SINGLE AND MULTIPLE SPREAD SPECTRUM WATERMARKING BASED ON PERIODIC CLOCK CHANGES

Vincent Martin, Marie Chabert, and Bernard Lacaze

ENSEEIHT/IRIT, National Polytechnic Institute of Toulouse
2 Rue Camichel, BP 7122, 31071 Toulouse Cedex 7, France
martin, marie.chabert, bernard.lacaze@enseeiht.fr

ABSTRACT

This paper analyses a spread spectrum watermarking embedding and decoding scheme based on periodic clock changes (PCC) for digital images. The PCC spreading properties and applications in multiuser communications are recalled. The theoretical and experimental decoding performance of this alternative spread spectrum technique are compared with a classical Direct Sequence (DS) method. PCC proves to be a simple alternative to pseudo-noise modulation spreading methods, that provides similar performance.

1. INTRODUCTION

Property and integrity protection of digital images, sounds and videos is currently of great commercial interest. Watermarking proposes to embed an imperceptible mark in the digital data. This mark allows data authentication or ownership evidence. Multiple marks can be used to identify the sellers and buyers and hence illegal copy sources in the fingerprinting application. Watermarks must be detectable and readable by their encoder, unnoticeable for the public and robust to malicious attacks or innocent signal processing operations. They are inserted in the perceptible components rather than in the file headers to be independent of the transmission formats.

Let consider the insertion of J marks M_j, $j = 1, ..., J$ ($J > 1$ in the case of multiple watermarking) in an image pixel luminance I. First M_j is transformed according to a secret key into the watermark W_j. Binary antipodal messages are considered for simplicity. Second, W_j is inserted in I providing the watermarked image pixel luminance I_W. These quantities are either handled as matrices or as vectors built by taking the rows in successive order as follows:

$$\begin{array}{c} M_j = [m_j(l)]_{l\in\{1,...,L\}}, W_j = [w_j(n)]_{n\in\{1,...,N\}} \\ I = [i(n)]_{n\in\{1,...,N\}} \text{ and } I_W = [i_W(n)]_{n\in\{1,...,N\}} \end{array} \quad (1)$$

L is called the payload. This study focuses on additive embedding of simultaneous watermarks in the spatial and DCT domains:

$$I_W = I + W \text{ or } I_W = \text{IDCT}(\text{DCT}(I) + W) \quad (2)$$

where $W = \alpha \sum_{j=1}^{J} W_j$. DCT and IDCT denote the 8x8 block two-dimensional Discrete Cosine Transform and Inverse Discrete Cosine Transform respectively. The masking factor α trades off watermark decoding performance and imperceptibility [1]. α can be replaced by a pixel dependent perceptual mask $[\alpha(n)]_{n\in\{1,...,N\}}$ taking into account the individual perceptual impact of each pixel or transformed domain coefficient. Note that the insertion can be as well multiplicative or performed in any transformed domain (full-frame DCT [2], time-scale ...).

The watermarked image I_W is transmitted and possibly attacked, leading to the image $I_W^{'}$. A classification of attacks can be found in [1]. A single noise source $B = [b(n)]_{n\in\{1,...,N\}}$ can model the distortions introduced as well by the transmission channel and by the so-called waveform attacks. Under the assumption of mild attacks, the noise model amounts to the widespread additive white Gaussian channel model:

$$I_W^{'} = I_W + B \text{ where: } B \sim \mathcal{N}(0, \sigma_B^2) \quad (3)$$

When more severe attacks occur, the noise model may be more sophisticated with possibly non-Gaussian distribution. Such attacks may lead to intractable derivation of the watermarking performance. In such case, the performance is studied through simulations only.

The watermark decoding step aims at recovering M from $I_W^{'}$ knowing the secret key. In the widespread blind public watermarking scheme, I is not required for decoding. The decoding performance is measured experimentally through the bit error rate (BER):

$$\text{BER} = \frac{\sum_{j=1}^{J}(1 - \sum_{l=1}^{L} \delta(d_j(l), m_j(l)))}{JL} \quad (4)$$

where δ denotes the Kronecker symbol and $D_j = [d_j(l)]_{l\in\{1,...,L\}}$ is the final hard decision on the message estimate.

