Fast Embedding Technique for Dirty Paper Trellis Watermarking

Marc Chaumont

University of Nîmes, Place Gabriel Péri, 30000 Nîmes, France
University of Montpellier II, Laboratory LIRMM, UMR CNRS 5506,
161, rue Ada, 34392 Montpellier cedex 05, France
marc.chaumont@lirmm.fr,
WWW home page: http://www.lirmm.fr/~chaumont

Abstract. This paper deals with the improvement of the Dirty Paper Trellis Code (DPTC) watermarking algorithm. This watermarking algorithm is known to be one of the best among the high rate watermarking schemes. Nevertheless, recent researches reveal its security weakness. Previously, we proposed to reinforce its security by using a secret space before the embedding. This secret space requires to compute projections onto secrets carriers. When dealing with high rate watermarking, the CPU cost for those projections is dramatically high. After introducing the watermarking scheme, we then propose two Space Division Multiplexing (SDM) approaches which reduce the complexity. Evaluations are achieved with four different attacks and show that our proposal gives better robustness results with SDM approaches.

1 Introduction

Dirty Paper Trellis Codes (DPTC) [1] watermarking is one of the most efficient high rate schemes. Nevertheless, it suffers of two major drawbacks: its CPU computational complexity for the embedding part and its security weakness. In this paper we propose to carry on the work proposed in [2] which gives a nice way to improve those two drawbacks while preserving a good robustness.

The recent work of Bas and Doërr [3] about security of DPTC [1] shows that in the Kerckhoffs's framework [4], i.e. when the embedding and extracting algorithms are known by an attacker, the trellis codebook may be retrieved observing a large number of watermarked images. Those conclusions are drawn based on a simplified version of the DPTC algorithm (non random-ordering of DCT coefficients) but show a certain security weakness of DPTC [1]. In [2], we proposed to use a *private embedding space* in order to better hide the structure of the trellis. Moreover, we provided a fast embedding strategy.

The *private space* is obtained by vector projections. If achived directly, the vector projections give a quadratic CPU complexity. In that paper, we propose two different Space Division Multiplexing (SDM) approaches in order to reduce the quadratic complexity to a linear one.

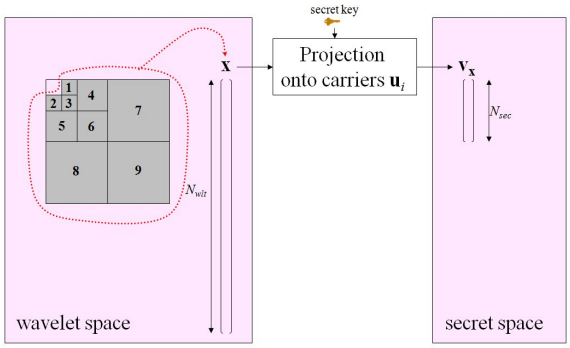

Fig. 1. Construction scheme of the secret embedding space.

In section 2, we briefly present the embedding space and the embedding approach already presented in [2]. In section 3, we present two SDM approaches in order to reduce the projections complexity. Finally, in section 4 we evaluate the schemes and conclude to the good behavior of the SDM approaches.

2 New embedding approach

In this section, we remind the embedding space and the embedding approach proposed in [2].

2.1 Embedding space

The embedding space is obtained by first, a wavelet transform of the image, and second, a projection 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 of same dimension. Carriers are denoted $\mathbf{u}_i$ with $i \in [0, N_{sec} - 1]$. Note that a projection is just a scalar product. Figure 1 illustrates the construction of the host signal $\mathbf{x}$ and the host vector (secret space) $\mathbf{v_x}$. The obtained vector $\mathbf{v_x}$ may then be used for the *informed-coding* and *informed-embedding* (see Section 2.2).

The carriers $\mathbf{u}_i$ are built from normalized bipolar pseudo-random sequences. For computational complexity reasons, carriers are neither orthonormalized nor drawn from a Gaussian distribution. This is not a weakness since in high dimension, carriers are orthogonal and Gaussian property is not essential. Nevertheless, computational complexity is still high since computing the N_{sec} coefficients of the secure space requires to compute $N_{wlt} \times N_{sec}$ multiplications (resp. sums).

