PERFORMANCE ANALYSIS OF SCALAR DC-QIM FOR WATERMARK DETECTION

*Jean-Philippe Boyer**, *Pierre Duhamel*†, *Jacques Blanc-Talon**

{jean-philippe.boyer, pierre.duhamel}@lss.supelec.fr
Jacques.Blanc-Talon@etca.fr
*CTA/GIP, 16 bis av. de la Côte d'Or - 94114 Arcueil - France
† LSS/CNRS, 3 rue Joliot-Curie - 91190 Gif sur Yvette - France

ABSTRACT

Quantization-based schemes, such as scalar DC-QIM, have demonstrated performance merits for data-hiding problem, which is mainly a transmission problem. However, a number of applications are stated in terms of *watermark detection* problem (also named one-bit watermarking), and this situation has been seldom addressed in the literature for quantization-based techniques. In this context, we carry out a complete performance analysis of uniform quantizers-based schemes with distortion compensation (DC) under additive white gaussian noise. Implementing an exact Neyman-Pearson test and using large deviation theory, performances are evaluated according to Receiver Operating Characteristic (ROC) and probability of error. Optimal DC's regarding to ROC performances are derived. It is pointed out that false-alarm and miss detection capabilities are jointly optimized by the same DC value. Then, performances are compared with raw quantized-schemes (*i.e.* without DC) and spread-spectrum (SS) watermarking. It is shown that DC-QIM always outperforms QIM and SS for detection task. The gain provided by the DC reaches several orders of magnitude for cases of interest, that is for low watermark-to-noise regimes. A short comparison is also provided with respect to the corresponding transmission problem, thus evaluating the loss in performance due to the detection.

1. INTRODUCTION

Data-hiding has intensively focused on quantization-based schemes these last five years. Being inspired by binning coding strategy, these approaches have demonstrated their "provably" efficiency [1]. In particular, low-complexity implementations involving uniform quantizers (namely DC-QIM or the equivalent form SCS [2]) have been largely studied. The performance of these systems are usually evaluated according to achievable transmission rates. For quantized-based systems, each message is associated to a specific reconstruction set and the distance between these codebooks is to be maximized in some sense. However, several practical problems involving watermarking (including steganalysis, semi-fragile watermarking applied to content authentication or copyright protection) can be formulated more naturally as a detection problem rather than a transmission one [3, 4, 5]. Some of them cannot even be stated in terms of transmission, due to applicative constraints (since some signals will not contain any watermark). The problem is then to determine whether an arbitrary watermark, often named signature, is embedded (one-bit watermarking) into a noisy content. The natural criterion associated to this task is the Receiver Operating Characteristic (ROC) but the overall probability of error can also be illustrative as a representative point of ROC curve. It is clear that any detection problem can always be reduced to a binary transmission issue in respectively associating the presence and the absence of the watermark with two modulation symbols. Detection problems thus involve a different modulation codebook in which one of the two modulation symbols (*i.e.* the absence of the watermark) is *imposed* by the context. Hence, there is not obvious link between the performance attained by these two modulations (transmission/detection). Whereas detection aspect has been largely treated for spread spectrum (SS) embedding schemes [3], this aspect has been seldom addressed for quantized-based schemes [5, 6, 7, 8], probably due to the fact that these techniques have been initially introduced for data-hiding purposes. In particular, [7, 8] have demonstrated that quantization-based schemes show encouraging improvements over classical SS watermarking. Eggers *et al.* [6] first introduced DC-QIM schemes for detection purposes, showing that this scheme can also be efficient in a detection context. However, this study adopts the overall error probability as criterion instead of the more general ROC criterion. In most detection problems, ROC is of particular interest since this is the relevant measure to tune the watermark semi-fragility [3, 5]. On another hand, [6] provides performance evaluation in a situation where the detector input is a single sample and actual optimal form of DC has not been given. In this paper, we propose to fill these gaps, providing a complete study of DC-QIM scheme with uniform quantizers applied to detection with white gaussian noise. Performances are evaluated according to large deviation theory and are compared with raw quantized scheme (QIM), SS and the corresponding transmission problem.

