Hyper-Cube Watermarking Scheme

Marc Chaumont, Dalila Goudia, William Puech

Hyper-Cube Watermarking Scheme

Marc CHAUMONT[a,b], Dalila GOUDIA[b], and William PUECH[b]

[a] University of Nîmes, Place Gabriel Péri, 30000 Nîmes, France.
[b] Laboratory LIRMM, UMR CNRS 5506, University of Montpellier II,
161, rue Ada, 34392 Montpellier cedex 05, France.

ABSTRACT

In 2007, Li and Cox showed that their scheme called Perceptual-QIM (P-QIM) was one of the solutions the most successful in order to watermark multi-bits in an image by a quantization approach. Our research led us to take some of their ideas and brought new proposals. This paper presents a new scheme named Hyper-Cube. In addition to re-express the mechanisms of watermarking from a different angle and to give a clear framework, we propose two improvements: the computation of the modified Watson *slacks* on a neighborhood, and the use of a cleverly integrated error correcting code. Additionally, we experimentally show that the addition of the JPEG quantization table for setting the size of *lattices* do not reduce performances. This demonstrate that the scheme may easily be integrated in a joint watermarking-compression scheme. Given the obtained results, we can conclude that the Hyper-Cube watermarking scheme is currently one of the most successful technique when one wants to watermark an image using quantization-based approaches.

Keywords: Robust watermarking, Quantization-based watermarking, Perceptual watermarking, Lattice codes, Watson model, Valumetric attack, High rate, Correcting codes.

1. INTRODUCTION

The informed watermarking appeared around 1998 when the Costa's work[1] has been rediscovered. The two main techniques of multi-bit watermarking are: *lattice* codes also known as quantization-based codes (DC-QIM,[2] SCS,[3] P-QIM[4] ...) and *Dirty Paper Trellis Codes* (DPTC[5]). Those two categories of informed watermarking are both competitive but there is still some place for improvement. In this article, we focus on the quantization-based family.

The most effective image watermarking quantization-based is currently the P-QIM[4] scheme (Perceptual-QIM). The P-QIM algorithm use a scalar QIM[2] with an encoding of the message by a repetition code. We can identify three major contributions in P-QIM. The first contribution is to incorporate the RDM[6] principle using the psycho-visual amended Watson model.[7] The second contribution is to compute the modified Watson *slacks* on an already watermarked DCT block thereby avoiding drift between insertion and extraction. The latest contribution consists in pseudo-randomly shuffling the codeword obtained by a repetition code, instead of pseudo-randomly shuffling the host signal built from DCT coefficients.

We propose in our paper, a new algorithm named Hyper-Cube watermarking. Moreover, we give a clear framework which may easily be enriched in the future. The Hyper-Cube watermarking scheme incorporates and extends the proposals presented in the P-QIM algorithm. Two improvements are made. The first improvement is based on the choice of the block on which the modified Watson *slacks* are computed. In the P-QIM watermarking scheme, the selected block is always the left block or if the top block. We propose to select the adjacent block which is the most similar. The second improvement is to cleverly integrate a convolution code in order to code the message. Indeed, in the P-QIM algorithm, the embedding acts simply as repeating the bits from the message. We propose to use a convolution code well integrated in order to improve the correction performances. Finally, experimental tests have been achieved in order to test the feasibility of the scheme in a joint compression-watermarking approach. For those experiments, the size of the *lattice* (that is to say, the quantization step) is jointly based on the modified Watson *slacks* and on the quantization table used in JPEG.[8]

In section 2 we discuss the general principle of insertion and extraction. In section 3 we present the computation principle of the modified Watson *slacks* and their use. Section 4 deals of the integration of the convolution code. Finally, in Section 5 we present the results, and then we conclude.

Send correspondence to Marc.Chaumont@lirmm.fr.