Knowing that $N_{wlt} = N \times (1 - 1/2^{2l})$ and $N_{sec} = N \times payload \times N_{arc}$, it gives[1] $N^2 \times payload \times N_{arc} \times (1 - 1/2^{2l})$ multiplications (resp. sums). The

[1] l is the number of wavelet decompositions, *payload* is the number of embedded bits by pixel, and N_{arc} is the number of output coefficients labeling an arc of the trellis.

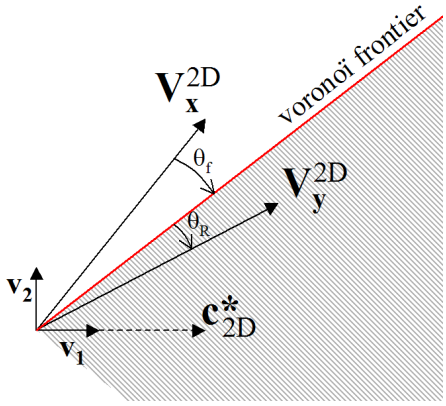

Fig. 2. Rotation-based embedding in the Miller, Cox and Bloom plane.

computational complexity is thus quadratic in function of the image size N. As an illustration, with a 256×256 image, $l = 3$ levels, $payload = 1/64$ bbp, and $N_{arc} = 12$ coefficients, there are 792 723 456 multiplications (resp. sums). Let us remark that it is impossible to reduce the number of multiplications and additions (thus it is impossible to reduce the complexity), and thus it is not useful to use a particular matrix multiplication routine.

2.2 Informed-coding and informed-embedding

After the projection of the host vector $\mathbf{x}$ onto carriers' $\mathbf{u}_i, i \in [0, N_{sec} - 1]$, we obtain the host vector $\mathbf{v_x}$. We then run the *informed-coding* which is the same as the original one [1]. The informed-coding takes as input the host vector $\mathbf{v_x}$ and the message m to be embedded and returns a codeword $\mathbf{c}^*$. This vector $\mathbf{c}^*$ (of size N_{sec}) is the closest one to $\mathbf{v_x}$ among vectors coming from the codebook $\mathcal{C}$, and representing the message m. For more details see [1] or [2].

The objective of the *informed-embedding* is to push the host vector $\mathbf{v_x}$ into the Voronoï region of $\mathbf{c}^*$ in order to obtain the watermarked vector $\mathbf{v_y}$. Many solutions exist which are either too CPU consuming [1], either too sub-optimal considering robustness-distortion tradeoff [5][2], [6]. In [1], a Monte-Carlo approach is used which requires many iterations of Viterbi decoder. On a Pentium 3 GHz, for a 256×256 image and a message size of 1024 bits, watermarking takes from half an hour to two hours depending on the robustness threshold. In [5] and [6], the Viterbi decoder is only used once or twice. On a Pentium 3 GHz, for a 256×256 image and a message size of 1024 bits, watermarking takes less than one minute. Nevertheless, those two last approaches degrade the image quality and are thus not fully satisfying.

[2] Paper [5] purpose is not informed-embedding but it uses a simple embedding solution.

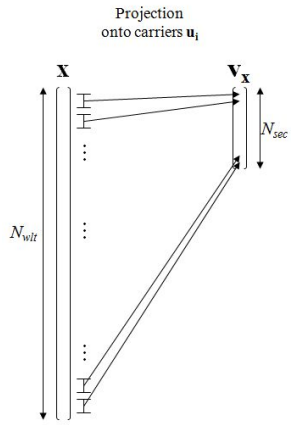

Fig. 3. General Space Division Multiplexing principle.

Our previous approach [2] is a good compromise between complexity and robustness. It is illustrated in Figure 2 in the plane defined by $\mathbf{v_x}$ and $\mathbf{c}^*$ (those two vectors are noted $\mathbf{v_x^{2D}}$ and $\mathbf{c^*_{2D}}$). This plane is usually named the Miller, Cox and Bloom plane (*abbr.* MCB plane).