For the public, W is a low-level noise. For the encoder, W is the signal of interest. Thus, the watermarking scheme amounts to the transmission of W through a highly noisy channel. This noise model includes both B and I contributions and the usual image distributions prevent from Gaussian noise assumption. For a given I and denoting σ_W^2 the variance of W, let define the document to watermark ratio (DWR) and the watermark to noise ratio (WNR):

$$\text{DWR} = \frac{\sum_{n=1}^{N} i(n)^2}{N\sigma_W^2}, \ \text{WNR} = \frac{\sigma_W^2}{\sigma_B^2} \ . \quad (5)$$

DWR measures W imperceptibility with respect to the host image. WNR measures transmission noise and attack influence.

This formulation as a transmission problem has inspired watermarking methods based on communication theory. In particular, a great interest has been devoted to spread spectrum techniques due to their security, their robustness to interference as well as their possible use for multiple access. Spread spectrum watermarking has been used for digital images [2], audio and video [1]. Direct Sequence (DS) spread spectrum is the most commonly used. M_j is modulated by a pseudo-random sequence providing a noise-like watermark W_j. The use of several orthogonal sequences allows for multiple watermarking. Many other spread spectrum methods have been studied in a communication framework: orthogonal Walsh functions can replace pseudo-random sequences, time or frequency division multiple access are rather based on multiplexing [3]. This study proposes the Periodic Clock Changes (PCC) as an alternative spread spectrum watermarking technique. DS and PCC multiuser communications have been compared in [4]. However, watermarking involves different noise models and performance criteria.

Section 2 recalls DS spread spectrum watermarking. Section 3 presents PCC general principle and proposes a PCC-based watermarking scheme. Section 4 compares the DS and PCC watermarking decoding performance with respect to noise, current signal processing operations and various attacks through simulations (the detection is not adressed).

2. DIRECT SEQUENCE SPREAD SPECTRUM WATERMARKING

DS spread spectrum multiple watermarking modulates the j^{th} message M_j by a particular zero-mean P-periodic pseudo-random sequence $C_j = [c_j(p)]_{p\in\{1,...,P\}}$ with:

$$c_j(p) = \pm 1, p \in \{1, ..., P\}, \\ < C_j, C_k > = 0 \text{ for } j \neq k, j, k \in \{1, ..., J\} \quad (6)$$

where $<,>$ denotes the inner product. These J orthogonal sequences act as secret keys. Each message bit $m_j(l)$ is associated to a symbol $\underline{w}_j^l$ of P samples such as:

$$\underline{w}_j^l = [w_j(k)]_{k \in \{(l-1)P+1, ..., lP\}} = m_j(l) C_j \quad (7)$$

The watermark $W_j = [\underline{w}_j^l]_{l \in \{1,...,L\}}$ exhibits a spread spectrum. In the following, given a vector X of length $N = LP$, $\underline{x}^l$ denotes $[x(k)]_{k \in \{(l-1)P+1, ..., lP\}}$. The family of Gold codes provides long orthogonal pseudo-random sequences [3]. The decoding derives $D_j = [sign(\hat{m}_j(l))]_{l \in \{(1,...,L\}}$. In the case of spatial embedding and assuming perfect synchronization between $\underline{i'_W}^l$ and C_j as well as perfect sequence orthogonality:

$$\hat{m}_j(l) = m_j(l) + \frac{1}{\alpha P} < \underline{i}^l + \underline{b}^l, C_j > \quad (8)$$

The scalar product derivation in (8) amounts to a noisy host image spreading. For a given image I and for large P, the sample are supposed independent and identically distributed [5], C_j being the only random variable. The Central-Limit theorem (CLT) states that

$$< \underline{i}^l + \underline{b}^l, C_j > \sim \mathcal{N}(0, \sigma^2) \text{ with } \sigma^2 = \sum_{k=1}^{P} (\underline{i}^l(k) + \underline{b}^l(k))^2 \quad (9)$$

As the luminance is bounded, $\lim_{P \to \infty} \frac{\sigma}{P} = 0$ and the additive Gaussian noise influence on detection performance is reduced for large αP. However, as α increases the watermark imperceptibility decreases and P is limited by the relation $N = PL$. The same properties hold when I is replaced by its block DCT coefficients and α by a perceptual mask.

