A Novel Embedding Technique For Dirty Paper Trellis Codes Watermarking

Marc Chaumont

A Novel Embedding Technique for Dirty Paper Trellis Codes Watermarking

Marc Chaumont[a,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

Dirty Paper Trellis Codes (DPTC) watermarking, published in 2004, is a very efficient high rate scheme. Nevertheless, it has two strong drawbacks: its security weakness and its CPU computation complexity. We propose an embedding space at least as secure and a faster embedding. The embedding space is built on the projections of some wavelet coefficients onto secret carriers. It keeps a good security level and has also good psycho-visual properties. The embedding is based on a dichotomous rotation in the Cox, Miller and Boom Plane. It gives better performances than previous fast embedding approaches. Four different attacks are performed and revealed good robustness and rapidity performances.

Keywords: Watermarking, Dirty Paper Trellis Codes, High rate, Informed-coding, Informed-embedding, Robustness, Secure embedding space, Rotation-based embedding, RB-DPTC.

1. INTRODUCTION

The generation of watermarking schemes named informed schemes or side information schemes appeared around 1998 when Costa's work has been rediscovered.[1] The two principal techniques' categories for multi-bits watermarking are the lattice codes also named quantized based watermarking schemes (DC-QIM,[2] SCS..[3]) and the Dirty Paper Trellis Codes (DPTC).[4]

The original DPTC algorithm is known for its good robustness and its high embedding payload but own two strong weaknesses: the *informed embedding* step uses a Monte Carlo approach which is very CPU time consuming and the scheme owns security weakness facing collusion attack.[5] In that paper, we thus propose a DPTC at least as secure and less complex.

Lin *et al.*[6] propose to replace the Monte Carlo approach with a non-optimal technique but of low complexity. We propose an even more efficient solution. We use the wavelet domain which gives less blocking effects than the DCT domain. In order to counter-attack the security hole given in,[5] we embed in a secret space. Finally, since our technique is rapid and the space well adapted, we increase the trellis size (i.e. the codebook' size) and thus the robustness-distortion efficiency.[7]

In Section 2, we remind the principle of the original Dirty Paper Trellis Codes (DPTC).[4] In Section 3 we present the embedding space and the embedding algorithm. In Section 4 we compare the original DPTC,[4] the Lin *et al.* approach[6] and our *rotation-based* approach (RB-DPTC).

2. DPTC WATERMARKING SCHEME

The original DPTC scheme applied on a $N = 240 \times 368$ image is shown on Fig.1. The first step of the scheme is the image transformation into a spatio-frequential space (DCT transformation) in order to obtain the host signal $\mathbf{x}$. In the original scheme, an image is 8×8 DCT transformed, the twelve first ACs coefficients of each DCT blocks are extracted and pseudo-randomly ordered in a vector $\mathbf{x}$ of size $12 \times N/64 = 3 \times N/16$. The second step of the DPTC scheme is the *informed coding*. The input message m is coded into a codeword $\mathbf{c}^*$ by taking

Send correspondence to Marc.Chaumont@lirmm.fr.
Telephone: + (33)4.67.41.85.14; Fax: + (33)4.67.41.85.00.
Website: http://www.lirmm.fr/~chaumont.

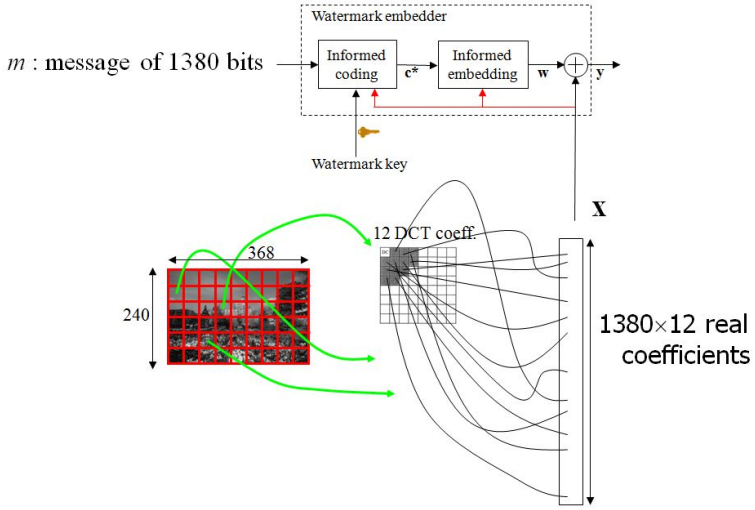

Figure 1. Dirty Paper Trellis Codes apply on a 240 × 368 image.

into account the host signal $\mathbf{x}$. The last step of the DPTC scheme is the *informed embedding*. It consists in modifying the host signal $\mathbf{x}$ in order to "put-it" in the Voronoï region of the codeword $\mathbf{c}^*$. Let's now define more precisely the trellis structure, the informed coding and the informed embedding.