Our approach consists in dichotomously reducing the angle between the host vector $\mathbf{v_x}$ and the codeword $\mathbf{c}^*$ until obtaining the smallest angle (noted θ_f) regarding all the other angles. Then, one penetrates inside the Voronoï region with a given angle θ_R. Our informed embedding is thus a rotation of $\mathbf{v_x}$ with an oriented angle equals to $\max(\theta_f + \theta_R, (\widehat{\mathbf{v_x}, \mathbf{c}^*}))$. This rotation gives the marked vector $\mathbf{v_y}$.

We then compute the watermark vector $\mathbf{v_w} = \mathbf{v_y} - \mathbf{v_x}$, retro-project it onto carriers in order to obtain the watermark signal $\mathbf{w}$ and then compute the watermarked signal $\mathbf{y} = \mathbf{x} + \mathbf{w}$. The inverse wavelet transform of $\mathbf{y}$ gives the watermarked image. At the extraction we project wavelet coefficients onto secret carriers and then retrieve the closest codeword (and thus the message) from the codebook $\mathcal{C}$.

3 Space Division Multiplexing (SDM) approaches

As explained in Section 2, the projections of the host signal $\mathbf{x}$ onto secret carriers are quadratic in (computational) complexity. In order to reduce this complexity to a more reasonable linear function, we decide to divide the wavelet space into disjoint *regions* and to use a carrier for each *region*. Figure 3 illustrates this concept. There is still N_{sec} carriers but their non-zero values are limited to a small *region*. Let $\overline{s} = N_{wlt}/N_{sec}$ be the mean *region* size. The number of multiplications (resp. sums) in order to compute the secret space is now approximately $N_{sec} \times \overline{s} = N_{wlt} = N \times (1 - 1/2^{2l})$. The computational complexity is thus linear

in function of the image size N. This division approach is called Space Division Multiplexing (SDM) [7].

We thus propose two approaches for SDM. In the first one, we build regions of equal size for each wavelet level (but not necessarily of equal size between the levels) and then re-arrange $\mathbf{v_x}$ coefficients in order to obtain a fair distribution. We call this approach the **structured SDM** (see Section 3.1). In the second approach, we build regions of quasi-equal sizes. We name this approach the **random SDM** (see Section 3.2).

3.1 Structured SDM

In order to obtain region sizes belonging to $\mathbb{N}^*$, we solve the equation below (in the case of a 3-level wavelet decomposition):

$$\left(3.\frac{N}{4}\right)\frac{1}{s_{789}} + \left(3.\frac{N}{16}\right)\frac{1}{s_{456}} + \left(3.\frac{N}{64}\right)\frac{1}{s_{123}} = N_{sec} \tag{1}$$

where $s_{789} \in \mathbb{N}^*$ is the size of regions in the wavelet sub-bands 7, 8 or 9 and so on (see Figure 1 for sub-bands numbering). Note that the regions sizes depend on the wavelet level.

Knowing that $N_{sec} = N \times payload \times N_{arc}$, Equation 1 is independent from the image size (3-level wavelet decomposition):

$$\begin{aligned} &16 \times s_{123} \times s_{456} + 4 \times s_{789} \times s_{123} + s_{789} \times s_{456} \\ &\quad -\frac{64}{3} \times payload \times N_{arc} \times s_{123} \times s_{456} \times s_{789} = 0. \end{aligned}$$

The retained solution among all the possible solutions is the one for which regions sizes are closest to[3] $\overline{s} = N_{wlt}/N_{sec}$. If no integer solution is found, we use overlapping on regions borders.

Before projecting the host signal $\mathbf{x}$ onto carriers, we pseudo-randomly shuffle its coefficients by group of wavelet level (see Figure 4). This ensures a good spreading of the influences coming from coefficients of the secret space. Moreover, it improves the security, the robustness (since it breaks spatial dependencies) and the psycho-visual impact.

