A Joint JPEG2000 Compression and Watermarking System Using a TCQ-Based Quantization Scheme

Dalila Goudia, Marc Chaumont, William Puech, Naima Hadj Said

A Joint JPEG2000 Compression and Watermarking System Using a TCQ-Based Quantization Scheme

D. Goudia[a,b], M. Chaumont[a], W. Puech[a] and N. Hadj Said[b]

[a]University of Montpellier II, Laboratory LIRMM, UMR CNRS 5506, 161, rue Ada, 34095
Montpellier cedex 05, France;
[b]University of Science and Technologies of Oran (USTO), Oran, Algeria

ABSTRACT

In this paper, we describe a Trellis Coded Quantization (TCQ)-based quantization and watermarking technique in the framework of JPEG2000 still image compression. Furthermore, we investigate the design of a novel joint compression and watermarking scheme based on a hybrid TCQ module which can perform at the same time quantization and watermark embedding. The watermark extraction process can be achieved both during and after image decompression. Another advantage is the lower complexity of the system because the quantization stage is used for both compression and watermarking purposes. Experimental results have demonstrated that the proposed joint scheme successfully survives JPEG2000 compression with minimal degradation of the image quality. We also studied the robustness of the scheme against gaussian filtering attack, gaussian noise attack, valumetric attack and jpeg attack.

Keywords: Image compression, digital watermarking, JPEG2000, TCQ

1. INTRODUCTION

The digital watermarking describes methods that hide information in digital media by modifying the media data. Modeling watermarking as communications with side information has led to the design of very efficient algorithms. This generation of watermarking schemes is called informed schemes.[1–3] One of the two main informed watermarking categories is the quantized-based watermarking schemes. In 1999, Chen and Wornell[1] have introduced the Quantization Index modulation (QIM), where the host signal is considered as the side information of Costa's scheme.[4] A practical and efficient implementation of the Costa's ideas is the Scalar Costa Scheme (SCS) proposed by Eggers et al.[2] which is quiet similar to the DC-QIM watermarking.[1]

It has been noticed that image compression and image watermarking share some common characteristics. There are several advantages to combine, at one end the image coding and watermark embedding operations and, at the other end, the image decoding and watermark extraction. On the other hand, combining image coding and image watermarking is highly desired in some classical applications, such as copyright protection, copy and access control and annotation, where image compression is performed before spreading abroad.

JPEG2000[5] is a compression standard developed by the Joint Photographic Experts Group (JPEG) that supports lossy or lossless compression of grayscale or color images. JPEG2000 supports a number of functionalities and includes many advanced features; it has thus become the solution of choice for many digital imaging fields and applications. A number of watermarking techniques for JPEG2000 images for authentication and ownership protection purposes have been proposed. Few among those methods are quantization-based watermarking schemes combined to JPEG2000.[5–7] Meerwald et al.[6] developed a watermarking process based on Quantization Index Modulation (QIM) integrated to JPEG2000 coding chain. Schlauweg et al.[5] have developed an image watermarking scheme by using an extended scalar quantization and hashing scheme in JPEG2000 coding chain. For these last two techniques, the watermark embedding is performed after quantization process. Makhloufi et al.[7] have proposed to integrate a modified QIM scheme in JPEG2000 part 2 before the quantization process. The QIM modification consists of reducing the distortion caused during quantization-based watermarking by using a non-linear scaling. It is worth noting that there is actually no genuine joint compression/watermarking

dalila.goudia@lirmm.fr, marc.chaumont@lirmm.fr, william.puech@lirmm.fr, nim_hadj@yahoo.fr

solutions in the JPEG2000 framework. The watermarking systems which are proposed in the recent literature integrate an **additional** watermark embedding/extraction stage in the JPEG2000 compression/decompression process.

The objective of this paper is to design a novel joint JPEG2000 compression and informed watermarking scheme based on a hybrid trellis coded quantization (TCQ[8,9]) module which can perform at the same time quantization and watermark embedding. The system allows both watermark recovery during and after image decompression. However, we have two major constraints to consider. First, the embedding of the mark must not lead to a significant deterioration of the compressor's performance (compression ratio and image quality). Second, the scheme also needs to be robust enough to allow a correct message extraction after some acceptable manipulations of the decompressed/watermarked image.

