PSYCHOVISUAL ROTATION-BASED DPTC WATERMARKING SCHEME

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
phone: + (33)4.67.41.85.14, fax: + (33)4.67.41.85.00,
email: marc.chaumont@lirmm.fr

ABSTRACT

The Dirty Paper Trellis Codes (DPTC) watermarking is a very efficient high capacity scheme. Nevertheless, it suffers of two drawbacks: its security weakness and its CPU computation complexity. In a previous work, we treat those drawbacks by proposing a more secure embedding space and a faster embedding technique. In the current paper, we study the robustness of the scheme with the use of a psychovisual mask and a correcting code. First, we explain how to integrate the psychovisual shaping inside of the DPTC watermarking scheme. Second, we treat of the correcting code integration. Two different masks are used, and robustness comparisons are drawn between the previous DPTC and the two protected psychovisual DPTC. One can observe that for a given SSIM degradation, the robustness results are better for the two protected psychovisual DPTC approaches.

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] and SCS [3]) and the Dirty Paper Trellis Codes (DPTC) [4].

The original DPTC algorithm is known for its good robustness and its high embedding capacity but owns two strong weaknesses: the *informed embedding* step uses a Monte Carlo approach which is very CPU time consuming and the scheme own security weakness facing collusion attack [5]. In this paper we present a psychovisually secure, robust and rapid approach.

In a previous work [6], we give a solution, named rotation-based DPTC (**RB-DPTC**), in order to embed rapidly and securely. In Section 2, we remind its principle. In this paper, we propose to improve RB-DPTC by using a psychovisual mask and a correcting code. We thus expose in Section 3 the psychovisual shaping and briefly present the used correcting code. Those improvements lead to two new watermarking schemes: the protected with rudimentary's mask RB-DPTC (**PR-RB-DPTC**) and the protected with Xie and Shen's mask RB-DPTC (**PXS-RB-DPTC**). Finally, in Section 4, we compare the three approaches with a fixed robustness criteria and with a fixed psychovisual metric.

2. THE ORIGINAL ROTATION-BASED DIRTY PAPER TRELLIS CODES (RD-DPTC)

In this section, we present the embedding space and the embedding approach.

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 noted $\mathbf{u}_i$ with $i \in [1, N_{sec}]$. Note that a projection is just a scalar product. The obtained vector $\mathbf{v_x}$ 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 nor orthonormalized neither drawn from a Gaussian distribution. This is not a weakness since in high dimension, carriers are orthogonal and Gaussian property is not essential. Moreover, in order to reduce projections complexity to a linear complexity (and even with better robustness) we are using a Space Division Multiplexing approach [7]. It consist in first, shuffling the wavelet coefficients of $\mathbf{x}$ and second, dividing $\mathbf{x}$ in quasi-equal region' size and attribute a carrier by region.

2.2 Informed-coding and informed-embedding

Once that the projection of the host vector $\mathbf{x}$ onto carriers $\mathbf{u_i}, i \in [1, N_{sec}]$ are proceeded we obtain the host vector $\mathbf{v_x}$. We then run the *informed-coding* which is the same as the original one [4]. The informed-coding takes as input the host vector $\mathbf{v_x}$ and the message m, to be embedded, and return 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 $\mathscr{C}$, and representing the m message. For more details see [4] or [6].

After proceeding to the informed-coding, the codeword $\mathbf{c}^*$ is extracted. 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 $\mathbf{v_y}$. Our approach consists in dichotomously reducing the angle between the host vector $\mathbf{v_x}$ and the codeword $\mathbf{c}^*$ until obtaining the smallest absolute angle regarding all the other angles; this angle is noted θ_f. Then, one 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 equal to $\max(\theta_f + \theta_R, (\widehat{\mathbf{v_x}, \mathbf{c}^*}))$. The marked vector $\mathbf{v_y}$ is then obtained.

One 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 $\mathscr{C}$.