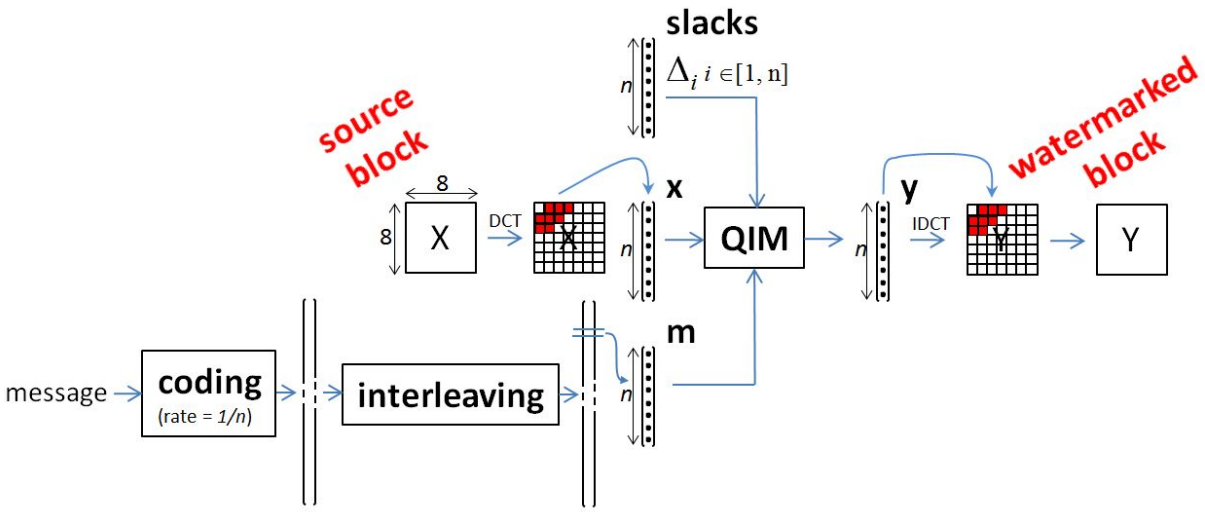


Figure 1. Hyper-Cube general scheme for a 8x8 pixels block.

2. EMBEDDING AND EXTRACTION

2.1 General scheme

Whether it be for P-QIM[4] algorithm or our Hyper-Cube algorithm, the general principle is substantially the same. The image is divided into 8x8 blocks, and one or more bits are embedded in each block. The embedding is summarized for an 8x8 block in Figure 1. The DCT transform is applied on the current block $\mathbf{X}$, then the first n ACs coefficients from the zig-zag scan are stored in a vector called the host signal and noted $\mathbf{x}$. Next, the n coefficients from $\mathbf{x}$ are watermarked using scalar QIM and thus n bits coming from the coded *message* are embedded (i.e vector $\mathbf{m}$ is embedded). For each of the n coefficients of $\mathbf{x}$ the quantization step (noted $\boldsymbol{\Delta}_i, i \in [1, n]$) necessary for the watermarking is a function of the modified Watson *slack* (see Figure 1 and Section 3.1) computed on a previously watermarked block.

2.2 Embedding

At the embedding, in our Hyper-Cube approach (it is similar for P-QIM), assuming that the interleaving function in Figure 1 is the identity function (i.e suppose that there is no interleaving), a message bit b is first encoded in a binary vector $\mathbf{m}$ consisting of n bits (the rate of the error correcting code is $1/n$; see Figure 1), then the watermarked signal $\mathbf{y}$ is obtained by quantifying each component of the host signal $\mathbf{x}$ with quantizers $\{Q_{\mathbf{m}[i]}\}_{i\in[1,n]}$ such that:

$$\forall i \in [1, n], \mathbf{y}[i] = Q_{\mathbf{m}[i]}(\mathbf{x}[i], \Delta_i), \tag{1}$$

with Δ_i the quantization step (see Section 3.2) associated with the i^{th} coefficient and quantizers Q_0 and Q_1 defined such that:

$$\begin{aligned} Q_0(\mathbf{x}[i], \Delta_i) &= 2\Delta_i \times round\left(\frac{\mathbf{x}[i]}{2\Delta_i}\right), \\ Q_1(\mathbf{x}[i], \Delta_i) &= 2\Delta_i \times round\left(\frac{\mathbf{x}[i] - \Delta_i}{2\Delta_i}\right) + \Delta_i. \end{aligned} \tag{2}$$

Note that our watermarking procedure is equivalent to displace the host signal $\mathbf{x}$ toward one of the vertex of the Hyper-Cube defined by the quantized points surrounding $\mathbf{x}$. This is why we named our algorithm: Hyper-Cube.

2.3 Extraction

At the extraction, for the P-QIM approach, authors compute the message bit b for a given watermarked-attacked word $\mathbf{z}$. This word $\mathbf{z}$ is retrieved from the first n ACs coefficients from the current DCT watermarked-attacked block. Assuming that the interleaving function is the identity function, the extraction of the message bit b is achieved as follow:

$$b = \arg \min_{\{b'\}} \min_{b' \in \{0,1\}} \sum_{i=1}^{i=n} (\mathbf{z}[i] - Q_{b'}(\mathbf{z}[i], \Delta_i))^2. \tag{3}$$