2. ONE-BIT SCALAR DC-QIM WATERMARKING ISSUE

First recall the DC-QIM embedding process which has been used previously in data-hiding problems [1, 2]. Let $\boldsymbol{s} \in \mathbb{R}^N$ be samples of an host signal. A watermark is embedded as $\boldsymbol{x} = \boldsymbol{s} + \boldsymbol{w}$ with $\boldsymbol{w} = \alpha \bmod_\Delta(\boldsymbol{s} - \boldsymbol{k}\Delta)$ where α and Δ are respectively a scaling factor belonging to $[0, 1]$ and a uniform quantization step and $\bmod_\Delta(.)$ denotes the quantization error induced by the cubic lattice quantizer $\Delta\mathbb{Z}^N$. $\boldsymbol{k}\Delta$ is a secret external dither sequence uniformly distributed over the Voronoï cell $\mathcal{V}_0 = [-\frac{\Delta}{2}, \frac{\Delta}{2})^N$, independent of $\boldsymbol{s}$, shared by the embedder and detector. Since $\boldsymbol{s}$ and $\boldsymbol{k}$ are assumed to be independent, use of dithering [9] ensures that quantization error signal $\boldsymbol{q} = \bmod_\Delta(\boldsymbol{s} - \boldsymbol{k}\Delta)$ remains statistically independent of the host signal and is forced to be i.i.d.

uniform over $\mathcal{V}_0$, regardless to the host distribution and even if the high-resolution quantizer assumption is violated. Hence, the embedded distortion reads $D_w \triangleq N^{-1}\mathbb{E}\|\boldsymbol{w}\|^2 = \alpha^2\Delta^2/12$. $\boldsymbol{x}$ undergoes an additive i.i.d. centered noise $\boldsymbol{v}$ with variance σ_v^2, producing signal $\boldsymbol{r}$. The watermark-to-noise power ratio is defined as $wnr = D_w/\sigma_v^2$. The one-bit watermarking issue is defined introducing the two following hypotheses:

$$H_0: \quad \boldsymbol{r} \text{ is actually not watermarked}, \quad \textit{i.e. } \boldsymbol{r}_{|H_0} = \boldsymbol{s} + \boldsymbol{v},$$
$$H_1: \quad \boldsymbol{r} \text{ contains the watermark}, \quad \textit{i.e. } \boldsymbol{r}_{|H_1} = \boldsymbol{x} + \boldsymbol{v},$$

and the detector has to decide between both hypotheses. Given a signal $\boldsymbol{r}$ to be tested and knowing key $\boldsymbol{k}$, the detector reduces $\boldsymbol{r}$ to the statistic $\boldsymbol{y} = \text{mod}_\Delta(\boldsymbol{r} - \boldsymbol{k}\Delta)$. Then, the optimal detection rule based on the Neyman-Pearson criterion is implemented. This is based on the log-likelihood ratio

$$\Lambda(\boldsymbol{y}) = \log \frac{Pr(\boldsymbol{y}|H_1, \boldsymbol{k})}{Pr(\boldsymbol{y}|H_0, \boldsymbol{k})} \quad (1)$$
$$= \sum_{n=1}^{N} \log \frac{Pr(y_n|H_1, k_n)}{Pr(y_n|H_0, k_n)} \triangleq \sum_{n=1}^{N} \log \frac{p_1(y_n)}{p_0(y_n)}. \quad (2)$$

(2) holds since the use of dithering ensures that $\boldsymbol{y}$ is i.i.d. For a given detection threshold τ, the associated decision rule is

$$\Lambda(\boldsymbol{y}) \begin{cases} \geq N\tau \Rightarrow H_1 \\ < N\tau \Rightarrow H_0. \end{cases} \quad (3)$$

The false-alarm and miss probabilities are respectively defined as $P_F^{(N)}(\tau) = Pr\left(\Lambda(\boldsymbol{y}) \geq N\tau | H_0, \boldsymbol{k}\right)$ and $P_M^{(N)}(\tau) = Pr\left(\Lambda(\boldsymbol{y}) < N\tau | H_1, \boldsymbol{k}\right)$. If H_0 and H_1 have equal priors and equal costs, another criterion of interest is the overall probability of error which follows from the Maximum Likelihood test, *i.e.* $P_E^{(N)} = \frac{1}{2}\left(P_M^{(N)}(0) + P_F^{(N)}(0)\right)$.