After the projection of the host signal $\mathbf{x}$ onto carriers $\mathbf{u}_i$ (carriers are built with this Space Division Multiplexing approach), we obtain the host vector $\mathbf{v_x}$. In order to better balance the influence distribution of the $\mathbf{v_x}$ vector coefficients, we re-arrange it. Indeed, the first coefficients of $\mathbf{v_x}$ are related to the low frequency wavelet sub-bands 1, 2 and 3, the next coefficients are related to higher frequency sub-bands 4, 5, and 6 etc. Thus the vector $\mathbf{v_x}$ is re-arranged such that in each consecutive group of N_{arc} coefficients, the probability distribution of influence is the same (see in Figure 4, the distribution influence re-arrangement).

[3] With 3 level wavelet decomposition, $payload = 1/64$ and $N_{arc} = 12$, the retained solution is $s_{7,8,9} = 6$, $s_{4,5,6} = 4$, $s_{1,2,3} = 3$.

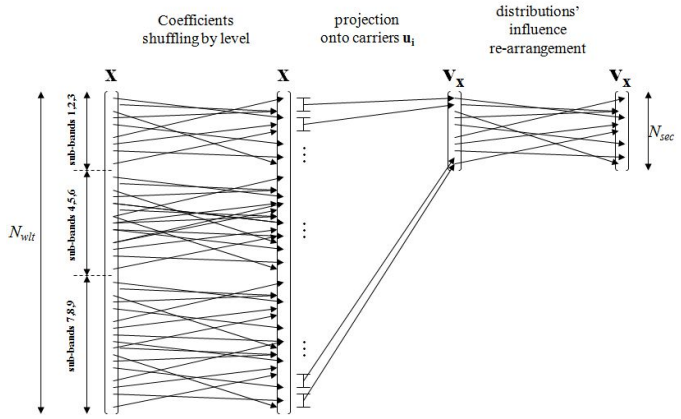

Fig. 4. Structured SDM: Space Division Multiplexing and re-arrangements for the projection onto carriers.

For example, with 3-level wavelet decomposition, in a block of N_{arc} coefficients of $\mathbf{v_x}$, the probability of coefficients coming from the different sub-bands are:

$$p_{1,2,3} = \frac{\frac{3N}{64s_{1,2,3}}}{N_{sec}}, p_{4,5,6} = \frac{\frac{3N}{16s_{4,5,6}}}{N_{sec}}, p_{7,8,9} = \frac{\frac{3N}{4s_{7,8,9}}}{N_{sec}} \tag{2}$$

In a block of N_{arc} coefficients of $\mathbf{v_x}$, the number of coefficients influencing the wavelet coefficients from sub-bands 1, 2, 3 (resp. 4, 5, 6 and 7, 8, 9), are thus respectively[4]:

$$\begin{aligned} n_{1,2,3} &= p_{1,2,3} \times N_{arc} = \frac{3}{64s_{1,2,3} \times payload}, \\ n_{4,5,6} &= p_{4,5,6} \times N_{arc} = \frac{3}{16s_{4,5,6} \times payload}, \\ n_{7,8,9} &= p_{4,8,9} \times N_{arc} = \frac{3}{4s_{7,8,9} \times payload} \end{aligned} \tag{3}$$

Note that each block of N_{arc} should respect this distribution but coefficients are again pseudo-randomly arranged in order to keep a good security level.

3.2 Random SDM

With the random SDM approach, we compute regions with no overlap, that fully cover the host vector $\mathbf{x}$ and whose sizes are integer and close to $\overline{s} = N_{wlt}/N_{sec}$. We talk of quasi-equal regions sizes (see Figure 5).

There are N_{sec} regions. A region r_i, with $i \in [0, N_{sec} - 1]$, is thus a set of contiguous wavelet coefficients, such that:

$$r_i = \{\mathbf{x}[i] | i \in [\lfloor i.\overline{s} \rfloor, \lfloor (i+1).\overline{s} \rfloor - 1]\}, \tag{4}$$

where $\mathbf{x}[i]$, with $i \in [0, N_{wlt} - 1]$, is a wavelet coefficient of the host vector $\mathbf{x}$.

[4] With 3 level wavelet decomposition, $payload = 1/64$ and $N_{arc} = 12$, the retained solution is $n_{7,8,9} = 8$, $n_{4,5,6} = 3$, $n_{1,2,3} = 1$.