2.1 Trellis structure

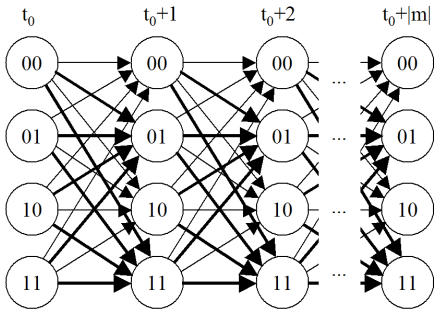

Figure 2. Dirty paper code's trellis with 4 states and 4 arcs per state.

In DPTC,[4] a special trellis is used. In this trellis, each state owns multiple possible transitions given an input bit. Each transition generates outputs coefficients. Fig.2 gives an example of a trellis with 4 states and 4 arcs per state. With this trellis, an input sequence owns multiple possible output codewords (a codeword is the result of the concatenation of outputs coefficients) since for each state there is multiple possible transitions for the same input bit. This signifies that an input sequence may be coded with different codewords. This property is essential in informed watermarking. In the original DPTC algorithm, the trellis own 64 states, 64 arcs per state and there is $N_{arc} = 12$ real coefficients pseudo-randomly generated as output arcs values.

2.2 Informed coding

The set of all the trellis paths i.e. all the possible outputs sequences, is the codebook $\mathcal{C}$ of the coder. A codeword $\mathbf{c}^i \in \mathcal{C}$ is the resultant coding of a message m. The informed coding is a way to choose the codeword $\mathbf{c}^i$ (encoding a given message m) the closest (for a given distance) to the host signal $\mathbf{x}$. Thus, informed coding allows to encode a message m by taking into account the host signal $\mathbf{x}$.

In the DPTC algorithm, given a message m, the informed coding is achieved:

- by pruning the trellis in order to keep the only valid paths. Thus, for a given transition, there is only the 0 input arcs or the 1 input arcs;
- by running a Viterbi decoder algorithm on this prune trellis in order to find the closest codeword $\mathbf{c}^*$. The distance used in order to compare the codewords with the original host $\mathbf{x}$ is the scalar product (the scalar product is a classical correlation measure). The Viterbi decoder thus retains the path (i.e. the codeword $\mathbf{c}^*$) of highest correlation with the host signal $\mathbf{x}$.

2.3 Informed embedding

In the original DPTC algorithm,[4] a Monte Carlo approach is used in order to displace the host signal $\mathbf{x}$ into the Voronoï region of the codeword $\mathbf{c}^*$. This embedding is achieved in order to meet a given robustness. Moreover the modification of $\mathbf{x}$ is achieved by taking into account the psycho-visual degradation by using the Watson perceptual measure.[8] The Monte Carlo principle is iterative and consists to attack and counter-attack a watermarked signal $\mathbf{y}$.

The Monte Carlo approach requires to run the Viterbi algorithm a high number of times. Even with the proposed optimizations in,[4] the time complexity is very high and this is at present a strong brake for intensive experiments studies and also for its use in industry. The DPTC watermarking scheme is thus seriously competed with faster quantization-based approaches.[2,3]

3. NEW EMBEDDING APPROACH

In this section, we present our new embedding space, our embedding approach and discuss about our proposition.

3.1 Embedding space

The recent work of Bas and Doërr[5] about security of DPTC shows that in the Kerckhoffs's framework,[9] i.e. when embedding and extracting algorithms are known by an attacker, the trellis codebook may be retrieved by observing a large number of watermarked images. Those conclusions are drawn based on a simplified version of the DPTC algorithm (non pseudo-random-ordering of DCT coefficients) but show a certain security weakness of DPTC.[4] The private space, that we use in this paper, allows to hide the structure of the trellis. A security attack based on the principle exposed in[5] is thus at least as difficult to lead with our proposition. Moreover, it is certainly very difficult to estimate the secret projections in the same way as[10] since there is a high number of codewords (with a trellis made of 128 states and 128 arcs per state and with a payload of 1024 bits, there is more than 10^{387} codewords).