3. PSYCHOVISUAL SPACE AND CORRECTING CODE

3.1 General scheme with psychovisual shaping

Psychovisual masks may be used in order to shape the watermark signal. Roughly speaking, the watermark signal power will be reduced in the flat regions and increased in the textured or contours regions. Figure 1 shows the general embedding scheme with the use of a psychovisual mask. Referring to that figure, there is three majors steps:

1. the construction of a psychovisual space $\mathbf{x_{psy}}$. In this space, coefficients are psychovisually equivalents. One thus, can fairly embed. This psychovisual space is such that: $\forall i \in [1, N_{wlt}], \mathbf{x_{psy}}[i] = \mathbf{x}[i]/\alpha[i]$, with α the psychovisual mask;

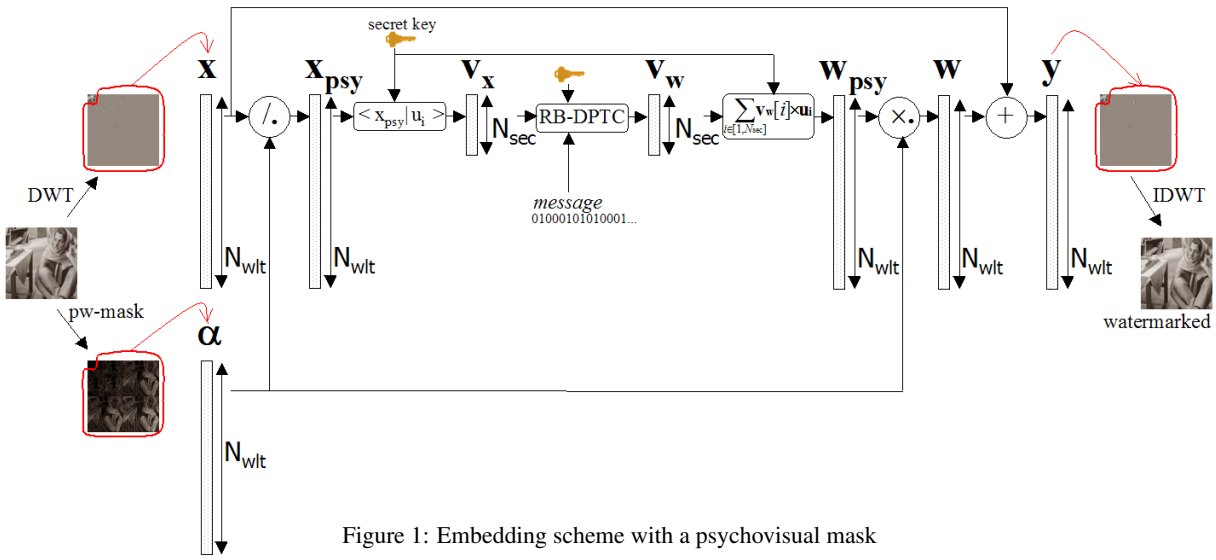


Figure 1: Embedding scheme with a psychovisual mask

2. the shaping of the watermark signal with the mask α: $\forall i \in [1, N_{wlt}], \mathbf{w}[i] = \mathbf{w_{psy}}[i] \times \alpha[i]$. This should reduce degradation, due to watermarking, in the visible regions. For example, flat regions should own a small α value in order to reduce the power of $\mathbf{w}$ in those regions.
3. the shaped watermark embedding. This embedding is such that: $\forall i \in [1, N_{wlt}], \mathbf{y}[i] = \mathbf{w}[i] + \mathbf{x}[i]$.

During the decoding, the decoder should re-compute the psychovisual mask. Note that this is a sensitive part since the re-computed mask should be the same than the one used during embedding. The decoder extract the wavelet (watermarked and attacked) signal, divide it component-wise by α, project coefficients onto secret carriers and then retrieve the closest codeword (and thus the message) from the codebook $\mathscr{C}$.

3.2 Rudimentary psychovisual's mask

Before using a psychovisual mask issued from the literature, we experiment the watermarking scheme behavior, if using a rudimentary mask. Results show that with a simple approach, the psychovisual impact is really good. The mask is obtained by, first, filtering the image with a sort of high-pass filter, second, apply a wavelet transform to the filtered image, and select the wavelet coefficients, and third, linearly scale their absolute value between two predefined scalar α_{min} and α_{max}[1].

The four steps are detailed above:

1. $\forall i \in [1, N], I^{filtered}[i] = 0.1 + 10 * |I[i] - I^{gauss}[i]|$ with I^{gauss} the result of a Gaussian filtering of image I.
2. Apply a wavelet transform to $I^{filtered}$ and order coefficients in a vector β.
3. Compute β_{min} and β_{max} such that $\beta_{min} = min_{i \in [1, N_{wlt}]} |\beta[i]|$ and $\beta_{max} = max_{i \in [1, N_{wlt}]} |\beta[i]|$ and then compute α by scaling absolute values of β between $[\alpha_{min}, \alpha_{max}]$ (knowing β_{min} and β_{max}).