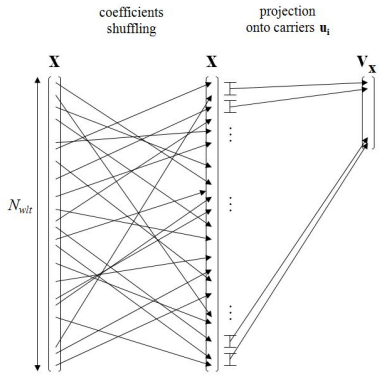

Fig. 5. Random SDM.

Note that before proceeding to the projection, the host signal $\mathbf{x}$ is pseudo-randomly shuffled in order to: break spatial dependencies, keep a good security level, and improve the robustness and the psycho-visual impact. The shuffled host signal $\mathbf{x}$ is then projected onto N_{sec} carriers using SDM with quasi-equal regions' sizes (see Equation 4 for regions definition). The host vector $\mathbf{v_x}$ is the result of this projection.

4 Results

Tests were carried on the first 100 images of the BOWS2 data-base[5] with images resized to 256×256[6]. Those images are 8-bits grey-level images and are personal photos.

The trellis structure has 128 states with 128 arcs per states. Outputs arcs labels are drawn from a Gaussian distribution and there are $N_{arc} = 12$ coefficients by output arc. The used payload is $payload = 1$ bit for 64 coefficients which is the same as the original DPTC algorithm [1]. The number of embedded bits is thus 1024 bits. 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 $payload = 1/64$ *bits per pixel* and that the number of outputs coefficients for an arc is $N_{arc} = 12$ coefficients, private space size is thus $N_{sec} = 1024 \times 12 = 12\ 288$ coefficients.

Four kinds of robustness attacks have been applied: Gaussian noise attack, 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

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

[6] The images sub-sampling has been achieved with xnview program and using Lanczos interpolation.

bits. The BER is computed for each attack. Three algorithms compete with a mean distortion close to 42.4 dB:

- the algorithm detailed in [2], having **carriers of high dimension** and whose projection complexity is quadratic. For this method the mean embedding PSNR is 42.42 dB and the inside angle penetration is $\theta_R = 0.1$ radian;
- the **structured SDM** algorithm (see Section 3.1). For this method the mean embedding PSNR is 42.23 dB and the inside angle penetration is $\theta_R = 0.05$ radian.
- and the **random SDM** algorithm (see Section 3.2). For this method, the mean embedding PSNR is 42.15 dB and the inside angle penetration is $\theta_R = 0.11$ radian.

In Figures 6, 7, 8, 9, we observe that the two SDM approaches perform equal or even better results than the high dimension carriers algorithm [2]. Results are similar for the Gaussian and the jpeg attacks, but for the filtering and the scaling attacks, the SDM approaches are better. This is a very interesting result since the high dimension carriers approach [2] is more complex (quadratic complexity) than the two SDM approaches. The high dimension carriers approach [2] may then be replaced with a faster (linear complexity) SDM approach.

If we compare the *structured SDM* approach with the *random SDM* approach, for the filtering and the scaling attacks, we observe that under 10% BER, the *random SDM* (i.e. the less complex approach) performs the best results. We conclude that in order to achieve the projection onto carriers, one should use *random SDM* since it is linear in complexity and it gives better robustness results than the *structured SDM* approach and the high dimension carriers' approach [2].

On a Pentium 3 GHz, for a 256×256 image and a message size of 1024 bits, watermarking takes less than one minute for the two SDM approaches and from half an hour to two hours for the original Miller *et al.* algorithm [1]. In [2], we show that our general scheme (using a secret space and a rotation-based embedding) has good robustness performances (except facing jpeg attack) compared to the original algorithm [1] or the Lin *et al.* approach [6]. We conclude that our scheme [2], enriched with the SDM technique, provides a good distortion - payload - robustness and complexity compromise.

Moreover, we believe that it is as least as difficult for an attacker to retrieve the codebook for our *random SDM* approach as for the Miller *et al.* one [1]. Indeed, the original approach only shuffles a subset of the DCT host coefficients whereas our approach shuffles and projects onto random carriers almost all the wavelet host coefficients.