Fig.3 illustrates our proposition : the Rotation-Based Dirty Trellis Codes (RB-DPTC). Our new embedding space is obtained by first, a wavelet transform of the image, and second, projections of the host signal $\mathbf{x}$ of dimension N_{wlt} ($\mathbf{x}$ is the concatenation of sub-bands coefficients except LL sub-band's coefficients) onto N_{sec} carriers (noted $\mathbf{u}_i$ with $i \in [1, N_{sec}]$). Note that a projection is just a scalar product. The obtained vector $\mathbf{v_x}$ of dimension N_{sec} may then be used for the informed-coding (see Section 2.2) and informed-embedding (see Section 2.3).

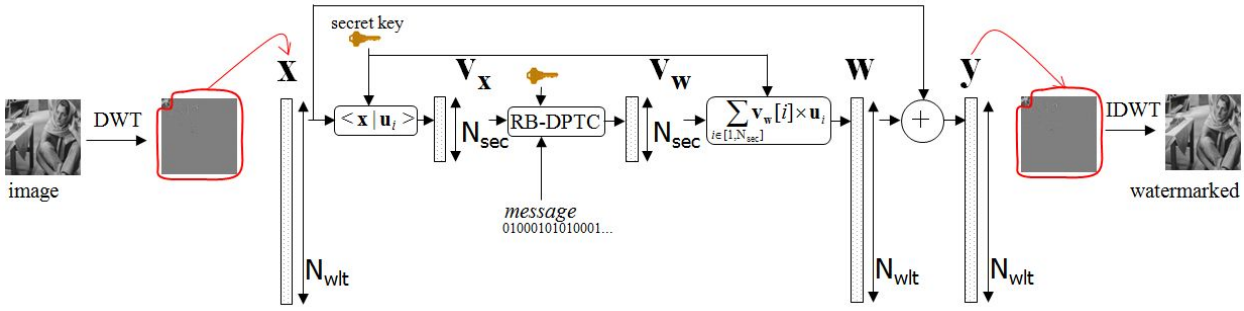

Figure 3. Our Rotation-Based Dirty Paper Trellis Codes (RB-DPTC) scheme.

This embedding space is at least as secure than the original one and it allows to spread the watermark signal on almost all the frequency domain (no super-robustness[11]). Moreover, the projections onto N_{sec} carriers give to the embedding space a Gaussian aspect which is known for its good property for the channel capacity.[1] Finally, the wavelet domain is known for its good psycho-visual properties and is less disturbing than the block effects present in the DPTC.[4]

3.2 Embedding algorithm

The informed coding in our approach is the same than the original one (see section 2.2) but is achieved with the host vector $\mathbf{v_x}$ (secret space). After achieving the informed coding, the codeword $\mathbf{c}^*$ is extracted. The Lin *et al.*[6] solution, in order to speed-up the embedding, and keeps a good robustness-distortion tradeoff, is not satisfying since the degradation is too strong. Our solution is not optimal but gives better results (The Lin *et al.* solution is also non optimal).

Remember that **at the decoder**, the most correlated codeword $\tilde{\mathbf{c}^*}$ is obtained by running the Viterbi algorithm. This codeword $\tilde{\mathbf{c}^*}$ belongs to the codebook $\mathcal{C}$ and maximizes the correlation with the attacked-watermarked vector $\tilde{\mathbf{v_y}}$ such that:

$$\begin{aligned}\tilde{\mathbf{c}^*} &= \arg\max_{\mathbf{c}^i \ \forall \mathbf{c}^i \in \mathcal{C}} (\tilde{\mathbf{v_y}}.\mathbf{c}^i) \\ &= \arg\max_{\mathbf{c}^i \ \forall \mathbf{c}^i \in \mathcal{C}} (||\tilde{\mathbf{v_y}}||.||\mathbf{c}^i||.cos\theta_i),\end{aligned}$$

with θ_i the angle between $\tilde{\mathbf{v_y}}$ and $\mathbf{c}^i$. Thus, the highest correlation gives the closest codeword $\tilde{\mathbf{c}^*}$ and the retrieved message m'.