The specific organization of the paper is as follows. Section 2 recalls the TCQ quantization both in the JPEG2000 standard and in the watermarking domain. Section 3 describes the proposed joint JPEG2000 coding and watermarking TCQ-based scheme. Section 4 presents experimental results and finally Section 5 concludes this work.

2. TRELLIS CODED QUANTIZATION (TCQ)

Trellis coded quantization (TCQ) is a particular kind of vector quantization proposed by Marcellin and Fischer[8] which could achieve performance near rate distortion bound. The main ideas behind TCQ are due to trellis coded modulation (TCM).[10] TCQ is a trellis-based quantization scheme associated with a structured codebook. A trellis is nothing more than a state transition diagram (that takes time into account) for a finite state machine. Each branch in the trellis represents a transition from one state to another, at the next point in time. Given an initial state at t = 0, this path can be specified by a binary sequence, since there are only two possible transitions from one state to another.
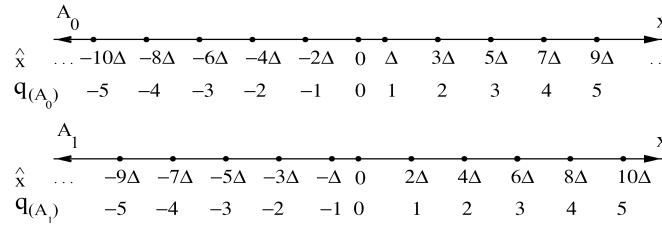
2.1 TCQ in JPEG2000

Figure 1. Union quantizers for TCQ in JPEG2000.

Several quantization options are provided within JPEG2000 Part 2 of the standard and include TCQ.[11] The variant of TCQ used in the JPEG2000 standard is the Entropy Coded TCQ (ECTCQ). A uniform scalar quantizer with step size Δ is partitioned into four subsets called D_0, D_1, D_2 and D_3. The subsets D_i are used to label the branches of a trellis. The union of the quantizers associated with each state is called a union quantizer. The two union quantizers used in JPEG2000 are $A_0 = D_0 \cup D_2, A_1 = D_1 \cup D_3$ and are illustrated in Fig. 1. Fig. 3.a shows a single stage of a typical 8-state trellis with branch labeling. At each state, we could choose between one of two groups of quantizers to quantize the source input **x**. In TCQ we pick up connected branches in trellis by using Viterbi algorithm[12] to quantize a sequence so as to have less accumulated distortion. The Viterbi Algorithm produces two sequences: the first one is a binary sequence defining the minimum distortion path. The second one is the sequence of corresponding TCQ quantization indices. The dequantization of TCQ indices at the decoder is straightforward. Given the initial state and the path sequence, the decoder is able to reproduce the reconstructed values by using the sequence of indices specifying which codeword was chosen from the appropriate union quantizer.

2.2 Watermarking techniques based on TCQ

There are only few watermarking techniques in the literature which use TCQ. In these algorithms, the paths in the trellis are forced by the values of the message and the samples of the host signal are quantized with the codebook corresponding to the trellis path. This approach is called the TCQ path selection (TCQ-PS).[13–15] Le Guelvouit[15] explores the use of trellis-coded quantization techniques (TCQ and turbo TCQ) to design a more efficient public-key steganographic scheme in the presence of a passive warden. Braci *et al.*[13] focused on the security aspects of informed watermarking schemes based on QIM and proposed a secure version of the TCQ-PS. The main idea is to cipher the path at the encoder side by shifting randomly each obtained codeword to a new one taking from another subset. Then, according to the secret key, a codebook different from the one used for the transmitted message is chosen. Ouled Zaid *et al.*[14] have developed a watermarking algorithm resilient to lossy compression attack by exploring the use of turbo TCQ techniques in the wavelet domain but not in the JPEG2000 coding scheme. The TCQ allows reduction of the complexity cost of the watermarking system and a reduction of the distortions.