The extraction is more complicated for the Hyper-Cube approach since the message has been encoded with a convolution code2. It is done by taking into account the whole image. Assuming that the interleaving function is the identity function, each DCT block is associated to a transition step in the trellis of the convolution code. For a DCT block, we calculate n Euclidean distances: the distances $d_0[i] = (\mathbf{z}[i] - Q_0(\mathbf{z}[i], \Delta_i))^2, i \in [1, n]$ computed between the watermarked-attacked word $\mathbf{z}[i]$ and the scalar corresponding to an embedded bit 0, and the distances $d_1[i] = (\mathbf{z}[i] - Q_1(\mathbf{z}[i], \Delta_i))^2, i \in [1, n]$ computed between the word $\mathbf{z}[i]$ and the scalar corresponding to an embedded bit 1. The distances $d_0[i], i \in [1, n]$ ($d_1[i], i \in [1, n]$, respectively) are then carefully summed in order to label the transition arc of the trellis for the input bit 0 (and respectively, the transition arc for the input bit 1). The decoding is then achieved using the Viterbi algorithm.[9]

Equation 3 show that for P-QIM, a bit noted b is coded in n ACs coefficients similarly to a repetition code (repetition of n zeros or n ones) since the same quantizer Q_0 or Q_1 is used depending of the bit b. In the Hyper-Cube approach, the bit b is firstly encoded with a convolution code (instead of just repeating bits) in order to obtain n bits. Those n bits are then embedded using either Q_0 either Q_1.

3. MODIFIED WATSON SLACKS COMPUTATION

3.1 Modified Watson slacks

For a given 8x8 DCT block, the **modified** Watson *slack* associated with a DCT coefficient x in position $i \in [0, 63]$ is:[4]

$$s(x, i) = max(t_L^M[i], |x|^{0.7} t_L^M[i]^{0.3}), \tag{4}$$

with t_L^M the brightness mask:

$$t_L^M[i] = t[i] \left(\frac{C[0]}{C_0} \right)^{0.649} \left(\frac{C_0}{128} \right), \tag{5}$$

with $C[0]$ the DC coefficient of the DCT block, C_0 the average of all the DCs coefficients of the image, and $t[i]$ the sensitivity value with position i.[7] Compared to the Watson *slack*, the **modified** Watson *slack* scales linearly with coefficient scaling. This is indeed due to the following property:

$$\forall x \in \mathbb{R}, \forall i \in [0, 63], \forall \nu \in \mathbb{R}_+, s(\nu.x, i) = \nu.s(x, i). \tag{6}$$

A valumetric attack changing the amplitude of pixels with a scalar $\nu \in \mathbb{R}_+$ will thus scale the **modified** Watson *slacks* of a factor ν. This property allows building a quantization-based watermarking system less sensitive to the valumetric attack. This trick has been introduced in 2004 and is known has the Rational Dither Modulation (RDM) approach.[6]

3.2 JPEG quantization table integration

In the P-QIM algorithm, for each DCT coefficient, the quantization step of a DCT coefficient x is a function of the modified Watson *slack* as:

$$\Delta_i = G_{PQIM} \times s(x, i), \tag{7}$$

with $G_{PQIM} \in \mathbb{R}$ a constant tuning the embedding strength. A valumetric attack changing the amplitude of pixels with a scalar $\nu \in \mathbb{R}_+$ will cause a change in the quantization step of a single factor ν. The watermarking scheme is thus theoretically invariant to valumetric attack. Moreover it takes into account the psychovisual aspect.

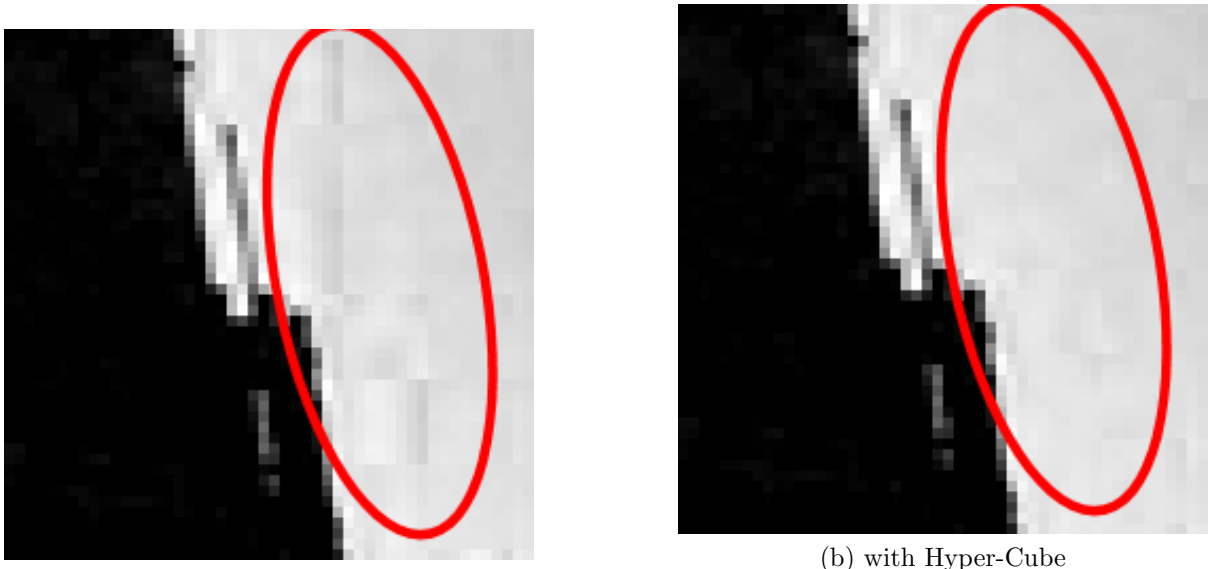
For the Hyper-Cube watermarking we decide, in the same manner as P-QIM, to tune the quantization step according to the modified Watson *slack* but also according to the quantization step of the JPEG quantization table $Q(i)$ (the table is the same as the one used in[5] with a quality factor fixed to 70):