The rudimentary mask for the Barbara 8-bit image (Figure 2.a), crop to a 512×512 image, is given in Figure 2.c. with pixels values multiply by 255. The Figure 2.b gives the 3 levels wavelet 9/7 Daubechies decomposition centered on the 127 value.

3.3 Xie and Shen's Pixel-Wise Mask

In [8], Xie and Shen propose an improvement of the well known pixel-wise masking model of Barni *et al.* [9]. The *pixel-wise mask* (PW-M) predicts the Human Visual Systems response to disturbance at a given coefficient position in the wavelet domain.

Let's note I_l^θ a sub-band at resolution level $l \in [1, L]$, with orientation $\theta \in \{a, h, v, d\}$. The PW-M value for a position (i, j) for a sub-band at level l is defined as the product of three terms:

$$\alpha_l^\theta(i,j) = \Theta(l,\theta).\Lambda(l,i,j).\Xi(l,i,j)^{0.2},$$

where the three terms are used to evaluate the sensitivity to noise changes depending on the band, the local brightness, and the local texture activities, respectively. The noise sensitivity function is computed as the following:

$$\Theta(l,\theta) = \left\{ \begin{array}{ll} \sqrt{2}, & if\ \theta = d \\ 1, & otherwise \end{array} \right\} . \left\{ \begin{array}{c} 1.00,\ if\ l = 1 \\ 0.32,\ if\ l = 2 \\ 0.16,\ if\ l = 3 \\ \ldots \end{array} \right\}.$$

The local brightness is computed by taking the *reconstructed* approximation $I_l^a(i,j)$ sub-band at the level, l, of interest[2], as the following:

$$\begin{array}{rcl} \Lambda(l,i,j) & = & 1 + L'(l,i,j), \\ with\ L'(l,i,j) & = & \left\{ \begin{array}{ll} 1 - L(l,i,j), & if\ L(l,i,j) < 0.5. \\ L(l,i,j), & otherwise. \end{array} \right. \\ with\ L(l,i,j) & = & \dfrac{I_l^a(i,j)}{255}. \end{array}$$

The texture activity in the neighborhood of a coefficient, is computed as the following:

$$\Xi(l,i,j) = \frac{[I_l^h(i,j)]^2 + [I_l^v(i,j)]^2 + [I_l^d(i,j)]^2}{3} . \mathbf{VAR}\{I_l^a(i,j)\}.$$

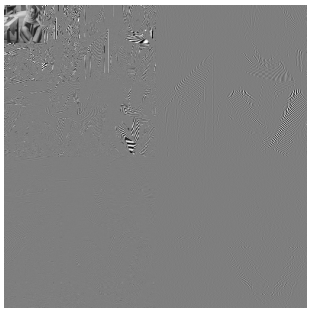
where the first contribution of the product is the local mean square value of the DWT coefficients at the same resolution level, l, and the second contribution, $\mathbf{VAR}\{I_l^a(i,j)\}$, is the local variance of the corresponding reconstructed approximation sub-band in a small neighborhood (3×3 window) corresponding to the location (i,j).

In order to compute α vector, we scale the values of each $\alpha_l^\theta(i,j)$ in the range $[\alpha_{min}, \alpha_{max}]$ as explain in section 3.2. Figures 2.d illustrate the Xie and Shen mask apply on Barbara image.

[1] $\alpha_{min} = 1$ and $\alpha_{max} = 8$ for PR-RB-DPTC and $\alpha_{min} = 1$ and $\alpha_{max} = 4$ PXS-RB-DPTC.

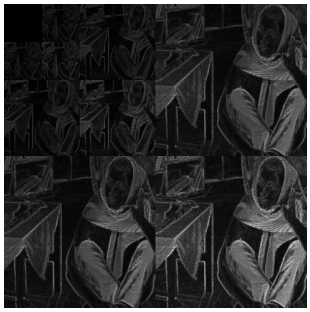
[2] In our implementation, the I_l^a images are build from a Gaussian pyramid.