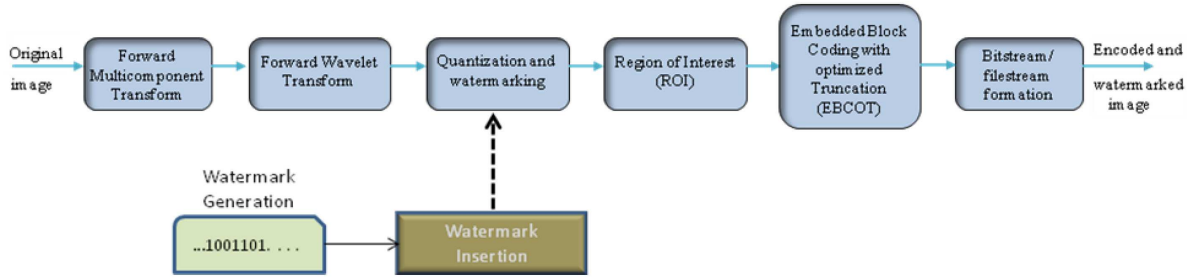## 3. THE JOINT JPEG2000 BASED COMPRESSION AND WATERMARKING SCHEME

Figure 2. An overview of the joint JPEG2000 encoder/watermarking insertion scheme.

The main idea behind the approach we proposed is to quantize and watermark wavelet coefficients at the same time by using a hybrid TCQ quantization module. The TCQ path selection method (TCQ-PS)[13] is not suitable for our purpose because the path corresponds to the embedded message. The security of the message is thus not ensured since the path is a non-secured part of the JPEG2000 bit-stream. We propose a new watermarking-based TCQ technique which is independent of the path selection. We chose to embed the watermark during the quantization process in the HL detail sub-band of the selected resolution levels. Wavelet coefficients of the other sub-bands are quantized with the classical uniform scalar quantization stage. We replace the uniform scalar quantizers used in JPEG2000 part II by shifted scalar quantizers with the same step size Δ as for the original ones. We can also use a higher step size by multiplying the original step size with a constant. These quantizers differ from the previous quantizers by the introduction of a shift $\mathbf{d}$ which is randomly obtained with a uniform distribution over $[-\Delta/2, \Delta/2]$.[1] We propose the following principle: if the bit to be embedded is the bit 0 then the quantizer $D_j^0, j = 0, 1, 2, 3$ with the shift $d[0]$ is used. If it is the bit 1, we employ the quantizer D_j^1 with the shift $d[1]$ satisfying the condition: $|d[1] - d[0]| = \Delta/2$. So, we will have two groups of union quantizers for the trellis structure used in our aproach: the group 0, $A_0^0 = D_0^0 \cup D_2^0, A_1^0 = D_1^0 \cup D_3^0$ which represents a watermark embedded bit 0 and the group 1, $A_0^1 = D_0^1 \cup D_2^1, A_1^1 = D_1^1 \cup D_3^1$ which represents a watermark embedded bit 1. The given trellis structure has four branches exiting each state (Fig. 3.b). Let us consider a binary message $\mathbf{m}$ to be embedded and a host signal $\mathbf{x}$. The embedding of the watermark guides the quantization process. For each transition i in the trellis, the union quantizers are selected according to the value $\mathbf{m}[i]$ and the subsets $D_j^{m[i]}, j = 0, 1, 2, 3$ are used to label the branches of the given trellis. The trellis is modified in order to remove all the branches that are not labeled with the union quantizers that encode the message as illustrated in Fig. 3.c. The process of quantization produces the binary sequence $\mathbf{p}$ defining the minimum distortion path and the

sequence of TCQ quantization indices $\mathbf{q}$ given by:

$$q[i] = Q_{D_j^{m[i]}}(x[i]) = sign(x[i] - d_i[m[i]]) \left\lfloor \frac{|x[i] - d_i[m[i]]|}{\Delta_j} \right\rfloor \tag{1}$$

where d_i is the shifting of the shifted scalar quantizer $D_j^{m[i]}$ at transition i and Q is the quantization function. In addition to $\mathbf{p}$ and $\mathbf{q}$, the sequence $\mathbf{l}$ is generated. It contains an extra information which ensures that the modified trellis structure is properly retrieved during the dequantization step. In the dequantization process, given $\mathbf{p}$, $\mathbf{q}$, $\mathbf{l}$ and $\mathbf{d}$, the decoder produces the reconstructed values $\hat{\mathbf{x}}$ as:

$$\hat{x}[i] = \bar{Q}_{D_j^{m[i]}}^{-1}(q[i]) = sign(q[i])(|q[i]| + \delta)\Delta_j + d_i[m[i]] \tag{2}$$

where $\bar{Q}^{-1}$ is the dequantization function and δ is a user selectable parameter within the range $0 < \delta < 1$. The dequantization stage utilizes the same trellis employed in the quantization step.
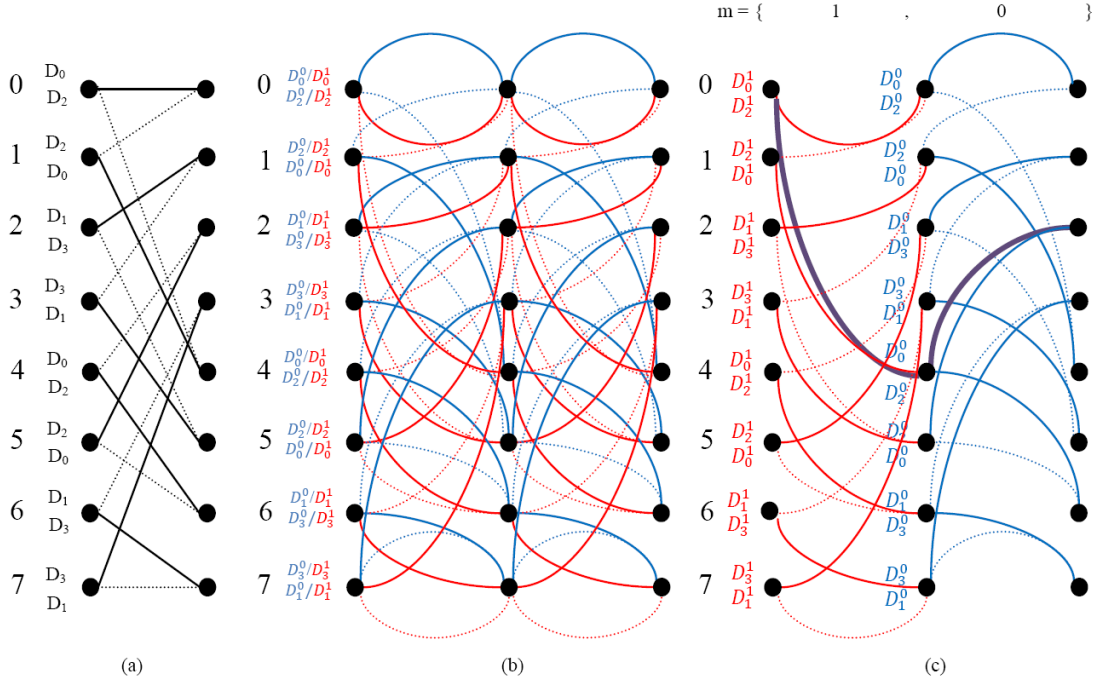

Figure 3. The trellis structure used in JPEG2000 and in our joint watermarking/JPEG2000 scheme: a) A single stage of an 8-state trellis with branch labeling used in JPEG2000, b) A two-stage of the trellis structure used in our approach with four branches entering and exiting each state, c) Insertion of the message m={1,0} with the modified trellis: all the branches that are not labeled with the union quantizers that encode the message are removed.

3.1 Quantization and watermark embedding

The watermark embedding (watermark extraction) process is performed independently into each code-block. First we generate the message to be inserted. In order to add more robustness to the transmitted message, we encode it with an error correcting code. For each code-block, the quantization/watermark embedding procedures are as follows: first of all, the shiftings $\mathbf{d}$ are computed using a pseudo random generator initialized by the secret key k. The union quantizer group 0 and group 1 for each transition are generated. The initial state of the given trellis structure is set to 0. The trellis is simplified so that all the branches through the trellis, and thus all the associated union quantizers, encode the message $\mathbf{m}$ as illustrated in Fig. 3.c. Finaly, the Viterbi Algorithm[12] is applied in order to find the minimum distortion path (the bold arcs in Fig. 3.c).