• Under H_0, the dithering forces each component of the quantization error $\boldsymbol{y} = \text{mod}_\Delta(\boldsymbol{s} + \boldsymbol{v} - \boldsymbol{k}\Delta)$ to be uniformly distributed over the Voronoï cell [9]. Hence, $p_0(y_n) = 1/\Delta$ for $y_n \in [-\frac{\Delta}{2}, \frac{\Delta}{2}]$ and is null otherwise. Expression (2) then reads $\Lambda(\boldsymbol{y}) = N\log\Delta + \sum_{n=1}^{N}\log p_1(y_n)$.

• Under H_1, one can easily derive the Modulo Lattice Additive Noise relation $\boldsymbol{y} = \text{mod}_\Delta\left((1-\alpha)\boldsymbol{q} + \boldsymbol{v}\right)$. $\boldsymbol{q}$ and $\boldsymbol{v}$ being independent, probability density function (pdf) $p_1(y_n)$ of each component y_n can be computed by a cyclic convolution. Choosing $\boldsymbol{v}$ as an i.i.d. centered gaussian noise, a simple analysis reveals that for any $\alpha \in [0, 1)$

$$p_1(y_n) = \frac{1}{\Delta(1-\alpha)} \sum_{i\in\mathbb{Z}} Q\left(\frac{y_n}{\sigma_v} + a_i\right) - Q\left(\frac{y_n}{\sigma_v} + b_i\right) \quad (4)$$

for $y_n \in [-\frac{\Delta}{2}, \frac{\Delta}{2}]$ and is null otherwise. Here $Q(x) = \frac{1}{\sqrt{2\pi}}\int_x^\infty e^{-u^2/2}du$, $a_i = \frac{\Delta}{\sigma_v}(i - \frac{1-\alpha}{2})$ and $b_i = \frac{\Delta}{\sigma_v}(i + \frac{1-\alpha}{2})$.

3. OPTIMAL DISTORTION COMPENSATIONS

DC has been introduced in Costa's binning coding strategy for maximizing the Shannon capacity over gaussian channel with non-causal side-information. For quantization based schemes, it increases the minimal distance between each quantizer cosets associated to each transmitted message without increasing the induced distortion [1]. For detection problems, DC can also provide substantial gain. We propose to determine DC's which maximize ROC performances of DC-QIM in presence of gaussian noise. Note that DC has no obvious reason to be the same as it has been proposed in data hiding scenario, that is $\alpha_{ICS} = \frac{wnr}{wnr+1}$ in [1] or $\alpha_{SCS} = (\frac{wnr}{wnr+2.71})^{1/2}$ in [2]. It has been pointed out in [6] that α_{SCS} remains a "good" value for keeping $P_E^{(N)}$ low when using one sample at the detector input. For nearly spherical Voronoï cell lattice quantizers, [7] has shown that α_{ICS} maximizes a lower bound on the miss error exponent (which is defined as $E_M = \lim_{N\to\infty} -\frac{1}{N}\log P_M^{(N)}$) for a given level of $P_F^{(N)}$. We also introduce the false-alarm error exponent as $E_F = \lim_{N\to\infty} -\frac{1}{N}\log P_F^{(N)}$. For a given distortion, we propose to derive α_F and α_M which respectively minimizes $P_F^{(N)}$ for a fixed upper bound on P_M^N (uniformly over all N) and minimizes $P_M^{(N)}$ for a fixed upper bound on P_F^N (uniformly over all N). These two tradeoffs respectively arise in an integrity checking context [5] and for copyright verification application [3]. Unfortunately, error probabilities do not admit any close-form expressions. Instead and in order to compute these DC's values independently of a chosen value of N, we resort to the Stein's Lemma [11] which states that, for any Neyman-Pearson test, we have