3. PERIODIC CLOCK CHANGES

3.1 Definition and properties

A linear periodic time varying (LPTV) filter is a filter whose impulse response is a T-periodic function $h(n, k)$ of the time indexed by $n \in \mathbb{N}$. Its transfer function $H_n(\omega)$ is defined by:

$$H_n(\omega) = \sum_{k=-\infty}^{+\infty} h(n, k) e^{-ik\omega}, \qquad H_n(\omega) = H_{n+T}(\omega) \quad (10)$$

LPTV have been successfully used for interleaving, blind equalization and spread spectrum communications [6].

Let $f : \mathbb{N} \to \mathbb{N}$ be a T-periodic function of n. In a stochastic framework, a Periodic Clock Change (PCC) transforms a stationary process $Z = \{Z(n), n \in \mathbf{Z}\}$ in the process

$$U(n) = Z(n - f(n)), \qquad f(n) = f(n + T) \quad (11)$$

PCC are particular LPTV filters ($H_n(\omega) = e^{-i\omega f(n)}$). For such a digital sequence Z, PCC amounts to a sample permutation. The output U is zero mean and cyclostationary. Let $V(n) = U(n + \phi)$ a stationarized version of U (where ϕ is a uniformly distributed random variable on $\{0, 1, ..., T-1\}$).

Now consider $f(n)$ as a T-periodic random permutation and let $f^{-1}(n)$ denote the PCC of the inverse permutation:

$$f(n) = \underline{n} - q_{\underline{n}}, \qquad f^{-1}(n) = \underline{n} - q_{\underline{n}}^{-1} \quad (12)$$

where q is a permutation of $(0, 1, 2, ..., T-1)$ and $\overline{n}$ and $\underline{n}$ are respectively the quotient and the remainder of the division of n by T ($n = \overline{n}T + \underline{n}$). Then for T large enough, V spectrum approaches a white noise spectrum [7].

PCC multiuser communications transmit a particular random permutation f_j of each message. The successive application of any two PCC $f_i \circ f_j$ is a PCC and spreads the spectrum. Only the inverse PCC f_j^{-1} allows to retrieve the input spectrum. This property is to be linked with DS spread spectrum orthogonality [4]. PCC and DS multiuser communication performance has been compared with respect to the number of users J. The BER estimations show that PCC and DS perform similarly for a large J, while PCC performs better for a small one [4]. However, the simulation parameter values (particularly the SNR range) reflected a multiuser communication environment but were unrealistic for the watermarking application.

3.2 Application to Watermarking

LPTV designed for a watermarking framework must be whitening, invertible, cryptographically secure and optionally form an orthogonal set for multiple embedding. Periodic random permutations meet all these hypotheses for a low computational cost.

Random permutations have been used in watermarking schemes at different levels: for block DCT domain embedding [8], for interleaving a spectrally colored information in an asymmetric watermarking scheme [9] or as a message interleaver for security improvement [5].

One-Dimensional Periodic Clock Changes (1D-PCC): 1D-PCC performs on vectorial format (1). To reach a reasonable BER in the watermarking SNR conditions, redundancy is first introduced. The resulting message M'_j is the concatenation of P replicas of M_j (recall that P is such that $N = LP$):

$$m'_j(l + (p-1)L) = m_j(l), l \in \{1, ..., L\}, p \in \{1, ..., P\} \quad (13)$$

The payload L is thus supposed large enough to guarantee a diversity in M'_j between the $+1$ and -1 bits. W_j is obtained by applying a T_{1D}-periodic PCC f_j (the secret key) to M'_j. The first decoding step applies the inverse PCC f_j^{-1} to I'_W. The second step averages the P samples corresponding to each bit of the initial message

$$\begin{aligned} \hat{m}_j(l) &= \frac{1}{\alpha P} \sum_{p=1}^{P} (f_j^{-1}(i'_W))(l + (p-1)L) \\ &= m_j(l) + \frac{1}{\alpha P} \sum_{p=1}^{P} (f_j^{-1}(i + b))(l + (p-1)L) \end{aligned} \quad (14)$$