Knowing that all the codewords own the same norm, the Viterbi algorithm extracts the codeword $\mathbf{c}^i$ owning the smallest angle with $\tilde{\mathbf{v_y}}$. The idea, in order to embed the message m at the coder side, is thus to reduce the angle between the host vector $\mathbf{v_x}$ and the codeword $\mathbf{c}^*$ until obtaining the smallest angle regarding all the other angles $(\widehat{\mathbf{v_x}, \mathbf{c}^i})$.

In order to reduce the angle between $\mathbf{v_x}$ and $\mathbf{c}^*$, we first express these two vectors in the Miller, Cox and Bloom plane (*abbr.* MCB plane).[12] Fig.4 illustrates this MCB plane. The MCB plane is defined by an ortho-normalize basis ($\mathbf{v_1}$, $\mathbf{v_2}$) such that $\mathbf{v_x}$ and $\mathbf{c}^*$ belong to that plane (Gram-Schmidt algorithm):

$$\begin{aligned}\mathbf{v_1} &= \frac{\mathbf{c}^*}{||\mathbf{c}^*||}, \\ \mathbf{v_2} &= \frac{\mathbf{v_x} - (\mathbf{v_x}.\mathbf{v_1})\mathbf{v_1}}{||\mathbf{v_x} - (\mathbf{v_x}.\mathbf{v_1})\mathbf{v_1}||}.\end{aligned}$$

In the MCB plane, the 2D coordinates of the host vector $\mathbf{v_x}$ are:

$$\begin{aligned}\mathbf{v_x^{2D}}(1) &= \mathbf{v_x}.\mathbf{v_1}, \\ \mathbf{v_x^{2D}}(2) &= \mathbf{v_x}.\mathbf{v_2},\end{aligned}$$

and the 2D coordinates of the codeword $\mathbf{c}^*$ are:

$$\begin{aligned}\mathbf{c^*_{2D}}(1) &= ||\mathbf{c}^*||, \\ \mathbf{c^*_{2D}}(2) &= 0.\end{aligned}$$

A rotation of the host vector $\mathbf{v_x^{2D}}$ of a θ angle in the MCB plane is such that:

$$\begin{aligned}\mathbf{v_y^{2D}}(1) &= cos\theta.\mathbf{v_x^{2D}}(1) - sin\theta.\mathbf{v_x^{2D}}(2), \\ \mathbf{v_y^{2D}}(2) &= sin\theta.\mathbf{v_x^{2D}}(1) + cos\theta.\mathbf{v_x^{2D}}(2).\end{aligned}$$

If we reduce the absolute angle between the host vector $\mathbf{v_x}$ and the codeword $\mathbf{c}^*$ in the MCB plane, it increases the correlation $\mathbf{v_x}.\mathbf{c}^*$. With a dichotomous approach on rotation angle, one can rapidly found a Voronoï frontier. The algorithm for obtaining this Voronoï frontier is iterative and dichotomous (there is less than 10 trials):

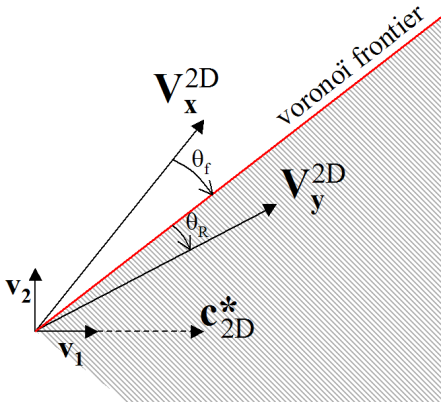

Figure 4. Rotation-based embedding in the Miller, Cox and Bloom plane.

1. rotate $\mathbf{v_x}$ and obtain $\mathbf{v_y}$ in the MCB,
2. run the Viterbi algorithm to check if $\mathbf{v_y}$ belongs or not to the Voronoï region of $\mathbf{c}^*$ i.e. that the decoded vector is equal or not to $\mathbf{c}^*$.
3. modify (dichotomous approach) the rotation angle depending on Voronoï region's belonging. Return to 1.