$$\Delta_i = G_{HC} \times s(x,i) \times Q(i), \tag{8}$$

with $G_{HC} \in \mathbb{R}$ a constant tuning the embedding strength. Results show that this add do not degrade the performances. This gives an interesting property: the approach may easily be used in a joint compression-watermarking scheme. It is thus easy to use the modified Watson *slacks* in a watermarking scheme integrated in an image/video codec (for example JPEG[8] or H.264/AVC[10]). Moreover, it does not reduce the robustness performances.

3.3 Slacks on a neighborhood

The method proposed in P-QIM uses for the watermarking of the current block, the modified Watson *slacks* of the previously watermarked block (the block on the left of the current block if there is one, and the block on the top otherwise). There is thus no drift between modified Watson *slacks* values computed at the embedding and modified Watson *slacks* values computed at the extraction. In return, a "blocks trail" appears in strong contour areas (see inside the red circle in Figure 2.a).



(a) with P-QIM
(Block artifacts in the red circle).

(b) with Hyper-Cube
(No block artifacts in the red circle)
.

Figure 2. Part of image 1 from BOWS-2 data-base watermarked with a SSIM=98% and a payload=1/64; (a) with P-QIM; (b) with Hyper-Cube.

To remove this psychovisual disagreement, we must use better modified Watson *slacks* values while avoiding excessive drift between the modified Watson *slacks* used at the embedding and those used at the extraction. We thus determine for each block, the closest neighborhood block in the sense of the L2 distance. The computation is performed **in the spatial domain** by comparing each already watermarked adjacent block with the current block. Note that before achieving the comparisons **in the spatial domain**, we nullify the DCT coefficients used for the watermarking of the current block. This indeed reduce the drift effect during the extraction. Moreover, we limit the research area in order to reduce the drift likelihood. After various experiments, it appears that a good compromise is to consider only 2 blocks: the block above the current block and the block on the left of the current block. Experimental results show that the "blocks trail" disappear (see for example Figure 2.b) and that the robustness is almost unchanged.

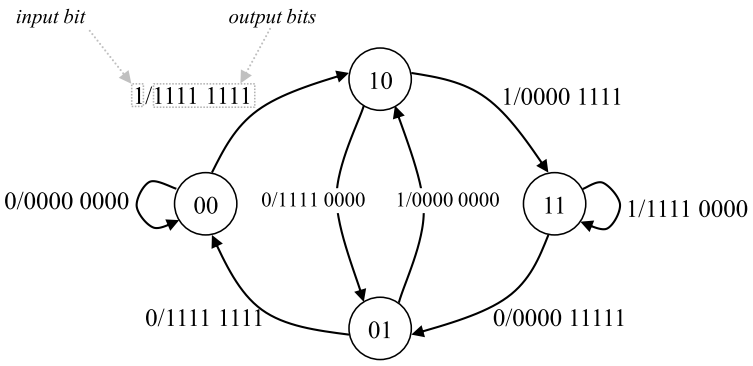


Figure 3. State machine of the convolution code 1/8-rate 2-memory.

4. MESSAGE CODING

In our implementation of P-QIM, 1 bit is embedded in each DCT block. More exactly 1 bit is embedded into n=9 coefficients ACs. The rate of the repetition code is thus 1/9 and the Hamming distance between the point (of dimension 9) representing 0 and the point (of dimension 9) representing 1 is 9. The repetition code can correct at most $\lfloor (9-1)/2 \rfloor = 4$ errors on 9 bits.

The use of codes more efficient than the repetition code improves the performance of the watermarking scheme. In the Hyper-Cube algorithm, we embed 1 bit in $n = 8$ coefficients ACs. We use a convolution code 1/8-rate 2-memory. The code 1/8-rate 2-memory is derived from a convolution code 1/2-rate 2-memory by repeating four times each output bit. The diagram of the state machine, for this 1/8-rate 2-memory code, is given in Figure 3. In our experiments, we also derived a code 1/8-rate 6-memories from the standard NASA code of $(133, 171)$ polynomial generators. Note that the add of a error correcting code necessitates to integrate a special soft decoding procedure as explain in Section 2.3.