Let $\mu(I_W)$ denote the mean of I_W and $\sigma_{I_W}^2$ its variance. Since f_j^{-1} spreads I spectrum for large P values (Fig.1 displays the effect of random permutation on Lena image spectrum), the permuted samples are independent and identically distributed. The CLT allows Gaussian assumption on $\hat{M}_j$ with mean $E[\hat{M}_j] = M_j + \mu(I_W)$ and variance $(\sigma_{I_W}^2 + \sigma_B^2)/\alpha^2 P$. Then $\hat{m}_j(l)$ is sufficient statistic and the decision rule is $D_j = [\text{sign}(\hat{m}_j(l) - \mu(I_W))]_{l \in \{(1,...,L\}}$. Such a detector is known as the *matched filter detector* [10] with rectangular waveform.

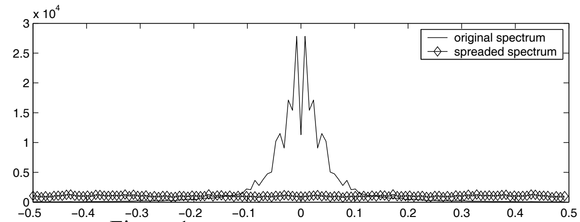

Figure 1: PCC spreading properties (Lena)

Two-Dimensional Periodic Clock Changes (2D-PCC): 2D-PCC performs on matrix format. The spread spectrum watermark results from successive column-wise f_j^1 and row-wise f_j^2 permutations of the redundant message. The insertion and decoding follow the same principle as 1D-PCC. 2D-PCC is expected to perform similarly with smaller periods: the association of two PCC at the decoding should efficiently remove the spatial correlation between pixels or transform domain coefficients.

3.3 Detector structure

The matched filter detector minimizes the probability of error under the assumption of Gaussian noise and orthogonality between users.

Under this assumption, the Minimum Mean Square Error (MMSE) detector corresponds to the matched filter.

Note that if the correlation between permuted messages is considered, the theoretical expression of the BER can be derived using Bayes' formula [11]. However, its computational cost grows exponentially with J and L. For low signal-to-noise ratios, a good approximation is obtained considering the Multiple Access Interference (MAI) $(\sum_{k \neq j} f_j^{-1} \circ f_k(M'_k))$ as Gaussian variables with variance σ^2_{MAI}. Using the CLT, BER $\simeq Q(\alpha\sqrt{P}/\sqrt{\sigma_I^2 + \sigma_B^2 + \sigma^2_{\text{MAI}}})$, where $Q(x) = \int_x^{+\infty} \frac{1}{\sqrt{2\pi}} e^{-u^2/2} du$. The literature for multi-user detection provides other structures of detectors [10]. The so-called *decorrelating detector* [11] allows to get rid of the MAI, at the price of a high computational cost. However, thanks to the large permutation period T in the watermarking application, σ^2_{MAI} is very small. Linear MMSE detection can also be achieved [10]. When the DWR is large enough, $\sigma^2_{\text{MAI}} << \sigma^2_{I_W}$. Consequently, the influence of MAI on detection performance has been neglected in this paper.

4. DIRECT SEQUENCE AND PERIODIC CLOCK CHANGES WATERMARKING PERFORMANCE COMPARISON

4.1 Implementation

Embedding domain: W can be embedded in the luminance I or in any invertible transform of I (DFT, DCT, Wavelet transform...). DS and PCC have been compared in the spatial (or luminance) domain (L-DS, L-PCC) and in the 8x8-block DCT domain (DCT-DS, DCT-PCC), that is the most popular transform domain since it is used in the JPEG compression format.

Perceptual masking: Embedding in the 8x8-block DCT domain (DCT-DS, DCT-PCC) benefits from research on perceptual analysis developed in image compression, since it is used in the JPEG format. The perceptual mask inspired from the work of A.J. Ahumada et al. [12] and used for instance by Hernandez [5] has been chosen in the DCT domain.