$$E_F = D(p_1||p_0) \text{ for a fixed upper-bound on } P_M^{(N)} \quad (5a)$$
$$E_M = D(p_0||p_1) \text{ for a fixed upper-bound on } P_F^{(N)} \quad (5b)$$

where $D(f||g) = \int f\log(f/g)$ is the Kullback distance which is naturally used as a dissimilarity measure between distributions f and g in hypothesis testing setup. (5a) means that, for a fixed $P_M^{(N)}$, $P_F^{(N)}$ decays exponentially in the number of observations (and reciprocally for (5b)). We then search α_F and α_M which respectively maximize these decay rates. Since $D(p_1||p_0) \neq D(p_0||p_1)$ in our case, note that $\alpha_F = \alpha_M$ is not trivial[1]. This exponential behavior also underlines that using a "good" (but not optimal) DC value such as α_{SCS} can have some significant sub-optimal effect as N grows, which remains not noticeable when taking N small. For each wnr, these one-dimensional optimizations have been performed numerically and plotted on Fig. 1. α_M and α_F turn out to be very close. Hence, false-alarm and miss detection capabilities are jointly optimized by the same DC value, which is practically convenient. The figure also shows the optimal values for a transmission scenario. Resulting DC's appear to be a bit less smooth, particularly at high wnr, but globally keep analogous shapes. Our optimized DC's are used in the sequel.

4. PERFORMANCE DERIVATION

We now address performance analysis when using N samples at the detector input. In order to measure the gain provided by distortion compensation, we also propose to compare to QIM (*i.e.* $\alpha = 1$) and SS cases.

4.1. DC-QIM Performances

The considered hypothesis testing problem does not provide exact calculation of performances. We resort to fair performance estimates to analyse the system. By considering the log-likelihood (2) as a sum of N i.i.d. variables, the Central Limit Theorem could

[1] More generally, ROC curves are generally not symmetrical around the diagonal for quantized-based schemes [7], contrary to SS schemes.

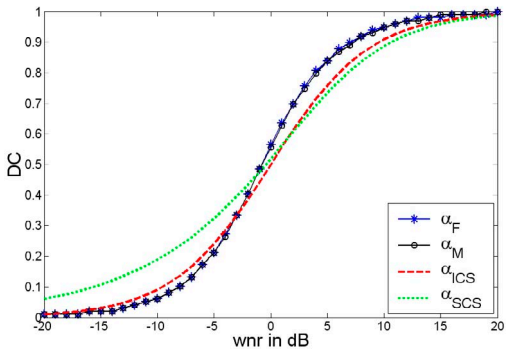

Fig. 1. Optimal distortion compensations $\alpha_M(wnr)$ and $\alpha_F(wnr)$. α_{ICS} and α_{SCS} are also depicted.

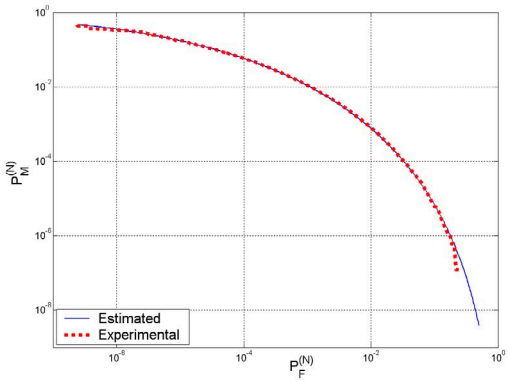

Fig. 2. Estimated and experimental ROC curves for DC-QIM with $N = 64$ and $wnr = 0$ dB. Our optimized DC has been used.