3.2 Watermark extraction

In order to extract the embedded message within the decompressed image, we perform the following operations: The decompressed watermarked image is first transformed with the DWT, secondly, we take the coefficients of the HL sub-bands included in the watermarking process and we stored it in the vector $\mathbf{y}$. Then, we perform the TCQ quantization onto $\mathbf{y}$ by applying the Viterbi algorithm onto the whole trellis (Fig. 3.b) in order to extract the watermarking message.

We can also extract the embedded message during the JPEG2000 decompression. For each code-block, the sequence $\mathbf{l}$ enable us to retrieve the trellis structure used during the quantization stage. The embedded message can be extracted by analyzing the labeling of the given trellis structure. At a transition i, if the quantizers which label the branches of the states belong to group 0, it means that the message bit inserted $\hat{m}[i]$ is the bit 0. Otherwise, the quantizers belong to group 1 and $\hat{m}[i] = 1$. This modified trellis is afterward used in the dequantization stage to reconstruct the wavelet coefficients.

4. EXPERIMENTAL RESULTS

To implement our joint JPEG2000-based watermarking algorithm, we chose to use the OpenJPEG library[16] which is an open-source JPEG2000 codec written in C language. The following set of compression and watermark parameters were fixed: irreversible DWT 9-7, 5 levels of wavelet decomposition, 1 tile, size of code-block: 64 x 64 and a watermark message of 1024 bits length inserted in the HL sub-band of the second resolution level. The message is encoded with a very simple convolution code 2-memory 1/16-rate. The shifting vectors are kept secret to protect the watermark.

In order to test the effect of JPEG2000 compression, series of experiments on different JPEG2000 grayscale test images of size 512 x 512 have been performed. We set the compression ratio from 2.5 bpp to 0.2 bpp. Δ_{TCQ} is the step size of the TCQ quantizers D_0, D_1, D_2 and D_3. We use different values of Δ_{TCQ} in our experiments: Δ, 2Δ, 3Δ and 4Δ (Δ is the JPEG2000 original step size). The message can be correctly detected during decompression for all tested compression bitrates. Experimental results shows that the embedded watermark information is also completely recovered after the decompression stage even at low bitrates. Table 1 shows the PSNR results obtained for the well known test images: bike, clown, lena and peppers. Based on the results reported in Table 1 we can notice that the PSNR decreases as the step size value increases. The decrease is more important at high bitrates. At low bitrates, the diminution is small when we compare between the PSNR results obtained at different step size values for the four images. For example, we obtain a PSNR of 33.46 dB at 0.2 bpp for $\Delta_{TCQ} = \Delta$ compared to 33.09 dB for $\Delta_{TCQ} = 4\Delta$. The PSNR results obtained by our joint scheme are compared with those obtained without watermarking. When considering the $\Delta_{TCQ} = \Delta$ step size, we observe that the degradation induced by the watermark embedding in terms of PSNR is relatively small for medium and low bitrates. As an example, for bike image, there is a loss of 0.12 dB at 1.6 bpp. For peppers image compressed at the same bitrate, the difference is about 1.83 dB. At 0.2 bpp, there is a difference of 0.56 dB between the lena image compressed with the classical JPEG2000 coder and the same image compressed and watermarked with the joint scheme. We note a loss of 1.35 dB for clown image at the same bitrate.

We should note that there is a trade off between the quantizer step size needed for a correct embedding (extraction) of the watermark and the expected quality of the decompressed/watermarked image. When using a larger Δ_{TCQ}, the fidelity will deteriorate because the distance between the quantization points will grow. However, the advantage of using a larger Δ_{TCQ} value is that an improved robustness is obtained. The step size used in JPEG2000 is small. It is big enough to ensure a correct extraction of the watermark during and after decompression. Nevertheless, the watermarks will not survive in case of strong power attacks of the decompressed/watermarked images. So a larger Δ_{TCQ} can be used in order to improve the robustness. We will obtain a lower quality (fidelity) in comparison with that obtained using the original JPEG2000 step size. This will result in an improved robustness. The PSNR obtained are still acceptable in the context of a joint scheme as shown in Table 1.

