QIM methods [14].

3. JPEG2000 CODING

The upcoming JPEG2000 image coding standard [16] is based on a scheme originally proposed by Taubman and known as EBCOT ("Embedded Block Coding with Optimized Truncation"). The major difference between previously proposed wavelet-based image compression algorithms such as EZW [17] or SPIHT [18] is that EBCOT as well as JPEG2000 operate on independent, non-overlapping blocks which are coded in several bit layers to create an embedded, scalable bitstream. Instead of zerotrees, the JPEG2000 scheme depends on a per-block quadtree structure since the strictly independent block coding strategy precludes structures across subbands or even code-blocks. These independent code-blocks are passed down the "coding pipeline" shown in figure 2 and generate separate bitstreams. Transmitting each bit layer corresponds to a certain distortion level. The partitioning of the available bit budget between the code blocks and layers ("truncation points") is determined using a sophisticated optimization strategy for optimal rate/distortion performance.

The main design goals behind EBCOT and JPEG2000 are versatility and flexibility which are achieved to a large extent by the independent processing and coding of image blocks [19]. The default for JPEG2000 is to perform a five-level wavelet decomposition with 7/9-biorthogonal filters and then segment the transformed image into non-overlapping code-blocks of no more than 4096 coefficients which are passed down the coding pipeline.

4. WATERMARK EMBEDDING

The watermark embedding stage is invoked after quantization and region-of-interest (ROI) scaling and prior to entropy coding (see figure

3). At that point, each code-block transports signed integer coefficients that have been normalized: the most significant bit (MSB) carries the sign bit and the remaining bits represent the absolute magnitude of the coefficient. We have to distinguish between code-blocks belonging to either the approximation image (LL subband) or the detail subbands (LH_j, HL_j, HH_j subbands, where $j = 1 \dots J$ is the decomposition level). The finest resolution subbands can not be used to encode information reliably.

In the first case, i.e. code-blocks belonging to the approximation image, we apply an embedding technique similar to Xie's [4] approach. We slide a non-overlapping $w \times 1$ running window over the entire code-block. At each window position, one bit of watermark information is encoded using the quantization embedding technique described in section 2. The size of the embedding window determines the coding rate. Given a gray-scale image of size 512×512, the watermark information that can be embedded in the approximation image is $\frac{512 \cdot 512}{2^{2 \cdot J}} \cdot \frac{1}{w}$ bits. Typical values of w range from 2 to 8.

For the code-blocks being part of one of the detail subbands, we have to use a larger embedding window because the energy is much lower. At least 256 coefficients are quantized to encode one watermark bit. Thus, if the size of the code-block allows, we can split it into several sub-blocks to increase the embedding capacity. The large magnitude coefficients represent edge and texture information. The human visual system (HVS) is less sensitive to changes in these regions, therefore we want to exploit this characteristic to maximize the watermark strength. To keep the implementation simple, a non-linear scaling function $f(x) = sign(x) \cdot \left| x^{\beta} \right|$, $\beta > 1$ is applied to all code-block coefficients. The scaling parameter β is chosen in a level-adaptive way between 6.5 and 5 . We obtain a more uniform coefficient representation since the high peaks in the coefficient distribution are reduced. This way, we can use simple uniform scalar quantization (as before) and still put more watermark energy in the image regions the HVS is less sensitive to. After quantization, the inverse scaling function f^{-1} is applied to derive the watermarked code-block.

5. RESULTS

We conducted our experiments with the JJ2000 implementation[1] of the JPEG2000 verification model (VM). The modularized architecture of the JJ2000 software allowed to easily integrate our watermarking module. If not noted otherwise, we use the default coding parameters for our experiments. To demonstrate the robustness and capacity of our watermarking method, a watermark with 85, 194 and 383 bits was em-