be applied to model $\Lambda(\boldsymbol{y})$ as a normal process under both hypotheses and then estimate $P_F^{(N)}$ and $P_M^{(N)}$. However, it is known [10] that this approach leads to poor accuracy for large deviations $\frac{N\tau - \mathbb{E}(\Lambda(\boldsymbol{y})|H_i,\boldsymbol{k})}{\sqrt{\text{Var}(\Lambda(\boldsymbol{y})|H_i,\boldsymbol{k})}}$, $i \in \{0,1\}$, that is for small error probabilities. Instead, we prefer to make use of some more reliable estimates based on the logarithm of the moment-generating function of $\Lambda(\boldsymbol{y})$ defined as $\mu(s) = \log \int_{\mathcal{Y}_0} e^{s\Lambda(\boldsymbol{y})} Pr(\boldsymbol{y}|H_0,\boldsymbol{k}) d\boldsymbol{y}$, $s \in [0,1]$. In our case, we have $\mu(s) = -N\lambda(s)$ with $\lambda(s) = (1-s)\log\Delta - \log \int_{-\frac{\Delta}{2}}^{\frac{\Delta}{2}} p_1(y)^s dy$. This quantity, which is closely related to the Chernoff Distance, can be shown to be concave in s. Whenever N becomes large, it can be shown that [11]

$$P_F^{(N)} \simeq \frac{1}{s\sqrt{-2\pi N\lambda''(s)}} e^{-N\left(s\tau+\lambda(s)\right)} \quad (6)$$

$$P_M^{(N)} \simeq \frac{1}{(1-s)\sqrt{-2\pi N\lambda''(s)}} e^{-N\left((s-1)\tau+\lambda(s)\right)} \quad (7)$$

where s is chosen so that $\lambda'(s) = -\tau$ is met. $\lambda'(s)$ and $\lambda''(s)$ are the first and the second derivatives of $\lambda(s)$ with respect to s. This leads to

$$P_E^{(N)} \simeq \frac{1}{2s_0(1-s_0)\sqrt{-2\pi N\lambda''(s_0)}} e^{-N\lambda(s_0)} \quad (8)$$

where s_0 verifies $\lambda'(s_0) = 0$. Fig. 2 assesses the validity of the proposed estimates.

4.2. QIM Performances

The case $\alpha = 1$ is singular for pdf (4). However, as α tends to one, quantity $b_i - a_i$ tends to zero and each term in sum (4) can be viewed as the first derivative value of function $-Q$ at point $(i\Delta + y_n)/\sigma_v$. Hence, it comes $p_1(y_n) = (2\pi\sigma_v^2)^{-1/2} \sum_{i\in\mathbb{Z}} \exp(-\frac{(i\Delta+y_n)^2}{2\sigma_v^2})$ for $y_n \in [-\frac{\Delta}{2}, \frac{\Delta}{2}]$ and is null otherwise. $(P_M^{(N)}, P_F^{(N)})$ and $P_E^{(N)}$ for QIM are derived according to the same method as in the DC case.

4.3. SS Performances

Since host-interference rejecting capability does not hold for SS, performances [3] depend on host signal. It is assumed that $\boldsymbol{s}$ is i.i.d. centered gaussian, with variance per component σ_s^2. We define the signal-to-noise power ratio by $snr = \sigma_s^2/\sigma_v^2$. Watermark $\boldsymbol{w}$ is generated by a centered pseudo-random sequence such that $N^{-1}\|\boldsymbol{w}\|^2 = D_w$. Thus, we have $\boldsymbol{r}_{|H_1} \sim \mathcal{N}\left(\boldsymbol{w}, (\sigma_s^2+\sigma_v^2)\boldsymbol{I}_N\right)$ and $\boldsymbol{r}_{|H_0} \sim \mathcal{N}\left(\boldsymbol{0}, (\sigma_s^2+\sigma_v^2)\boldsymbol{I}_N\right)$ where $\boldsymbol{I}_N$ denotes the $N \times N$ identity matrix. Likelihood ratio test then reads $\Lambda(\boldsymbol{r}) = \log \frac{Pr(\boldsymbol{r}|H_1)}{Pr(\boldsymbol{r}|H_0)}$ and it is straightforward to establish that $P_M^{(N)} = Q\left(\sqrt{\frac{Nwnr}{1+snr}} - Q^{-1}(P_F^{(N)})\right)$ and $P_E^{(N)} = Q\left(\frac{1}{2}\sqrt{\frac{Nwnr}{1+snr}}\right)$.