Once the frontier angle θ_f in the MCB is found, we improve the embedding robustness by penetrate inside the Voronoï region with a given angle θ_R. Our informed embedding is thus a rotation of $\mathbf{v_x}$ of an oriented angle equals to the $\max(\theta_f + \theta_R, (\widehat{\mathbf{v_x}, \mathbf{c}^*}))$. Fig.4 illustrates $\mathbf{v_x}$, $\mathbf{v_y}$, θ_f and θ_R in the MCB plane.

4. RESULTS

Tests were carried on the first 100 images of the BOWS2 data-base* with images resized to 256×256†. Those images are 8-bits grey-level images and are personal photos.

The trellis structure owns 128 (resp. 64) states with 128 (resp. 64) arcs per states for Lin *et al.* **cone-based** algorithm and our **rotation-based** algorithm (resp. for the **original DPTC**). Outputs arcs labels are drawn from a Gaussian distribution and there are 12 coefficients by output arc. The payload is 1 bit for 64 pixels which is the same as the original DPTC algorithm.[4] The number of embedded bits is thus 1024 bits.

For Lin *et al.* cone-based algorithm and our rotation-based algorithm, Wavelet transform is a 9/7 Daubechies with $l = 3$ decompositions levels. Except the LL sub-band, all the other sub-bands are used to form the host signal $\mathbf{x}$. With 256×256 images, the wavelet space size is thus $N_{wlt} = 64\,512$ coefficients. Knowing that the payload is 1/64 *bits per pixel* and that the number of outputs coefficients for an arc is $N_{arc} = 12$ coefficients, the private space size is thus $N_{sec} = 1024 \times 12 = 12\,288$ coefficients. The carriers $\mathbf{u}_i$ are built from normalized bipolar pseudo-random sequences.

Four kinds of robustness attacks have been applied: Gaussian noise attack, Gaussian filtering attack, valumetric attack and jpeg attack. The Bit Error Rate (BER) is the number of erroneous extracted bits divided by the total number of embedded bits. The BER is computed for each attack. Three algorithms are competing: the **original DPTC** with an average embedding PSNR = 42.6 dB, the Lin *et al.* **cone-based** algorithm with the robustness set to a noise power of $n^2 = 1$ (it corresponds to $R_t = 1$ in the paper[6]) and an average embedding PSNR = 34.2 dB (Note that it is impossible to increase the Lin *et al.* PSNR. Indeed, their technique is really sub-optimal with real images), and our **rotation-based** algorithm with the inside angle penetration set to $\theta_R = 0.1$ radian and an average embedding PSNR = 42.4 dB.

*BOWS2 data-base is located at http://bows2.gipsa-lab.inpg.fr/.

†The images subsampling has been achieved with xnview program and using Lanczos interpolation.

In Figure 5, 6, 7, 8 we observe the different BER results for the four different attacks. The Lin *et al.* curves just give an idea of the BER bound. They may not be used for fair comparison, since the average embedding PSNR is only of 34.2 dB. We should conclude that Lin *et al.* algorithm may not be used as a faster DPTC[4] substitute, since it is not able to achieved a reasonable PSNR of 42 dB. Comparison are thus only achieved between the **original DPTC** and the **rotation-based** algorithm.

For the comparison, we just look at BER below 10% which is large enough. With this criteria, the **rotation-based** algorithm performs identical or close results to the **original DPTC** algorithm for filtering and Gaussian attack. The two approaches strongly differ with jpeg and valumetric scaling. For the jpeg attack, the **original DPTC** performs very good robustness whereas the **rotation-based** is not robust at all. Results are opposite for the valumeric scaling, since the **rotation-based** is really better than the **original DPTC**.

We should then conclude that our **rotation-based** approach is the currently best approach in order to reduce the **original DPTC** complexity. Moreover, our approach assures a good security by using a secure embedding space as in.[13] The approach should nevertheless be improved in order to be robust to jpeg compression.