In a second round of experiments, a database of 200 grayscale images of size 512 x 512 has been considered to evaluate the robustness of the joint scheme. Four kinds of attacks have been performed: gaussian filtering attack, gaussian noise attack, valumetric attack and jpeg attack similarly to Miller et al.[3] The Bit Error Rate

Image test	bitrate (bpp)	PSNR (dB) with JPEG2000	PSNR (dB) with the joint scheme $\Delta_{TCQ} = \Delta$	PSNR (dB) with $\Delta_{TCQ} = 2\Delta$	PSNR (dB) with $\Delta_{TCQ} = 3\Delta$	PSNR (dB) with $\Delta_{TCQ} = 4\Delta$
Bike	2.5	43.23	41.48	40.94	40.18	39.33
	2	39.64	40.30	39.86	39.14	38.50
	1.6	39.33	39.45	39.07	38.55	37.97
	1	38.11	38.25	38.07	37.55	37.05
	0.5	36.51	36.45	36.30	35.99	35.61
	0.2	33.52	33.46	33.39	33.29	33.09
Clown	2.5	44.08	41.20	36.51	34.32	32.378
	2	42.78	39.95	36.04	34.15	32.25
	1.6	40.77	37.92	34.11	31.18	30.62
	1	38.71	37.13	33.05	30.71	30.24
	0.5	35.76	31.80	31.20	30.39	30.26
	0.2	31.09	29.74	29.12	29.03	28.95
Lena	2.5	47.47	42.30	40.18	39.77	38.65
	2	45.33	42.08	40.32	39.09	37.58
	1.6	43.38	41.17	39.98	39.27	37.46
	1	41.55	40.07	39.10	38.59	36.69
	0.5	40.03	39.26	37.54	37.02	36.29
	0.2	36.56	36.00	35.76	35.38	34.95
Peppers	2.5	43.13	41.01	39.11	37.53	36.42
	2	39.69	38.63	36.51	35.00	35.42
	1.6	39.20	37.37	36.02	34.34	33.94
	1	39.03	37.47	36.15	34.42	34.45
	0.5	36.50	34.64	34.88	34.12	33.86
	0.2	29.35	29.78	29.75	29.67	29.55

Table 1. PSNR(dB) for compressed image tests obtained with the joint scheme with different step sizes and comparison with the PSNR obtained with the classical JPEG2000 part 2 coder.

(BER) is computed for each attack. The BER is the number of erroneous extracted bits divided by the total number of embedded bits. When analyzing the results, the BER values lower than 0.1 are considered. The BER results for the four attacks are presented in Fig. 4 and Fig. 5. The logarithmic (base 10) scale is used for the Y-axis (BER results).

The watermarked images are filtered by gaussian filter of width σ_g. The experiment was repeated for different values of σ_g, and the BER has been computed. The obtained results are reported in Fig. 4.a. The watermarks survive filtering effects up to $\sigma_g = 0.6$ for $\Delta_{TCQ} = \Delta$. As expected, the robustness is improved when the step size value increase. The BER obtained is lower than 0.1 when the joint scheme undergo gaussian filtering up to: $\sigma_g = 0.8$ for $\Delta_{TCQ} = 2\Delta$, $\sigma = 0.9$ for $\Delta_{TCQ} = 3\Delta$ and $\sigma_g = 1$ for $\Delta_{TCQ} = 4\Delta$. Fig. 4.b shows the results obtained when the watermarked images are corrupted by additive white gaussian noise (AWGN) with mean 0 and standard deviation σ. The joint scheme is not very robust to this kind of attack. Indeed, the proposed joint approach gives BER results below 0.1 against AWGN with standard deviation σ up to 4 for $\Delta_{TCQ} = 4\Delta$.