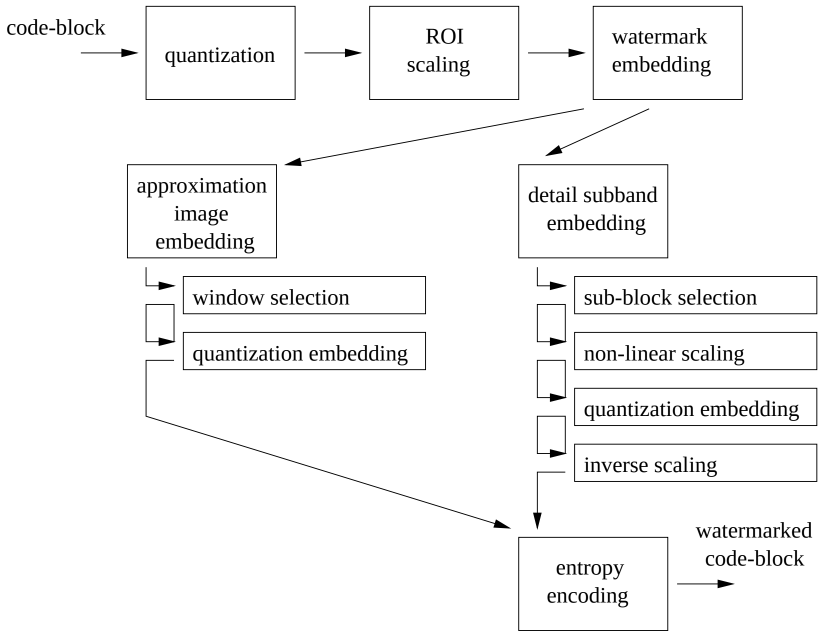


Figure 3 The watermark embedding process in the coding pipeline.

image	window size	sub-block size	capacity	PSNR
Lena	4	64	85	32.05
Fishing Boat	2	32	194	31.45
Goldhill	2	16	383	32.09

Table 1 Embedding parameters and the corresponding bit capacity for three 512×512 gray-scale images, together with the resulting PSNR.

bedded in the 512×512 gray-scale images "Lena", "Fishing Boat" and "Goldhill", respectively. Figure 4 shows the watermarked images "Lena" and "Goldhill" together with their difference images. The effect of our simple scaling function is clearly visible: the edges contain more watermark energy than smooth regions. The different watermark capacities were achieved by choosing the embedding parameters from table 1. The resulting PSNR is also given.

For copyright protection, we embed a binary message that identifies the owner of the image. The dither vectors are kept secret to protect the watermark. The normalized correlation result of the recovered versus the embedded message is depicted in figure 5. The watermarked images were subjected to JPEG and JPEG2000 compression with varying compression parameters (top row). To simulate image processing attacks, the images were blurred and sharpened using the ImageMagick[2] convert program (bottom row). The results indicate our watermark survives the attacks, but additional error-corrective coding is required to achieve perfect recovery of the embedded information.

The tamper detection application requires a fragile watermark that breaks in order to indicate the areas that have been manipulated. At the same time, however, the watermark should be robust against unintentional distortion, e.g. caused by lossy image compression. Figure 6 (a) shows the "Fishing Boat" image, watermarked with a sequence of all-zero bits. Next, we manipulated three regions using the GIMP[3] and JPEG compressed the image with default quality; see figure 6 (b) and the difference image, highlighting the changes (c). The detection results of our watermarking schemes are depicted in figure 6 (d). The malicious tampering has been detected and localized while the distortion due to JPEG compression did not raise a false alarm.

One coefficient in the approximation image of the wavelet domain corresponds to a block of pixels in the spatial domain. In order to achieve good spatial resolution for our tamper detection example, we had to limit the wavelet transform to three decomposition steps. Therefore, we can authenticate pixel blocks of size 8×8 individually. Since the watermark consists of sequence of zero bits, we could use sliding window detection [20] in horizontal, diagonal and vertical direction in the approximation image. The tamper detection results from the three directions were accumulated and contribute to the brightness of the tamper detection image of figure 6 (d).

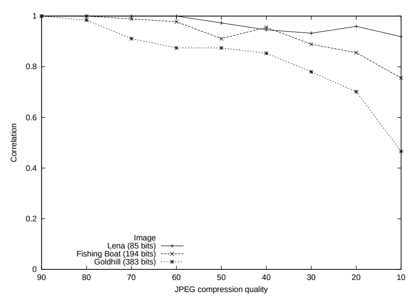
6. CONCLUSION

We demonstrated our watermarking scheme can be integrated in the JPEG2000 coding process and discussed some of the limitations. A novel embedding algorithm based on QIM and suitable for watermarking independent JPEG2000 code-blocks was proposed which allows blind watermark recovery during image decompression. We investigated a copyright protection and an image authentication application and provided robustness as well as capacity results. Future work will try to improve the performance of the embedding method and consider ROI coding.