5. RESULTS

The experiments were performed on the first 100 images of the BOWS-2 database* with images resized to 256×256.† These images are grayscale photos taken by amateurs and coded on 8 bits.

Four attacks to robustness have been tested: the Gaussian noise attack, the filtering attack, the valumetric scaling attack, and the JPEG compression attack. The four attacks are described in detail in.[5] The Bit Error Rate (BER) is computed from the extracted message and is equal to the number of erroneous bits divided by the total number of embedded bits. The BER is computed for each attack. We fixed the degradation to a SSIM[11] value of 98%‡.

We tested our propositions by progressively enriching an algorithm that we will name P-QIM. The algorithm that we name P-QIM in this paper is a somewhat modified version from the original.[4] For each block, only the first 9 ACs coefficients (zig-zag scan) are used for watermarking. There is no dithering but: the modified Watson *slacks* values of the current block are computed from the already watermarked left block or top block if there is no left block, the message is shuffled and encoded by a repetition code, the message is softly decoded using the sum of Euclidean distances. In the Figures 4, 5, 6, 7 the P-QIM curves are drawn in solid line.

The first test we achieved is to compute the quantization step depending not only on modified Watson *slacks* but also on the JPEG quantization table (see Section 3.2). This test is called "*+ slacks JPEG* " in the Figures.

*The BOWS-2 database is downloadable at http://bows2.gipsa-lab.inpg.fr/.

†The image sub-sampling has been achieved with the xnview program using Lanczos interpolation.

‡SSIM is a classical measure well correlated to the Human Visual System. The SSIM values are real positive numbers lower or equal to 1. Stronger is the degradation and lower is the SSIM measure. A SSIM value of 1 means that the image is not degrade. To compute the SSIM value, we use the C++ implementation of Mehdi Rabah available at http://mehdi.rabah.free.fr/SSIM/.

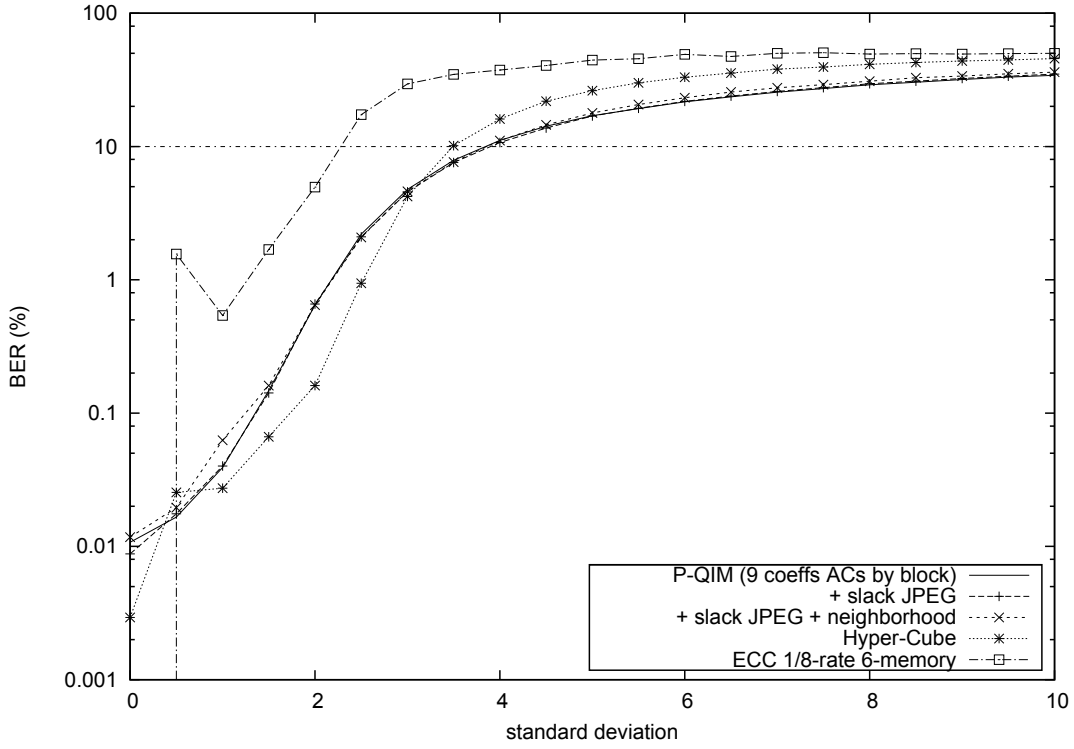


Figure 4. BER for the Gaussian noise attack.