5 Conclusion

In this paper, we introduce a new Dirty Paper Trellis Code (DPTC) algorithm having a security space built by projecting the wavelet coefficients onto secret carriers. In comparison to the original DPTC algorithm [1], our scheme is as least

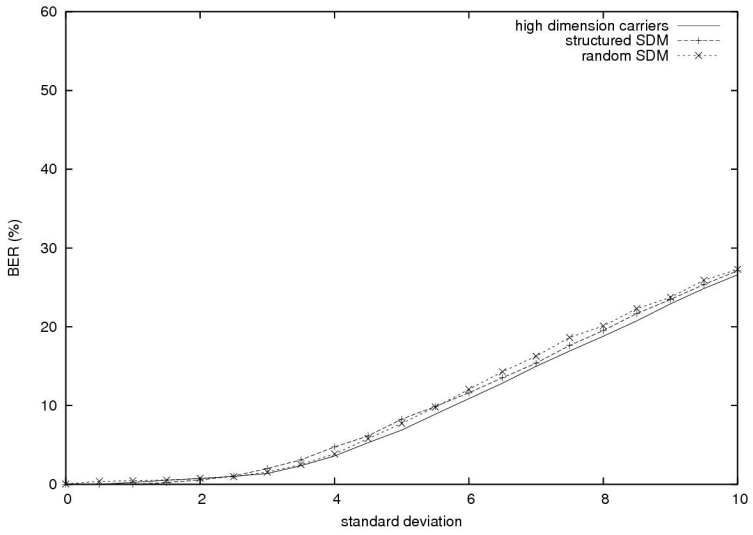

Fig. 6. Gaussian attack : BER for attack on the **high dimension carriers** algorithm [2], on the **structured SDM** algorithm and on the **random SDM** algorithm.

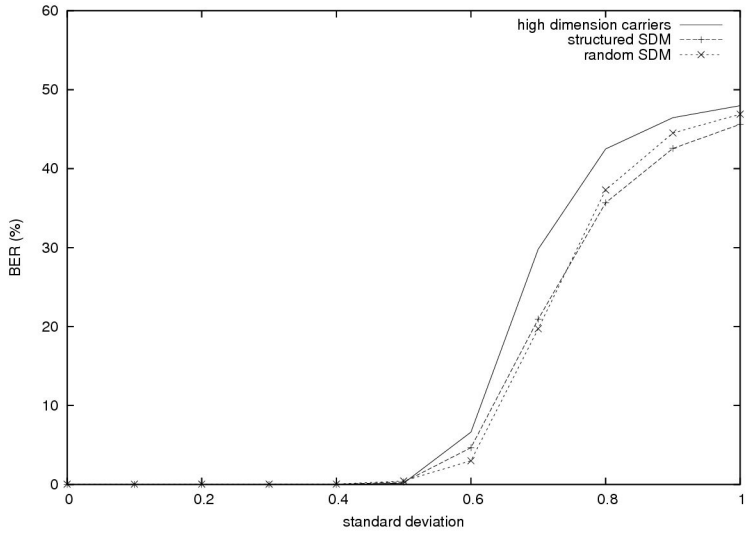

Fig. 7. Filtering attack : BER for attack on the **high dimension carriers** algorithm [2], on the **structured SDM** algorithm and on the **random SDM** algorithm.