The results against the valumetric scaling attack are summarized in Fig. 5.a. The quantized-based watermarking algorithms are recognized to be very sensitive to valumetric scaling (each pixel is multiplied with a constant). Experiments show significant resistance of our joint scheme to this kind of attack. The BER results are still under the 0.1 limit when there are changes in scaling with a scaling factor in the range of 0.7 and 1.3 for $\Delta_{TCQ} = \Delta$. As usual, the robustness is better for $\Delta_{TCQ} = 4\Delta$: the valumetric scaling attack with a scaling factor in the range of 0.6 and 1.6 gives BER values lower than 0.1. Fig. 5.b shows the BER results to jpeg attack. We observe that the watermarks are only able to cope with jpeg quality factor up to 70 for $\Delta_{TCQ} = 4\Delta$. The weak robustness to jpeg attack is inherent to the approach since the coefficients included in the watermarking process are high frequency wavelet coefficients. It should also be noted that the quantized-based methods are
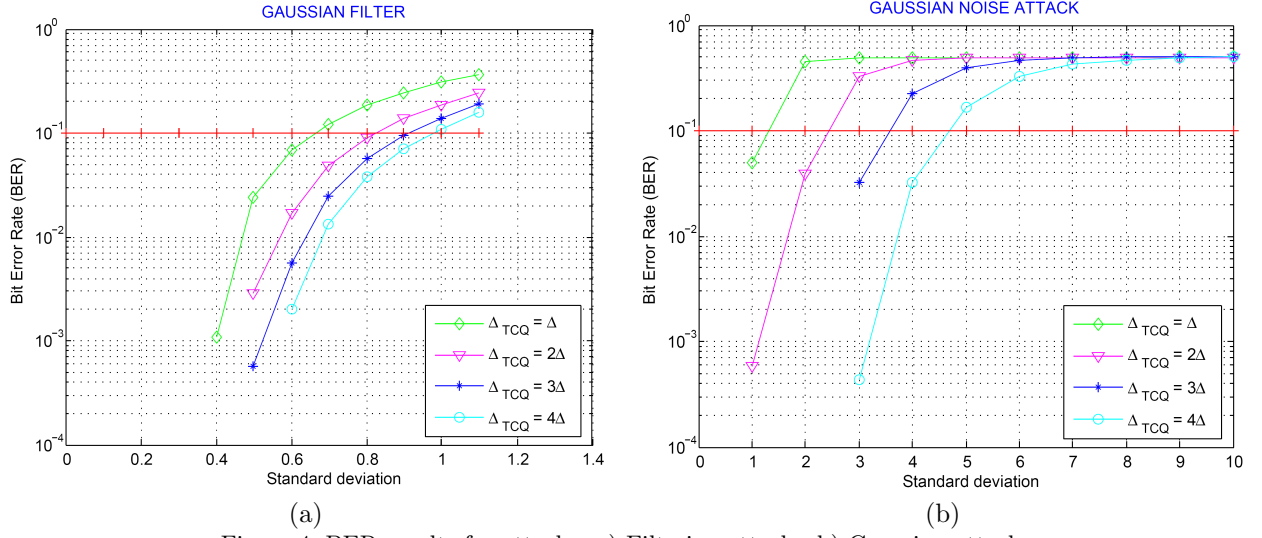
sensitive to jpeg attack.

(a)   (b)

Figure 4. BER results for attacks: a) Filtering attack , b) Gaussian attack.

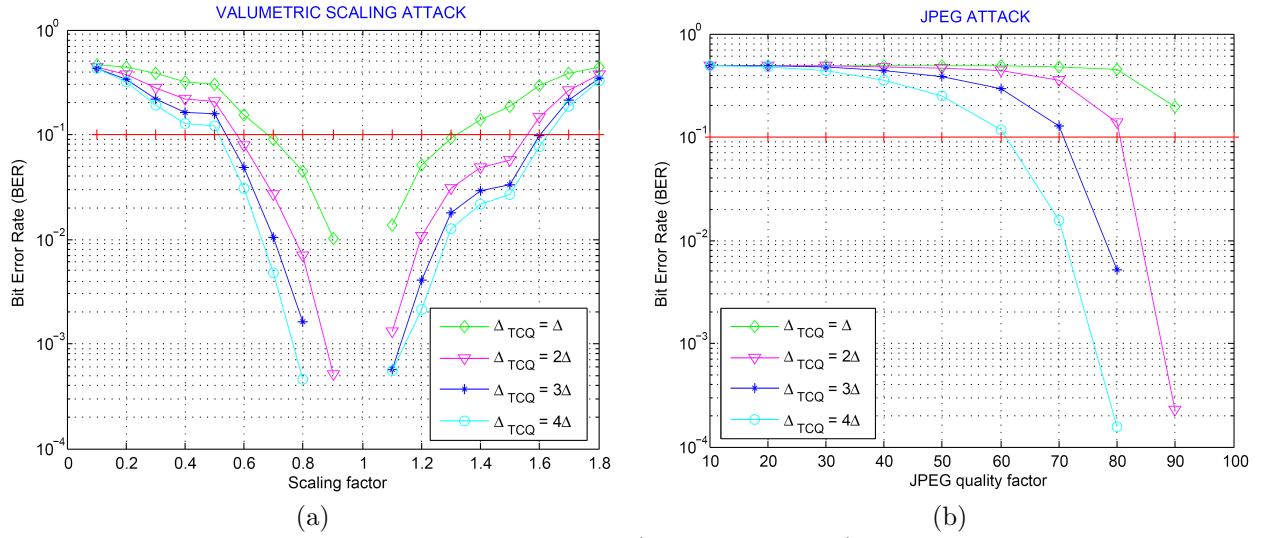(a)   (b)