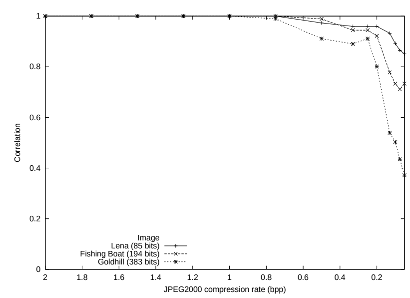
Notes

1. The JJ2000 source is available for download at `http://jj2000.epfl.ch`.
2. The ImageMagick programs are at `http://www.simplesystems.org/ImageMagick`.
3. The GNU Image Manipulation Program is available at `http://www.gimp.org`.

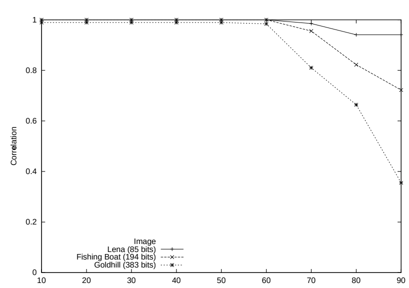
Figure 4 The watermarked images “Lena” and “Goldhill”, together with their difference images.



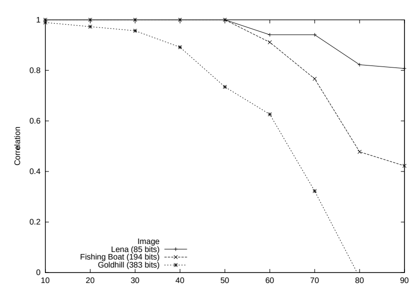
(a) JPEG



(b) JPEG2000



(c) blur

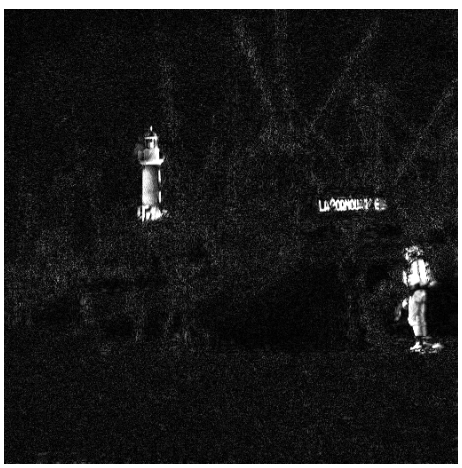


(d) sharpen

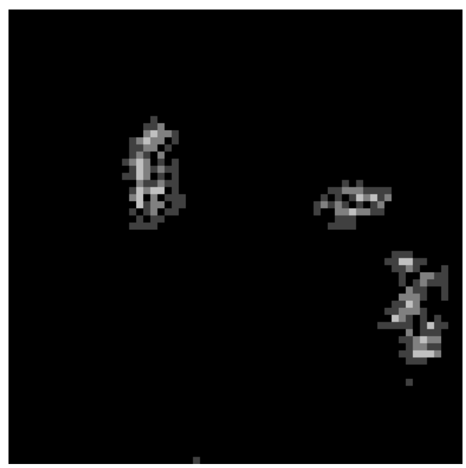
Figure 5 The robustness against JPEG compression (a) and JPEG2000 compression (b), blurring (c) and sharpening (d). Measured using normalized correlation between the recovered and embedded message.

(a) watermarked image

(b) manipulated image



(c) difference image



(d) tamper detection

Figure 6 The watermarked "Fishing Boat" image (a) and the tampered version (b). The manipulations are highlighted after default JPEG compression in the difference image (c). The manipulated regions detected by the algorithm (d).

References

[1] I. J. Cox, J. Kilian, T. Leighton, and T. G. Shamoon, "Secure spread spectrum watermarking for multimedia," in *Proceedings of the IEEE International Conference on Image Processing, ICIP '97*, vol. 6, pp. 1673 – 1687, (Santa Barbara, California, USA), October 1997.

[2] M. Corvi and G. Nicchiotti, "Wavelet-based image watermarking for copyright protection," in *Scandinavian Conference on Image Analysis, SCIA '97*, (Lappeenranta, Finland), June 1997.