(a) Barabara crop to 512x512



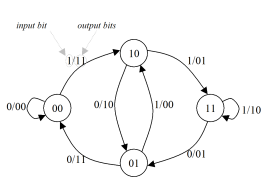
(b) wavelet decomposition

(c) rudimentary's mask

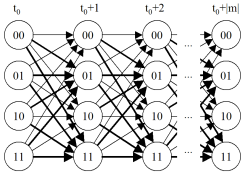


(d) Xie and Shen's mask

Figure 2: Illustration of psychovisual's masks



a) Binary convolution code's state-machine with 4 states



b) Binary convolution code's trellis with 4 states

Figure 3: Convolution code 2-memory, 1/2-rate.

3.4 Error Correcting Code

In order to add more robustness to the transmitted message m, one encode it with a very simple convolutional code 2-memory 1/2-rate. The state machine of this code is given in Figure 3.a. When an input bit enter into the coder, it causes a transition to a new state and outputs two bits. The two outputs bits are the resulting coded bits. The state machine can also be represented as it evolves in time with a trellis diagram. Figure 3.b shows the trellis associated to the state machine of Figure 3.a. Usually, a trellis is constructed by placing all the states in column and each possible transition are drawn with an arc between states at t time and states at $t+1$ time. By convention, bold arcs represent the 1 input and non-bold arcs the 0 input.

The convolutional coder takes a sequence of bits in input and generates an output sequence thanks to the state machine. The output sequence form a codeword representing the message m and is embedded into the image thanks to our rotation-based DPTC. The decoder, when receiving the possibly degraded codeword, finds the closest codeword and returns it. In order to find this closest codeword, the Viterbi algorithm is used [10].

4. RESULTS

Tests have been proceeded on the first 100 images of the BOWS2 data-base[3] with images resized to 256×256[4]. Those images are 8-bits grey-level images and are personal photos.

The trellis structure owns 128 states with 128 arcs by states. Outputs arcs labels are drawn from a Gaussian distribution and there are $N_{arc} = 12$ coefficients by output arc for the RB-DPTC approach and $N_{arc} = 10$ coefficients by output arc for PR-RB-DPTC and PXS-RB-DPTC. The used payload is $payload = 1$ bit of the (non-coded) message for 64 pixels which is the same as the original DPTC algorithm [4]. The number of embedded bits is thus 1024 bits for RB-DPTC and 2048 for the two improved RB-DPTC (since correcting code rate is $rateECC = 1/2$). Wavelet transform is a $9/7$ Daubechies with $l = 3$ decomposition 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. For the RB-DPTC, there are 1024 bits to embed and the number of outputs coefficients for a trellis' arc $N_{arc} = 12$ coefficients. The private space size is thus $N_{sec} = 1024 \times 12 = 12\,288$. For the two improved RB-DPTC there are 2048 bits to embed and the number of outputs coefficients for a trellis' arc is $N_{arc} = 10$ coefficients. The private space size is thus $N_{sec} = 2048 \times 10 = 20\,480$.

Lets remark that for the RB-DPTC, one bit of the message influences $N_{arc} \times N_{wlt}/N_{sec} = 63$ wavelet coefficients and with the two improved RB-DPTC, one bit of the message influences $N_{arc} \times N_{wlt}/N_{sec}/rateECC = 63$ wavelet coefficients. Thus, the two major differences are:

1. the spreading ratio N_{wlt}/N_{sec}. The spreading is higher for RB-DPTC (ratio = 1 coefficient of the secure space is spread on 5.25 coefficients of the wavelet space) than for the improved RB-DPTC (ratio = 1 coefficient of of the secure space is spread on 3.15 coefficients of the wavelet space);
2. the number of outputs coefficients for a trellis' arc. The RD-DPTC ($N_{arc} = 12$) should be more robust than the two improved RD-DP ($N_{arc} = 10$). A contrario, the "adds" of a correcting codes for the two improved RD-DPTC improves the robustness to error and the "add" of a psychovisual mask should allows to increase watermarking strength.

Four kinds of robustness attacks have been proceeded: Gaussian noise attack, Gaussian filtering attack, valumetric attack and jpeg attack. The Bit Error Rate (BER) is the number of erroneous extracted bits divide by the total number of embedded bits. The BER is computed for each attack. Two protocols are used in order to evaluate the robustness. For the first protocol, the inside angle penetration (which stand for the robustness parameter) is fix in order to obtain a quasi-equivalent PSNR degradation and for the second protocol, we choose to fix the SSIM degradation to 98%[11][5].