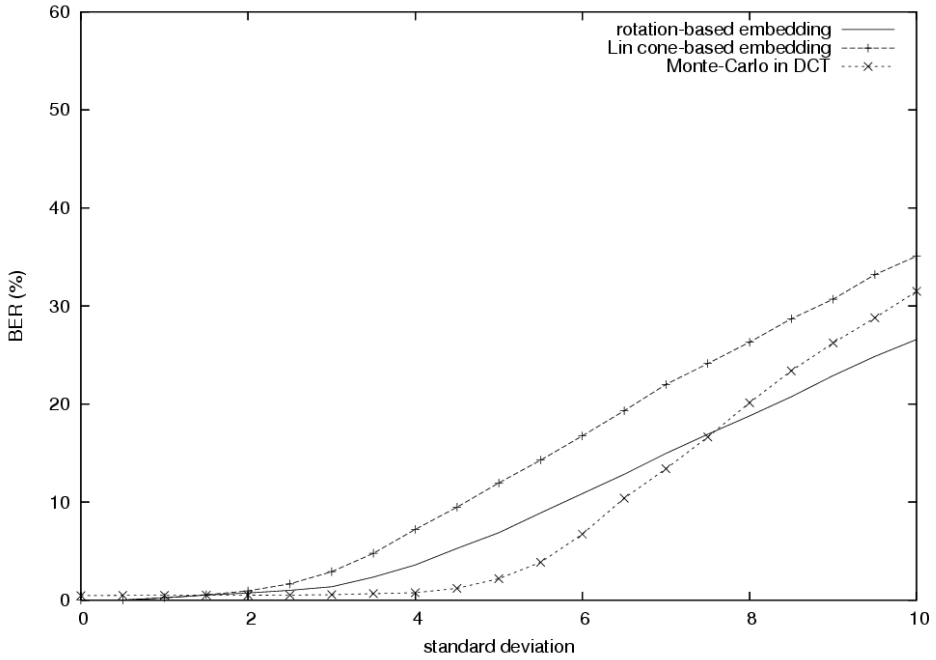

Figure 5. BER for Gaussian noise attack on the original DPTC algorithm (average PSNR = 42.6 dB), on Lin *et al.* cone-based algorithm (average PSNR = 34.2 dB) and on our rotation-based algorithm (average PSNR = 42.4 dB).

5. CONCLUSION

In that paper, we introduce a new Dirty Trellis Paper Codes algorithm (the Rotation-Based Dirty Paper Trellis Codes : RB-DPTC). Compared to the original algorithm, the wavelet domain is used instead of the DCT one. The security is assured by the add of a secret embedding space. This secret space is obtained by projecting the wavelet coefficients onto quasi-orthogonal carriers. Those projections also ensure (during the retro-projections) a spreading of the watermark on the majority of wavelet coefficients. Another interesting point is the embedding proposition based on a penetration into the Voronoï region of interest. This penetration necessitate first, to localize a frontier thanks to few rotations trials and second, to rotate of a fixed angle. The obtained results are good in comparison to the state of the art original DPTC.[4]

We explained how to reduce CPU complexity of the projections step in.[14] We also studied the psychovisual aspects in.[15] Future work will improve the robustness to the jpeg attack. The trellis structure and the codeword