The results are slightly better than the P-QIM approach using this addition. This proposal highlight the fact that P-QIM approach can be easily include in a joint watermarking-compression scheme (i.e. inside JPEG,[8] H.264,[10] ...).

The second test we achieved is to allow the choice of the block on which modified Watson *slacks* are computed. This test is called "*+ slacks JPEG + neighborood* " in Figures. The closest left or right neighbour block to the current block is used to compute the modified Watson *slacks* (see Section 3.3). The results, if we just stick to the curves, are slightly worse. This is because in some cases the decoder uses the bad block to compute the modified Watson *slacks*. Looking closer to the results, we find that although the value of SSIM is 98 %, the images obtained with P-QIM are of lower psychovisual quality since there is "block trail" artefacts. Thus, the "*+ slacks JPEG + neighborood* " approach outperform visually P-QIM if we use a subjective evaluation.

The third test we achieved is to encode the message with a more powerful code than the the repetition code used in P-QIM. The rate of the two tested convolution codes is 1/8. For each DCT block, we only take the first 8 ACs coefficients. We use the JPEG quantization step in the computation of the quantizing steps, we use the best neighborhood block to compute the modified Watson *slacks*, and we interleave the message codeword before embedding. Since there is codeword interleaving, precautions for distances computations should be taken during the decoding step (see Section 2.3). In the Figures, we note those two tests: *ECC* 1/8-*rate* 6-*memory* and *Hyper-Cube*. The results are good for the *Hyper-Cube* algorithm compared to P-QIM. At low-level attack, we obtain 0.3% BER less compared to P-QIM, while providing better psychovisual quality since there is a better choice for the modified Watson *slacks* values. It may be noted that the code *ECC* 1/8-*rate* 6-*memory* gives a null BER when there is no attack, but in return when the watermarking system is attacked, the BER increases dramatically. This type of catastrophic behaviour is not desirable for a watermarking scheme.

6. CONCLUSION

In this paper, we proposed a new algorithm that we named the Hyper-Cube approach. This algorithm takes part in the principles of the P-QIM approach by adding two new proposals, by giving a practical framework,

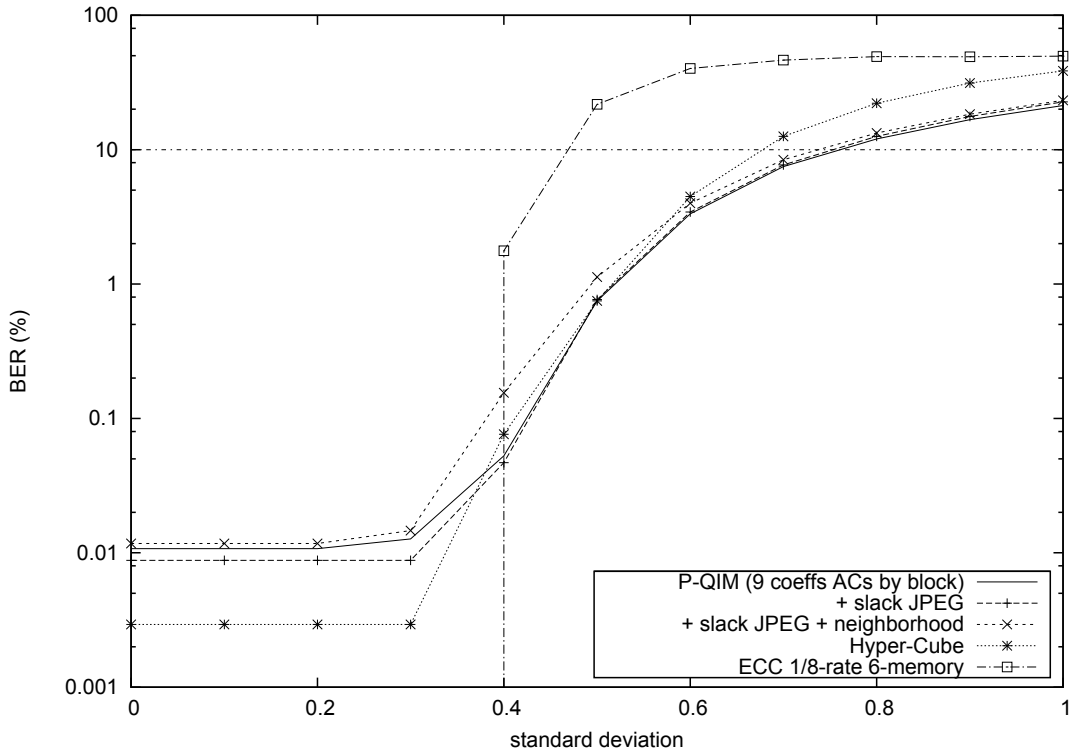


Figure 5. BER for the Gaussian filtering attack.