[3] M. Barni, F. Bartolini, V. Cappellini, A. Lippi, and A. Piva, "A DWT-based technique for spatio-frequency masking of digital signatures," in *Proceedings of the 11th SPIE Annual Symposium, Electronic Imaging '99, Security and Watermarking of Multimedia Contents*, P. W. Wong, ed., vol. 3657, (San Jose, CA, USA), January 1999.

[4] L. Xie and G. R. Arce, "Joint wavelet compression and authentication watermarking," in *Proceedings of the IEEE International Conference on Image Processing, ICIP '98*, (Chicago, IL, USA), 1998.

[5] H. Inoue, A. Miyazaki, and T. Katsura, "Wavelet-based watermarking for tamper proofing of still images," in *Proceedings of the IEEE International Conference on Image Processing, ICIP '00*, (Vancouver, Canada), September 2000.

[6] J. R. Kim and Y. S. Moon, "A robust wavelet-based digital watermark using level-adaptive thresholding," in *Proceedings of the 6th IEEE International Conference on Image Processing, ICIP '99*, p. 202, (Kobe, Japan), October 1999.

[7] D. Kundur, "Improved digital watermarking through diversity and attack characterization," in *Proceedings of the ACM Workshop on Multimedia Security '99*, pp. 53 – 58, (Orlando, FL, USA), October 1999.

[8] H.-J. Wang and C.-C. J. Kuo, "An integrated approach to embedded image coding and watermarking," in *Proceedings of IEEE ICASSP '98*, (Seattle, WA, USA), May 1998.

[9] P.-C. Su, H.-J. Wang, and C.-C. J. Kuo, "Digital watermarking on EBCOT compressed images," in *Proceedings of SPIE's 44th Annual Meeting: Applications of Digital Image Processing XXII*, vol. 3808, (Denver, CO, USA), July 1999.

[10] H.-J. Wang and C.-C. J. Kuo, "High fidelity image compression with multithreshold wavelet coding (MTWC)," in *SPIE's Annual meeting - Application of Digital Image Processing XX*, (San Diego, CA, USA), August 1997.

[11] D. Taubman, "High performance scalable image compression with EBCOT," *IEEE Transactions on Image Processing* **9**, pp. 1158 – 1170, July 2000.

[12] M. Ramkumar and A. N. Akansu, "Self-noise suppression schemes for blind image steganography," in *Proceedings of SPIE: Multimedia Systems and Applications II*, vol. 3845, (Boston, MA, USA), September 1999.

[13] M. H. M. Costa, "Writing on dirty paper," *IEEE Transactions on Information Theory* **29**, pp. 439 – 441, May 1983.

[14] B. Chen and G. W. Wornell, "Preprocessed and postprocessed quantization index modulation methods for digital watermarking," in *Proceedings of IS&T/SPIE's 12th Annual Symposium, Electronic Imaging 2000: Security and Watermarking of Multimedia Content II*, P. W. Wong, ed., vol. 3971, (San Jose, CA, USA), January 2000.

[15] J. J. Eggers and B. Girod, "Quantization watermarking," in *Proceedings of IS&T/SPIE's 12th Annual Symposium, Electronic Imaging 2000: Security and Watermarking of Multimedia Content II*, P. W. Wong, ed., vol. 3971, (San Jose, CA, USA), January 2000.

[16] "JPEG2000 part 1 final committee draft version 1.0," tech. rep., ISO/IEC FCD15444-1, March 2000.

[17] J. M. Shapiro, "Embedded image coding using zerotrees of wavelet coefficients," *IEEE Transactions on Signal Processing* **41**, pp. 3445 – 3462, December 1993.

[18] A. Said and W. A. Pearlman, "A new, fast, and efficient image codec based on set partitioning in hierarchical trees," in *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 6, pp. 243 – 250, June 1996.

[19] M. Charrier, D. S. Cruz, and M. Larsson, "JPEG2000, the next millennium compression standard for still images," in *Proceedings of the IEEE International Conference on Multimedia & Computing Systems, ICMCS '99*, vol. 1, pp. 131 – 132, (Florence, Italy), June 1999.

[20] J. J. Eggers and B. Girod, "Blind watermarking applied to image authentication," in *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing, ICASSP '01*, (Salt Lake City, UT, USA), May 2001.