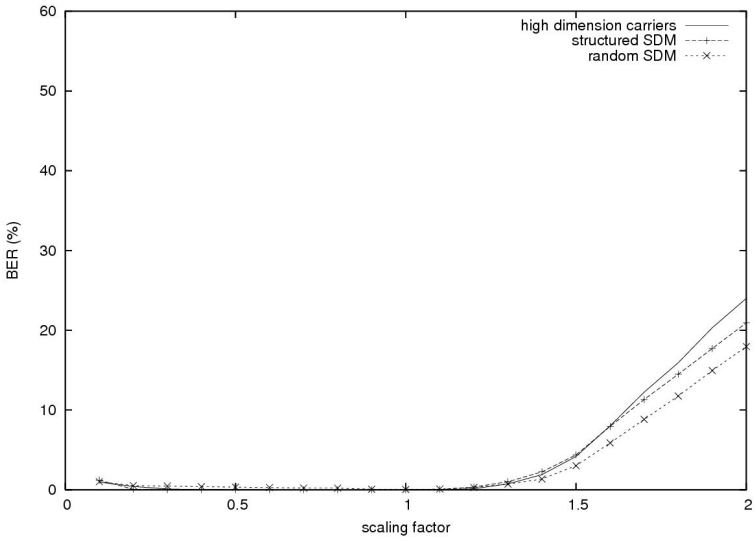

Fig. 8. Valumetric attack : BER for attack on the **high dimension carriers** algorithm [2], on the **structured SDM** algorithm and on the **random SDM** algorithm.

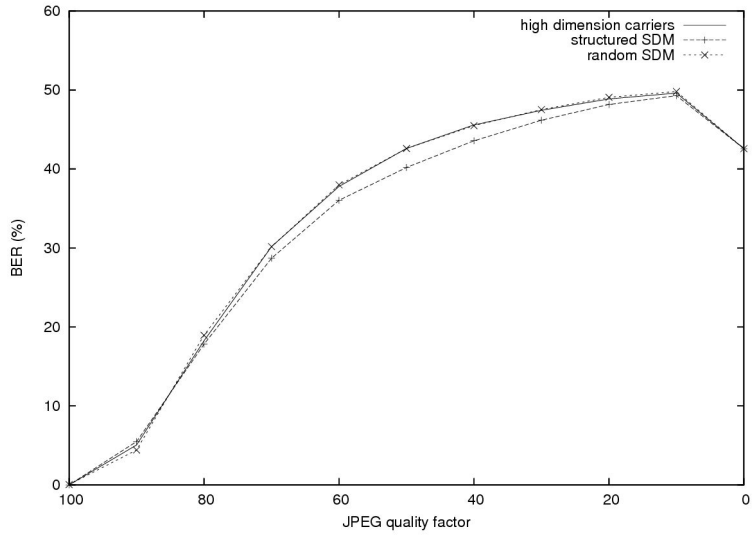

Fig. 9. Jpeg attack : BER for attack on the **high dimension carriers** algorithm [2], on the **structured SDM** algorithm and on the **random SDM** algorithm.

as secure and the visual degradation is better adapted to the human psychovisual system. After introducing the general problem of projections, we have proposed two Space Division Multiplexing (SDM) algorithms in order to decrease the projections complexity to a more reasonable linear computational complexity. We evaluated robustness with and without SDM approaches and observed that projection with SDM approaches give more robust results than projecting with high dimension carriers. We finally observe that the *random SDM* approach, which is the less complex approach, is the more robust.

Acknowledgements

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.

References

1. Miller, M.L., Doërr, G.J., Cox, I.J.: Applying Informed Coding and Informed Embedding to Design a Robust, High Capacity Watermark. IEEE Transactions on Image Processing **13**(6) (2004) 792–807
2. Chaumont, M.: A Novel Embedding Technic for Dirty Paper Trellis Watermarking. Submitted in: IEEE International Conference On Image Processing, ICIP'2009, Cairo, Egypt (November 2009)
3. Bas, P., 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, Oxford, United Kingdom (September 2008) 227–232
4. Kerckhoffs, A.: La Cryptographie Militaire. Journal des Sciences Militaires **IX** (pp. 5-38 Jan. 1883, pp. 161-191, Feb. 1883)
5. Wang, C., Doërr, G., Cox, I.J.: Toward a Better Understanding of Dirty Paper Trellis Codes. In: IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP'2006. Volume 2., Toulouse, France (May 2006) 233–236
6. Lin, L., Cox, I.J., Doërr, G., 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. Volume 1., Genova, Italy (September 2005) 697–700
7. Cox, I., Miller, M., Bloom, J., Fridrich, J., Kalker, T.: 5. in Multimedia Information and Systems. In: Digital Watermarking and Steganography. 2nd edition edn. Morgan Kaufmann (November 2007) 110–117