Figure 5. BER results for attacks: a) Scaling attack , b) JPEG attack.

5. CONCLUSION

We investigate a TCQ quantization based algorithm integrating image watermarking into JPEG2000 coder. The main contribution is that the proposed system allows both quantization of wavelet coefficients and watermark embedding by using the same quantization module. Experimental investigations demonstrate that this joint scheme is able to achieve good visual quality in terms of PSNR. The proposed embedding technique can survive JPEG2000 compression at very low bitrates. The watermark robustness against common image attacks have also been studied. It has been noticed that the robustness is improved when a higher quantizer step size value is used. Thus, the selection of the quantizer step size must be done optimally so that the best trade off between robustness and minimum quality degradation should be achieved.

REFERENCES

[1] Chen, B. and Wornell, G., "Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding," *IEEE Transaction on Information Theory* **47**, 1423–1443 (2001).

[2] Eggers, J. J., Buml, R., Tzschoppe, R., and Girod, B., "Scalar costa scheme for information embedding," *IEEE Transaction on Signal Processing* **51**, 1003–1019 (2003).

[3] Miller, M. L., Doerr, G. J., and Cox, I. J., "Applying informed coding and informed embedding to design a robust, high capacity watermark," *IEEE Transactions on Image Processing* **13**, 792–807 (2004).

[4] Costa, M., "Writing on dirty paper," *IEEE Transaction on Information Theory* **29**, 439–441 (1983).

[5] Schlauweg, M., Profrock, D., and Muller, E., "JPEG2000-based secure image authentication," *workshop on Multimedia and security* , 62–67 (2006).

[6] Meerwald, P., "Quantization watermarking in the JPEG2000 coding pipeline," *Communications and Multimedia Security* , 69–79 (2001).

[7] Makhloufi, A., Zaid, A. O., Boualleg, R., and Boualleg, A., "Improved Quantization Index Modulation Based Watermarking Integrated to JPEG2000 Coding Scheme," in [*Visual Information Processing and Communication*], *Proc. SPIE* **7543**, 17–21 (2010).

[8] Marcellin, M. and Fischer, T., "Trellis coded quantization of memoryless and gauss-markov sources," *IEEE Transaction on communication* **38**, 82–93 (1990).

[9] ISO/IEC JTCI/SC29 WG1, [*JPEG2000 Part II Final Committee Draft Version 1.0*] (March 2000).

[10] Ungerboeck, G., "Channel coding with multilevel/phase signals," *IEEE Transaction on Information Theory* **28**, 55–67 (1982).

[11] Taubman, D. and Marcellin, M., [*JPEG2000 image compression fundamentals, standards and practice*], Kluwer Academic Publishers, Boston/Dordrecht/London (2002).

[12] Forney Jr, G. D., "The viterbi algorithm," *IEEE Transaction on Information Theory* **61**, 268–278 (1973).

[13] Braci, S., Boyer, R., and Delpha, C., "Security evaluation of informed watermarking schemes," in [*ICIP09, Cairo, Egypt*], *Proc. ICIP*, 117–120 (2009).

[14] Zaid, A. O., Makhloufi, A., and Bouallegue, A., "Wavelet Domain Watermark Embedding Strategy using TTCQ Quantization," *IJCSNS* **7**, 268–278 (2007).

[15] Le-Guelvouit, G., "Trellis-coded quantization for public-key watermarking, 2005, see the website http://www.gleguelv.org/pub/index.html."

[16] the openjpeg library is available for download at http://www.openjpeg.org.