and by slightly modifying few parameters. The first proposal is to compute the modified Watson *slacks* on the most similar adjacent block. This approach leads to similar robustness performances, but in return provides images of better quality. The second contribution is to cleverly integrating a convolution encoding and decoding taking into account the pseudo-random interleaving of the message. Additionally, we propose to integrate the JPEG quantizations into the setting of the size of *lattices*. This proposal shows how easy it is to integrate the Hyper-Cube algorithm to a joint watermarking and compression scheme (JPEG or H.264). In conclusion, the Hyper-Cube watermarking scheme provides performance in terms of robustness and visual quality which are better than the P-QIM algorithm. Our future work will focus on the integration of the T-TCQ[12,13] in the Hyper-Cube scheme, the use of *lattices* suitable for large dimension,[14] and the robustness to additional attacks.[15]

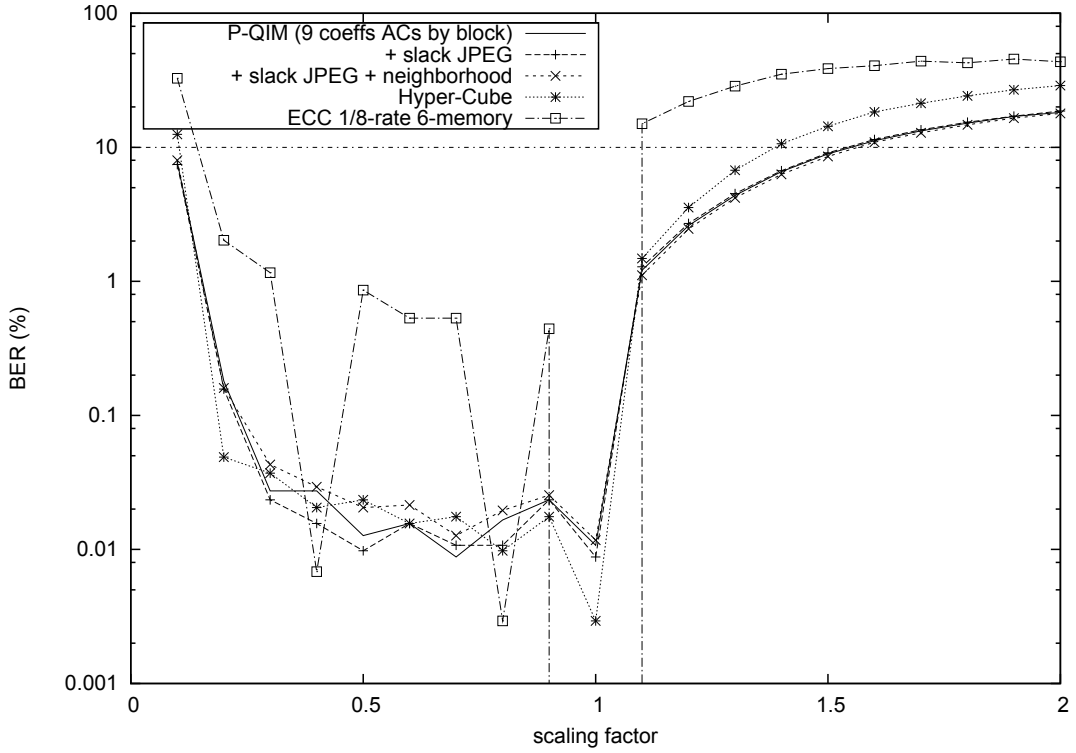


Figure 6. BER for the valumetric scaling attack.

REFERENCES

[1] Costa, M., "Writing on dirty paper," *IEEE Transactions on Information Theory* **29**(3), 439–441 (1983).

[2] Chen, B. and Wornell, G., "Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding," *IEEE Transactions on Information Theory* **47**(4), 1423–1443 (2001).

[3] Eggers, J. J., Bäuml, R., Tzschoppe, R., and Girod, B., "Scalar Costa Scheme for Information Embedding," *IEEE Transactions on Signal Processing* **51**(4), 1003–1019 (2003).

[4] Li, Q. and Cox, I., "Using Perceptual Models to Improve Fidelity and Provide Resistance to Valumetric Scaling for Quantization Index Modulation Watermarking," *IEEE Transactions on Information Forensics and Security* **2**(2), 127–139 (2007).

[5] Miller, M. L., Doërr, G., and Cox, I. J., "Applying Informed Coding and Informed Embedding to Design a Robust, High Capacity Watermark," *IEEE Transactions on Image Processing* **13**(6), 792–807 (2004).

[6] Pérez-González, F., Barni, M., Abrardo, A., and Mosquera, C., "Rational Dither Modulation: A Novel Data-hiding Method Robust to Valuemetric Scaling Attacks," in [*IEEE International Workshop on Multimedia Signal Processing, IWMSP'2004*], 139–142 (sep. 2004).