5. PERFORMANCE COMPARISON

We now compare performances of the three considered schemes. We also recall the performance of the data-hiding version of the DC-QIM [1] also evaluating with large deviation techniques. In terms of ROC and $P_E^{(N)}$, DC-QIM (with a DC suitably optimized) always outperforms QIM and SS for all wnr and for all N, particularly for wnr's of interest, *i.e.* low and medium wnr's (see Figs. 3, 4, and 5). For $wnr = 0$ dB, it is shown that DC-QIM with 64 samples in the detector outperforms QIM with 256 samples. Moreover, for $wnr = 0$ dB and for $N = 64$, $P_E^{(N)}$ for DC-QIM, QIM and SS are respectively 3.3×10^{-3}, 0.13 and 0.35, illustrating that DC provides improvements of several orders of magnitude. For high wnr's, DC-QIM and QIM tend to be equivalent since α tends to one. As a typical result, DC-QIM achieves both false-alarm and miss probabilities of about 10^{-8} for $N = 256$, which corresponds to the (relatively small) surface of 4 DCT blocks of 8×8 pixels. This stands as a promising point for practical image watermarking [5]. One can note that SS with $snr = 20$dB performs better than QIM with respect to the probability of error for wnr lower than about -2.6 dB (see Fig. 5). On this limit, QIM and SS ROC curves provide equivalent performances. Above this value, QIM performs better. For low wnr's (< -4 dB), QIM turns out to perform very poor with a probability of error constantly close to 0.5. Without use of DC, QIM becomes unusable for low wnr's.

As mentioned before, our problem can be viewed with a modulation point a view. The use of DC-QIM as a detection system involves a particular binary modulation (say '0' is coded by the null symbol and '1' is coded by a DC-QIM symbol of power D_w) where the two symbols are assumed to be equally likely. For $N = 1$, Eggers [6] already noticed that this modulation is less effi-

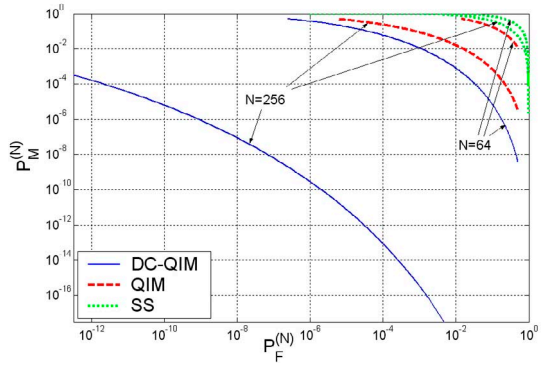

Fig. 3. ROC curves for DC-QIM, QIM and SS with $N = 64$ and $N = 256$ ($wnr = 0$ dB and $snr = 20$ dB).

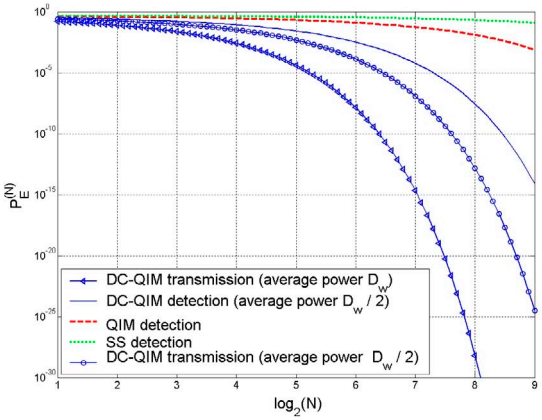

Fig. 4. $P_E^{(N)}$ with respect to N for DC-QIM, QIM, SS and transmission versions of DC-QIM ($wnr = 0$ dB and $snr = 20$ dB).

cient than the one used for data-hiding application (where the two messages are coded by two rival DC-QIM symbols). For evaluating this gap when N increases, we have basically two approaches: (i) the watermarking context imposed a maximal distorsion for perceptual reasons. Then, for $N = 64$ and $wnr = 0$ dB, the transmission version of DC-QIM performs a probability of error of 1.4×10^{-8}whereas we have 3.3×10^{-3} in the detection application. (ii) for a fair comparison of modulations, a communication context generally imposes to transmit with constant average power. In this case, note that the average transmitted power in the detection case is $(0 + D_w)/2$ thus the symbols transmitted in the transmission context should have power of $D_w/2$. The transmission probability of error is now 1.3×10^{-4} and the gap is notably reduced. However, it is likely that applicative considerations will forbid the use of such a high power in the detection problem, since the distortion in presence of watermark would become perceptible.