Parameters of the simulations: In this section, BER is estimated under various classical attacks as a function of DWR, WNR, R (message bit rate) or J (number of watermarks). For an accurate BER estimation, messages are randomly generated until at least 100 erroneous bits have been observed. For computational reasons, the computed BER is sometimes poor (BER= 10^{-2}). It could be improved by decreasing L (more redundancy) or increasing DWR (provided that the imperceptibility constraint is respected). The simulations provide the averaged performance on the test image set composed of Lena, Baboon, Fishingboat, Pentagon and Peppers [13]. Unless otherwise stated, the parameter values are: $L = 100$ bits (message length), $N = 2^{18}$ pixels (image length) and $J = 1$ (single watermark). For simulations involving attacks, DWR=36 dB offers the best decoding performance under the imperceptibility constraint. $T_{1D} = 2^{12}$ (1D-PCC period) and $T_{2D} = 2^6$ (2D-PCC period) trade off imperceptibility, decoding performance and computational cost on this image set.

4.2 Robustness with respect to noise

Recall that the watermark is submitted to different noise sources: the host image and additive or multiplicative noises modelling current signal processing or malicious attacks. Fig.2 displays the decoding performance as a function of DWR. Redundancy and averaged decoding provide DS, 1D-PCC and 2D-PCC similar robustness to the host image noise. Fig.3 shows that detection performance of the three algorithms are not altered by an acceptable additive noise. The same performance hold for multiplicative noise.

4.3 Message bit rate influence and multiple watermarking

DS, 1D-PCC and 2D-PCC decoding performance is first estimated as a function of the message redundancy P. The decoding performance is expected to increase with P.

Fig.4 shows that DS and PCC behave similarly when the message bit rate $R = 1/P$ increases, whith a light superiority of 2D-PCC in the spatial domain.

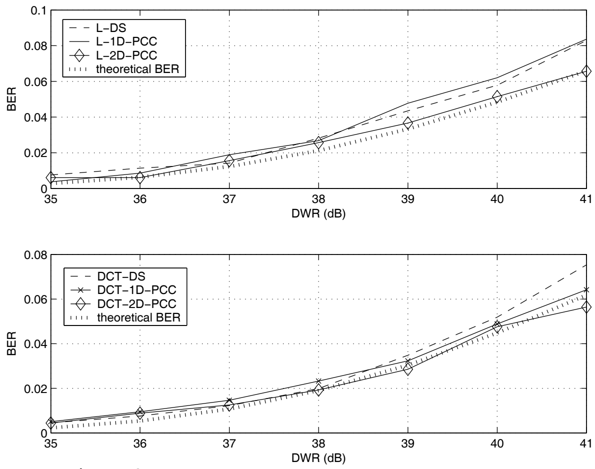

Figure 2: Decoding performance with respect to DWR

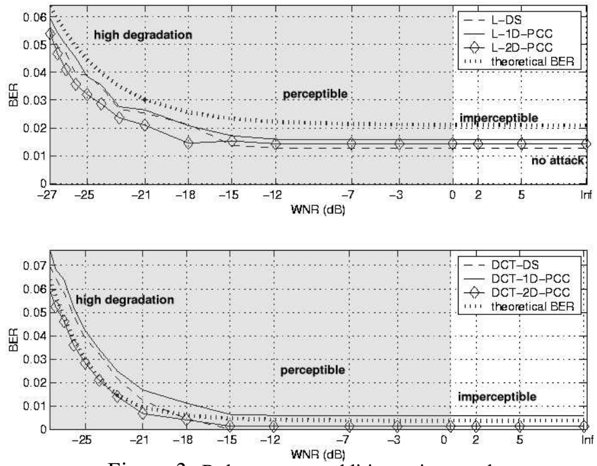

Figure 3: Robustness to additive noise attack

Multiple ($J > 1$) watermarking offers another way to transmit a given number of bits. Fig.5 displays the performance with respect to J in the case of multiple watermarking. Tests are performed with $J = 2$ to 14 messages. The multiple bit rate defined by $R_J = JL/N$ increases proportionally. The algorithms perform similarly when R_J increases.