[7] Watson, A. B., "DCT Quantization Matrices Optimized for Individual Images," in [*Human Vision, Visual Processing, and Digital Display IV, SPIE'1993*], **1913**, 202–216 (1993).

[8] "ISO/IEC IS 10918-1 — ITU-T Recommendation T.81," tech. rep., ISO and ITU-T (1991).

[9] Viterbi, A. J., [*CDMA: Principles of Spread Spectrum Communication*], Addison-Wesley Wireless Communications (1995).

[10] "Draft ITU-T Recommendation and Final Draft International Standard of Joint Video Specification (ITU-T REC. H.264 ISO/IEC 14496-10 AVC)," tech. rep., Joint Video Team (JVT) (2003).

[11] Wang, Z., Bovik, A. C., Sheikh, H. R., and Simoncelli, E. P., "Image Quality Assessment: From Error Visibility to Structural Similarity," *IEEE Transactions on Image Processing* **13**(4), 600–612 (2004).

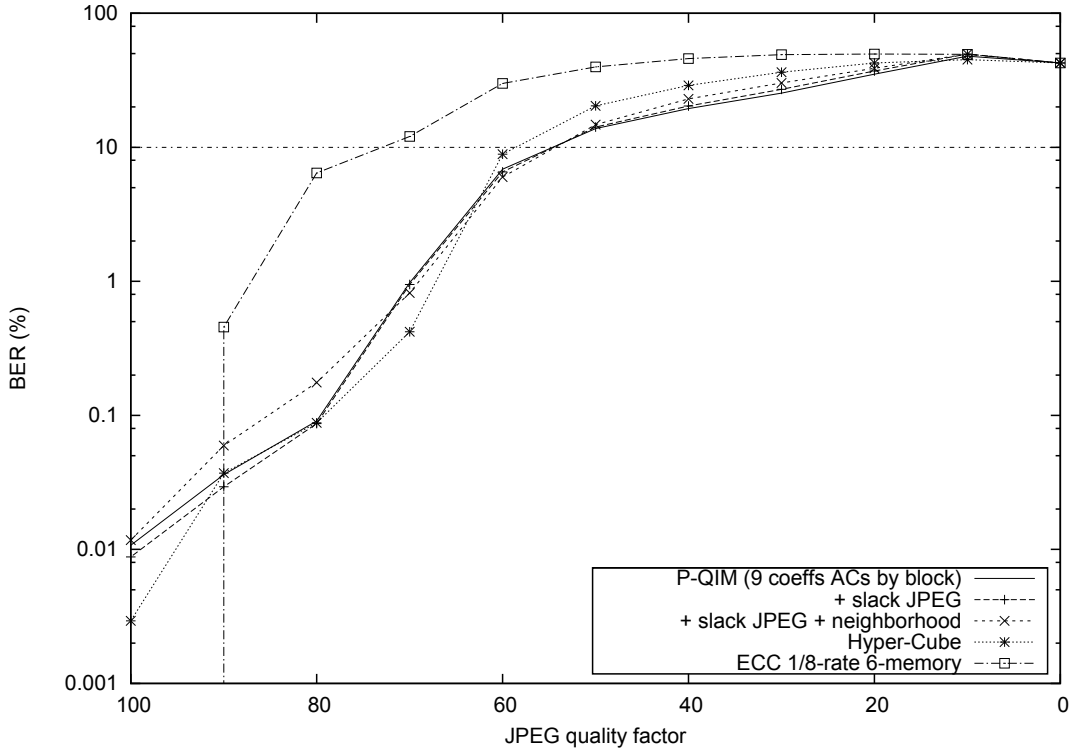


Figure 7. BER for the JPEG compression attack.

[12] Le Guelvouit, G., "Trellis-Coded Quantization for Public-key Watermarking," **Initially accepted** for IEEE International Conference on Acoustics, Speech and Signal Processing, ICASP'2005 (mar. 2005).

[13] Le Guelvouit, G., "Tatouage Robuste d'Images par Turbo TCQ," *Traitement du Signal* **25** (apr. 2009).

[14] Bardyn, D., Dooms, A., Dams, T., and Schelkens, P., "Comparative Study of Wavelet Based Lattice QIM Techniques and Robustness against AWGN and JPEG Attacks," in [*8th International Workshop on Digital Watermarking, IWDW'2009*], Ho, A. T., Shi, Y. Q., Kim, H., and Barni, M., eds., *Lecture Notes in Computer Science* **5703**, 39–53, Springer, University of Surrey, Guildford, United Kingdom (aug. 2009).

[15] Zhu, X. and Tang, Z., "Improved Quantization Index Modulation Watermarking Robust Against Amplitude Scaling Distortions," in [*IEEE International Conference on Multimedia & Expo, ICME'2008*], 237–240 (june 2008).