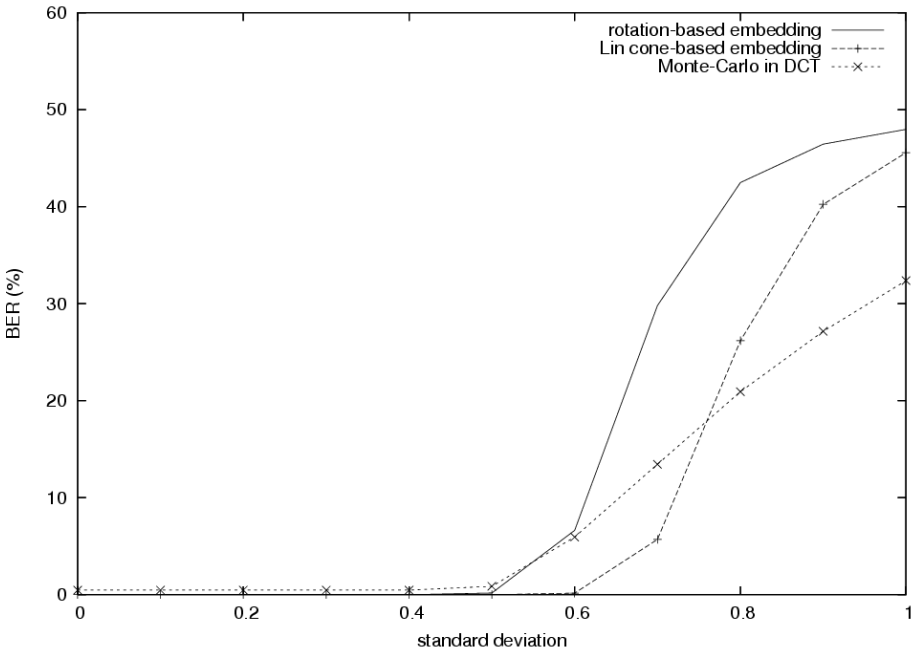

Figure 6. BER for Gaussian filtering attack on the original DPTC algorithm (average PSNR = 42.6 dB), on Lin *et al.* cone-based algorithm (average PSNR = 34.2 dB) and on our rotation-based algorithm (average PSNR = 42.4 dB).

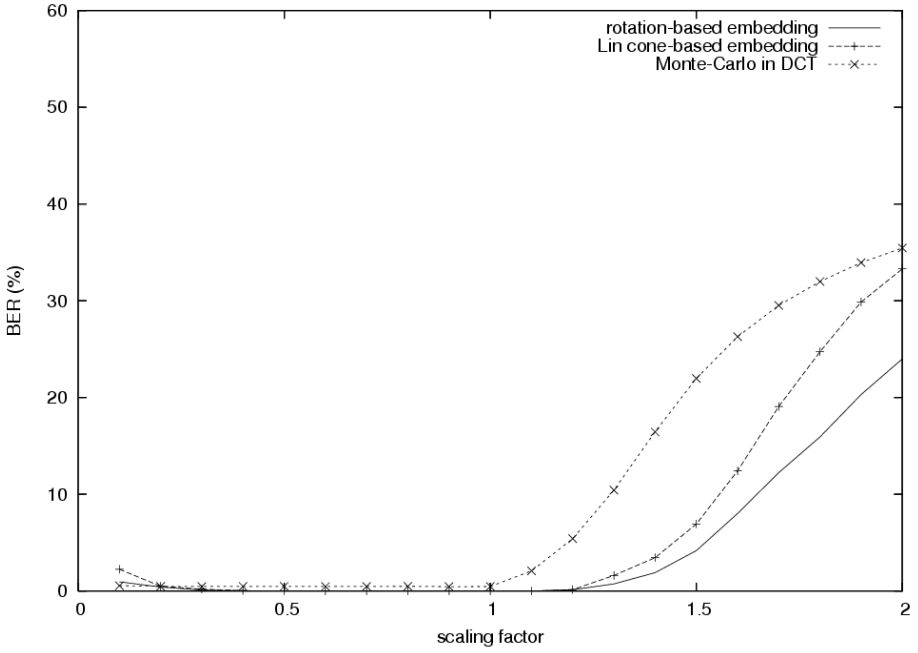

Figure 7. BER for valumetric up and down scaling attack on the original DPTC algorithm (average PSNR = 42.6 dB), on Lin *et al.* cone-based algorithm (average PSNR = 34.2 dB) and on our rotation-based algorithm (average PSNR = 42.4 dB).