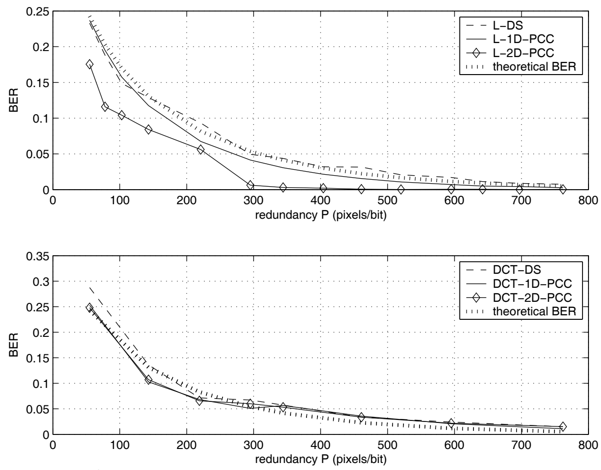

Figure 4: Decoding performance with respect to P

4.4 Robustness to sophisticated attacks

Waveform attacks: this comparison has been extended to sophisticated attacks such as scaling (the image is shrunk by a factor S and then re-scaled to its original size by the nearest-neighbors method) and Wiener filtering (the watermark is considered as a noise to be

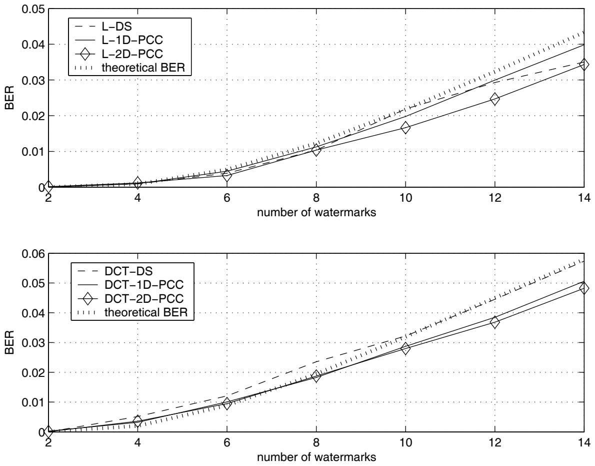

Figure 5: Decoding performance with respect to J

removed). Simulations show similar performance for DS and PCC, while both algorithms are more robust in the DCT domain.

Desynchronizing attacks: attacks such as cropping, translation or rotation [1] are not considered since they lead to catastrophic BER for the three considered algorithms in their basic form. Indeed the inner product derivation for DS or the inverse permutation for PCC yield totally erroneous results when derived on slightly shifted vectors or matrices. Several solutions (which are outside the scope of this study) use the insertion in appropriate transformed domains [14] or insertion of a synchronizing signal (template) [15]. Both methods can be applied to PCC as well as DS. However, an efficient synchronizing method robust to local, non-affine geometric tranforms and to template removal is still to be found.

JPEG Compression: I_W is JPEG compressed with a given compression rate, leading to similar performance of the three algorithms. Embedding in the DCT domain allows for a good robustness (Fig.6), since the JPEG compression algorithm involves a progressive quantification of the 8x8 block DCT with small impact on the middle frequencies coefficients.

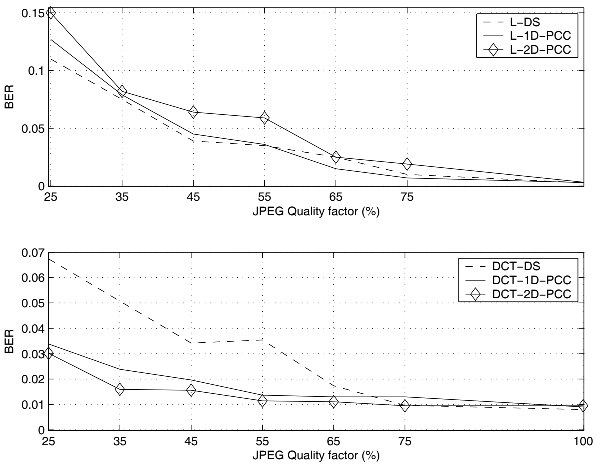

Figure 6: Robustness to JPEG compression

4.5 Averaged performance on a simulated image bank

Fig.7 provides the DCT-domain decoding performance as a function of DWR when this study is extended to a simulated image bank. The coefficients of the middle frequencies of each image I are generated following generalized Gaussian distributions with shape randomly chosen around $c = 0.8$. This 8x8 block DCT coefficient model is commonly used in the literature [5]. The results are consistent with those of Fig. 2.