Three algorithms are competing with the two different evaluation protocols:

- the **RB-DPTC** detailed in [6]. For the first protocol, the inside angle penetration is fixed to $\theta_R = 0.11$ radian and we are obtaining a mean embedding PSNR of 42.15 dB.
- the **PR-RB-DPTC** using the rudimentary mask (see Section 3.2) and the convolutional code 2-memory and 1/2 rate (see Section 3.4). For the first protocol, the inside angle penetration is fixed to $\theta_R = 0.09$ radian and we are obtaining a mean embedding PSNR of 41.75 dB.
- the **PXS-RB-DPTC** using the Xie and Shen's mask (see Section 3.3) and the convolutional code 2-memory and 1/2 rate (see

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

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

[5] 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. Lets remark that we are using the C++ implementation by Mehdi Rabah at http://mehdi.rabah.free.fr/SSIM/.

Section 3.4). For the first protocol, the inside angle penetration is fixed to $\theta_R = 0.001$ radian and the mean embedding PSNR is 42.38 dB.

For the first evaluation protocol, we can observes on Figures 4.a, 4.b, 4.c and 4.d that below 1% BER, it is better to use the PR-RB-DPTC approach. Indeed, for very low attack power, comparing to the two other approaches, there are no bit errors. A contrario, at higher attack power, the BER is stronger for PR-RB-DPTC and PXS-RB-DPTC than for the original RB-DPTC. This could be explained by the fact that we are using correcting code in the two new approaches. When errors are too numerous, the performances of the correcting code collapse. We should nevertheless note that their is a very strong variance of PSNR over the 100 images: RB-DPTC PSNR $\in$[35.4, 61.7]; PR-RB-DPTC PSNR $\in$ [29.9, 56.9]; PXS-RB-DPTC PSNR $\in$ [33.2, 60.8]. Those high fluctuations are too strong and may lead to wrong interpretation. Since psychovisual mask have been used, in order to better compare the three watermarking schemes, we decide to fix the degradation criteria to a SSIM value of 98%.

For the second protocol, for each scheme, we dichotomically approach the SSIM 98% value by modifying the penetration angle[6]. Figure 5.a, 5.b, 5.c, 5.d, illustrate the BER for the different attacks with a SSIM = 98% embedding. Note that a SSIM of 98% gives images of very good quality. We can observe that for low power attacks, the two improved approach (PR-RB-DPTC and PXS-RB-DPTC) give better results than the original RB-DPTC (there is an improvement of the BER of a factor up to 10% for gaussian, filtering and scaling attacks). For those low power attacks, the approach using the rudimentary mask (PR-RB-DPTC) is a little bit better than the one using the Xie and Shen's mask (PXS-RB-DPTC). For higher power attack, except for the Gaussian attack, the results are comparable for the three approaches. The weak robustness to jpeg attack was already observed in previous work of [6] and [7] and is inherent to the approach since the host vector $\mathbf{x}$ is in part, made up of high frequency wavelet coefficients. We can remark that the same sensitivity to jpeg attack is observed with quantized-based approaches when all the DCT coefficients are used [12].

5. CONCLUSION

In this paper, we propose improvements to a previous work on DPTC. Our previous approach named rotation-based DPTC (noted RB-DPTC), treated two major problems of security and complexity for DPTC. In this paper, we essentially improve psychovisual degradation due to watermark embedding and add a correcting code in order to reduce the BER due to the use of a psychovisual mask. More precisely, we explain how to integrate a psychovisual mask inside of the original RB-DPTC, we briefly present the used correcting code and explain how to modify the trellis parameters. Results show that for a fix SSIM value, there is a strong improvement (of a factor 10) at low power attack. Future work should investigate: the link between SSIM metric and penetration angle, the construction of robust psychovisual masks, the use of RDM concept, the robustness to jpeg attack and sensitivity to regression attack.