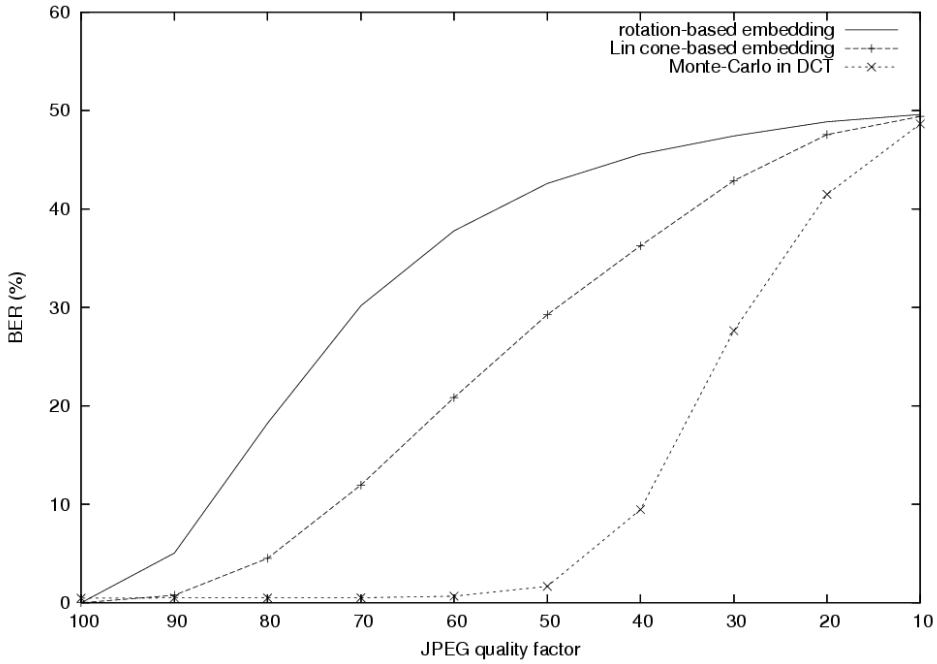

Figure 8. BER for jpeg attack on the original DPTC algorithm (average PSNR = 42.6 dB), on Lin *et al.* cone-based algorithm (average PSNR = 34.2 dB) and on our rotation-based algorithm (average PSNR = 42.4 dB).

construction should also be clarified as exposed in.[16] Security of our approach should also be evaluated as it has been done for the original DPTC in[5] and for the Broken Arrows algorithm in.[10]

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] Miller, M. L., Doërr, 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**(6), 792–807 (2004).

[5] Bas, P. and Doërr, G., "Evaluation of an Optimal Watermark Tampering Attack Against Dirty Paper Trellis Schemes," in [*10th ACM workshop on Multimedia and Security, MM&Sec'2008*], 227–232 (Sept. 2008).

[6] Lin, L., Cox, I. J., Doërr, G., and Miller, M. L., "An Efficient Algorithm for Informed Embedding of Dirty Paper Trellis Codes for Watermarking," in [*IEEE International Conference on Image Processing, ICIP'2005*], **1**, 697–700 (Sept. 2005).

[7] Wang, C., Doërr, G., and Cox, I. J., "Toward a Better Understanding of Dirty Paper Trellis Codes," in [*IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP'2006*], **2**, 233–236 (May 2006).

[8] 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).

[9] Kerckhoffs, A., "La Cryptographie Militaire," *Journal des Sciences Militaires* **IX** (pp. 5-38 Jan. 1883, pp. 161-191, Feb. 1883).

[10] Bas, P. and Westfeld, A., "Two Key Estimation Techniques for the Broken-Arrows Watermarking Scheme," in [*11th ACM workshop on Multimedia and Security, MM&Sec'2009*], 1–8, ACM (Sept. 2009).

[11] Craver, S., Atakli, I., and Yua, J., "How we broke the BOWS watermark," in [*IS&T/SPIE 19th Annual Symposium on Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents IX edited by Edward J. Delp III, Ping Wah Wong, SPIE'2007*], **6505**, 1–8 (Jan. 2007).

[12] Cox, I., Miller, M., Bloom, J., Fridrich, J., and Kalker, T., [*Digital Watermarking and Steganography*], ch. 5, 142–143, in Multimedia Information and Systems, Morgan Kaufmann, 2nd ed. (Nov. 2007).

[13] Furon, T. and Bas, P., "Broken Arrows," *EURASIP Journal on Information Security* **2008** (2008).

[14] Chaumont, M., "Fast Embedding Technique For Dirty Paper Trellis Watermarking," in [*8th International Workshop on Digital Watermarking, IWDW'2009*], 110–120, Springer-Verlag, Berlin, Heidelberg (Aug. 2009).

[15] Chaumont, M., "Psychovisual Rotation-based DPTC Watermarking Scheme," in [*17th European Signal Processing Conference, EUSIPCO'2009*], (Aug. 2009).

[16] Wang, C., Doërr, G., and Cox, I. J., "Trellis Coded Modulation to Improve Dirty Paper Trellis Watermarking," in [*IS&T/SPIE 19th Annual Symposium on Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents IX edited by Edward J. Delp III, Ping Wah Wong, SPIE'2007*], **6505**, 0G1–0G10 (Jan. 2007).

ACKNOWLEDGMENTS

This investigation was supported by the VOODDO project which is a French national project of the ANR (*Agence Nationale de la Recherche*) "Contenu et Interaction". We would also like to thank the Languedoc-Roussillon Region.