5. CONCLUSION

This study has proposed to use random permutation based watermarking in the PCC theoretic general framework. A PCC blind spread spectrum watermarking scheme has been compared to the classical DS algorithm in the spatial domain and in the block DCT domain. PCC and DS performance are similar and consistent with those expected for spread spectrum techniques: a high robustness to additive and multiplicative noise but vulnerability to desynchronizing attacks. As expected, embedding in the DCT domain allows for a better robustness to sophisticated attacks. 2D-PCC would be preferred to 1D-PCC for its lower computational cost and better performance provided a good choice of the permutation length.

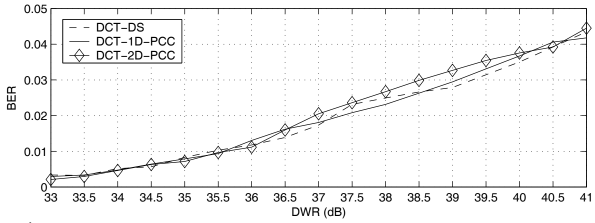

Figure 7: Decoding perf. with respect to DWR (simulated images)

This study concludes at a general equivalence between PCC spreading and classical spreading techniques using random pseudo-noise modulation, thanks to theoretical and experimental arguments. It justifies also the use of random permutations as an alternative spreading technique in existing algorithms. Random-permutation based PCC is very simple in its concept, implementation and computation and can be inserted in various watermarking schemes concerning different transform domains. The use of PCC spreading could also be advised to watermarking documents such as audio and video, where the redundancy would be greater and the periodicity would be better exploited. The spreading properties of more general LPTV's, that allow to perform simultaneously spectral shaping and whitening, are under study.

REFERENCES

[1] F. Hartung, *Digital Watermarking and Fingerprinting of Uncompressed and Compressed Video*. Aachen, Germ.: Shaker Verlag, 99.

[2] I. Cox, J. Kilian, F. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *Image Processing, IEEE Transactions on*, vol. 6, no. 12, pp. 1673–1687, 1997.

[3] J. Proakis, *Digital Communications*. NY: McGraw, 4th ed., 2001.

[4] D. Roviras, B. Lacaze, and N. Thomas, "Effects of Discrete LPTV on Stationary Signals," *IEEE ICASSP'02, Proc.*, vol. 2, pp. 1127–1220, 2002.

[5] J. Hernández and F. Pérez-González, "Statistical analysis of watermarking schemes for copyright protection of images," *IEEE Proc., Special Issue on Identification and Protection of Multimedia Information*, vol. 87, no. 7, pp. 1142–1166, 1999.

[6] D. McLernon, "One-dimensional Linear Periodically Time-Varying structures: derivations, interrelationships and properties," *IEE Proc.-Vis. Image Signal Proc.*, vol. 146, no. 5, pp. 245–252, 1999.

[7] B. Lacaze and D. Roviras, "Effect of random permutations applied to random sequences and related applications," *Signal Processing*, vol. 82, pp. 821–831, 2002.

[8] C.-T. Hsu and J.-L. Wu, "Hidden Digital Watermarks in Images," *IEEE Transactions on Image Processing*, vol. 8(1), pp. 58–68, 1999.

[9] T. Furon and P. Duhamel, "An asymmetric watermarking method," *IEEE. Trans. on Signal Proc.*, vol. 51, no. 4, pp. 981–995, 2003.

[10] S. Verdu, *Multiuser Detection*. Cambridge: Cambridge University Press, 1998.

[11] M. Coulon and D. Roviras, "Multi-user Detection for Random Permutation-Based Multiple Access," *IEEE ICASSP'03, Proc.*, vol. 4, pp. 61–64, 2003.

[12] A. Ahumada and H. Peterson, "Luminance-model-based DCT quantization for color image compression," *Proc. SPIE on Human Vision, Visual Proc., and Digital Display III*, vol. 1666, pp. 365–374, 1992.

[13] "http://www.petitcolas.net/fabien/watermarking/image_database/."

[14] J.J.K. Ó Ruanaith and T. Pun, "Rotation, scale and translation invariant spread spectrum digital image watermarking," *Signal Processing*, vol. 66, no. 3, pp. 303–317, 1998.

[15] S. Pereira and T. Pun, "Fast robust template matching for affi ne resistant image watermarking," *IEEE Transactions on signal processing*, vol. 51, no. 4, pp. 1045–1053, 2003.