Acknowledgment

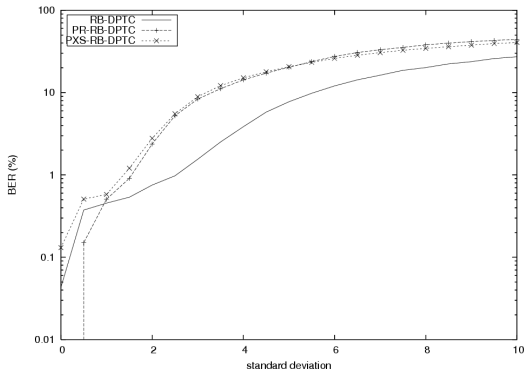
This work is in part supported by the VOODDO (2008-2011) project of the french ANR (Agence Nationale pour la Recherche).

REFERENCES

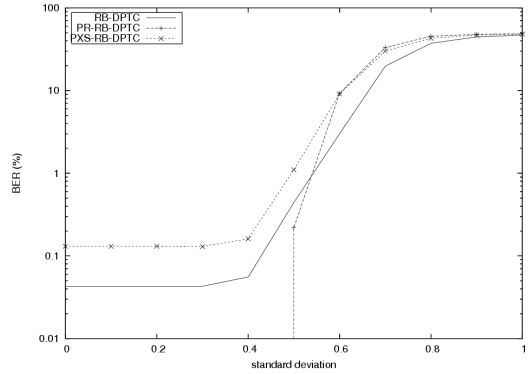
[1] M. Costa, "Writing on dirty paper," *IEEE Transactions on Information Theory*, vol. 29, no. 3, pp. 439–441, 1983.

[2] B. Chen and G. Wornell, "Quantization index modulation: A class of provably good methods for digital watermarking and information embedding," *IEEE Transactions on Information Theory*, vol. 47, no. 4, pp. 1423–1443, 2001.

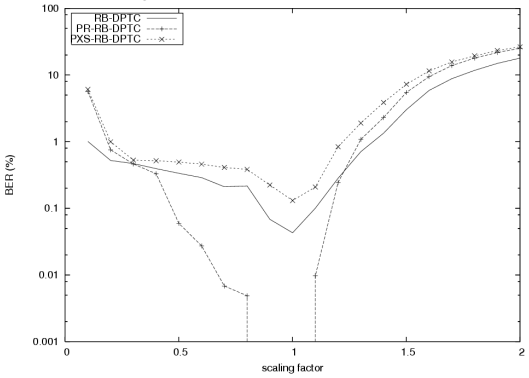
[6]For few images, SSIM may not be tune to the 98% value depending on the original angle between $\mathbf{v_x}$ and $\mathbf{c}^*$, and the angle of the Voronoï region.