6. CONCLUSIONS AND PERSPECTIVES

We have investigated the performances of uniform quantized-based schemes using distortion-compensated principle applied to one-bit watermarking. To achieve the watermark detection, exact

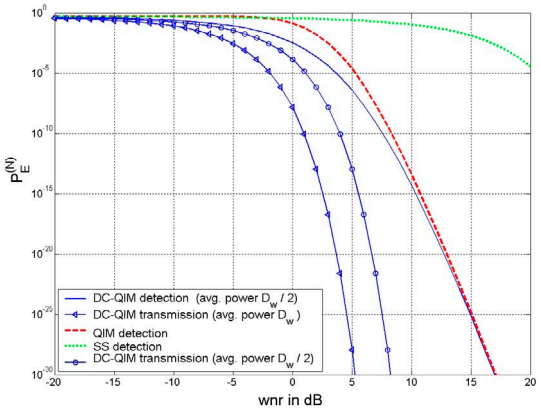

Fig. 5. $P_E^{(N)}$ with respect to wnr for DC-QIM, QIM, SS and transmission versions of DC-QIM ($N = 64$ and $snr = 20$ dB).

likelihood ratio test has been implemented. We have established that the optimal distortion compensation factor for the considered context is analogous to ones shown to be optimal in data-hiding context. Besides, it has been pointed out that false-alarm and miss detection capabilities are jointly optimized by the same DC value. Then, using large deviation theory, we have derived system performance profile. Regarding to both ROC and probability of error criteria, DC-QIM always outperforms QIM and SS. It has been underlined that DC improves significantly quantized-based schemes, particularly in the range of wnr of interest, that is 0 dB. For low wnr's, the used of DC is even needed to ensure better performance than spread spectrum embedding. Such as in data-hiding context, the perspective of using more sophisticated lattice quantizers [7] than the elementary cubic structure promises potential performance gain.

7. REFERENCES

[1] 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, pp. 1423-1443, may 2001.

[2] J. J. Eggers, R. Bauml, R. Tzschoppe, B. Girod, "Scalar Costa Scheme for Information Embedding", *IEEE Trans. Signal Processing*, vol 51, No 4, pp. 1003-1019, April 2003.

[3] J.R. Hernandez, F. Perez-Gonzalez, "Statistical Analysis of Watermarking Schemes for Copyright Protection of Images", Proc. of the IEEE, Volume 87, Issue 7, July 1999, pp. 1142-1166.

[4] Y. Steinberg and N. Merhav, "Identification in the Presence of Side Information with Application to Watermarking", *IEEE Trans. Information Theory*, vol. 47, No. 4, pp. 1410-1422 , May 2001.

[5] J. P. Boyer, P. Duhamel and J. Blanc-Talon, "Game-Theoretic Analysis of a Semi-Fragile Watermarking Scheme Based on SCS", *ICIP 2005*, Genoa, Italy.

[6] J. J. Eggers, B. Girod, "Blind Watermarking Applied to Image Authentication", *ICASSP*, Salt Lake City, USA, May 2001.

[7] T. Liu, P. Moulin, "Error Exponent for One-Bit Watermarking", *ICCASP 2003*, Hong Kong, China.

[8] L. Pérez-Freire, , P. Comesaña-Alfaro, and F. Pérez-González. "Detection in quantization-based watermarking: performance and security issues", *SPIE, Watermarking of Multimedia Contents VII*, San Jose, USA, January 2005.

[9] R. M. Gray, D. L. Neuhoff, "Quantization", *IEEE Trans. on Information Theory*, Vol. 44, No. 6, pp. 2325-2383, October 1998.

[10] A. Shwartz and A. Weiss, "Large Deviation for Performance Analysis: Queues, Communications, and Computing", Chapman & Hall, 1995.

[11] H.L. Van Trees, "Detection, Estimation, and Modulation Theory", *John Wiley & Sons, Inc.*, Part I.