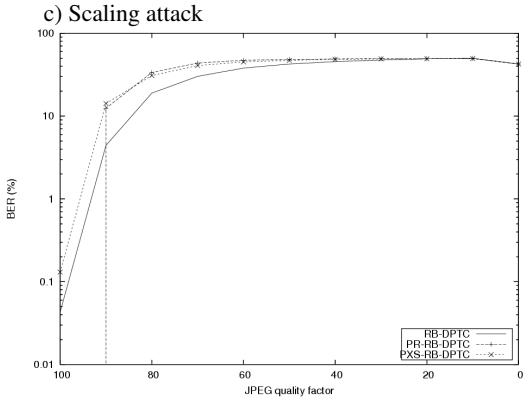
a) Gaussian attack



b) Filtering attack

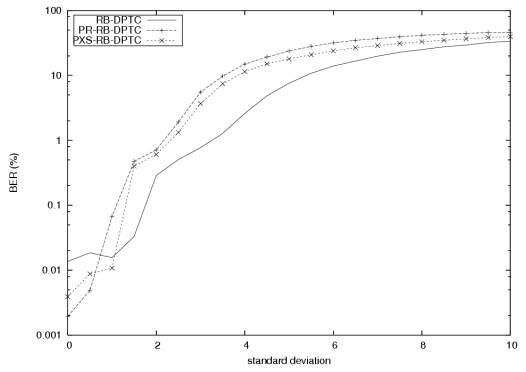


c) Scaling attack

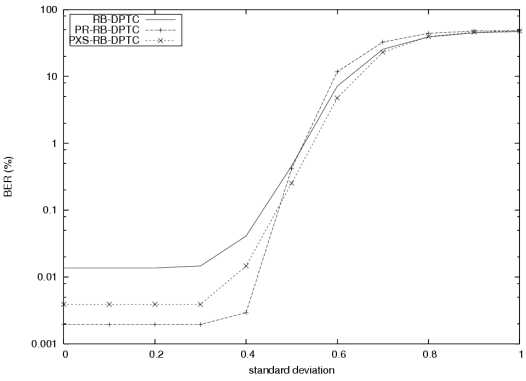


d) Jpeg attack

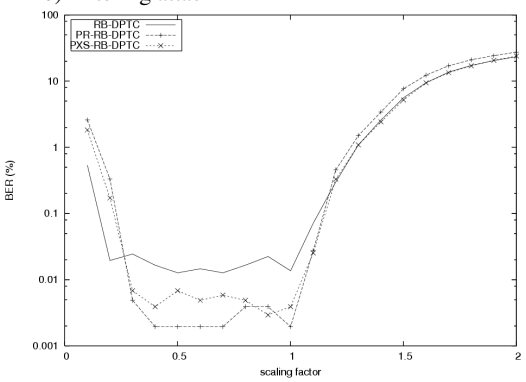
Figure 4: BER for attacks on RB-DPTC, PR-RB-DPTC and PXS-RB-DPTC. Embedding is proceeded with a fix penetration angle.



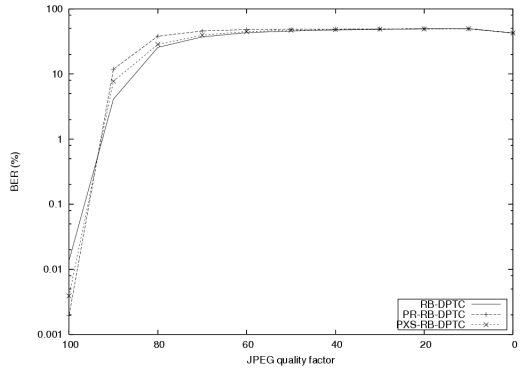
a) Gaussian attack



b) Filtering attack



c) Scaling attack



d) Jpeg attack

Figure 5: BER for attacks on RB-DPTC, PR-RB-DPTC and PXS-RB-DPTC. Embedding is proceeded with a with a fix SSIM of 98%.

[3] J. J. Eggers, R. Bäuml, R. Tzschoppe, and B. Girod, "Scalar Costa Scheme for Information Embedding," *IEEE Transactions on Signal Processing*, vol. 51, no. 4, pp. 1003–1019, 2003.

[4] M. L. Miller, G. J. Doërr, and I. J. Cox, "Applying Informed Coding and Informed Embedding to Design a Robust, High Capacity Watermark," *IEEE Transactions on Image Processing*, vol. 13, no. 6, pp. 792–807, 2004.

[5] P. Bas and G. Doërr, "Practical Security Analysis of Dirty Paper Trellis Watermarking," in *Information Hiding 2007, IH'2007*, Saint-Malo, France, June 2007, pp. 174–188.

[6] M. Chaumont, "A Novel Embedding Technic for Dirty Paper Trellis Watermarking," *Submited in IEEE International Conference On Image Processing, ICIP'2009*, Cairo, Egypt, Nov. 2009.

[7] M. Chaumont, "A Fast Embedding Technique For Dirty Paper Trellis Watermarking," in *8th International Workshop on Digital Watermarking, IWDW'2009*, University of Surrey, Guildford, UK, Aug. 2009.

[8] Gui Xie and Hong Shen, "Toward Improved Wavelet-Based Watermarking Using The Pixel-Wise Masking Model," in *IEEE International Conference on Image Processing, ICIP'2005*, 2005, vol. 1, pp. 689–692.

[9] M. Barni, F. Bartolini, and A. Piva, "Improved Wavelet-Based Watermarking Through Pixel-Wise Masking," *IEEE Transactions on Image Processing*, vol. 10, no. 5, pp. 783–791, May 2001.

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

[11] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image Quality Assessment: From Error Visibility to Structural Similarity," *IEEE Transactions on Image Processing*, vol. 13, no. 4, pp. 600–612, 2004.

[12] Qiao Li and I. J. Cox, "Using Perceptual Models to Improve Fidelity and Provide Resistance to Valumetric Scaling for Quantization Index Modulation Watermarking," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 2, pp. 127–139, June 2007.