Some theoretical aspects of watermarking detection

Teddy Furon, Julie Josse, Sandrine Le Squin

Some theoretical aspects of watermarking detection

T. Furon, J. Josse, and S. Le Squin

INRIA, IRISA Campus de Beaulieu, Rennes, France

ABSTRACT

This paper considers watermarking detection, also known as zero-bit watermarking. A watermark, carrying no hidden message, is inserted in content. The watermark detector checks for the presence of this particular weak signal in content. The paper aims at looking to this problem from a classical detection theory point of view, but with side information enabled at the embedding side. This means that the watermarking signal is a function of the host content. Our study is twofold. The first issue is to design the best embedding function for a given detection function (a Neyman-Pearson detector structure is assumed). The second issue is to find the best detection function for a given embedding function. This yields two conditions, which are mixed into one 'fundamental' differential equation. Solutions to this equation are optimal in these two senses. Interestingly, there are other solutions than the regular quantization index modulation scheme. The JANIS scheme, for instance, invented in a heuristic manner several years ago, is justified as it is one of these solutions.

1. INTRODUCTION

In the past five years, side-informed embedding strategies have been shown to greatly improve watermark *decoding*. They exploit knowledge of the host signal during the construction of the watermark signal. The theory underlying these side-informed schemes was presented in the famous paper "Writing on Dirty paper" by M. Costa in 1983. Our work gives some theoretical aspect of the achievable performances when using side-information at the embedding side, as in Costa's correspondence, but for the watermark *detection* (aka zero-bit watermarking) problem. This surprisingly received almost no study compared to the issue of watermark decoding, although it is perceived as a non trivial problem.[1] Some exceptions are works from M. Miller et al (embedding cone),[2] JANIS[3] and watermark detection with QIM schemes.[4]

1.1. Motivations from the application side

The trade-off between payload of the hidden message and robustness is a well known fact in watermarking. The main rationale for zero-bit watermarking, as defined in Sect. 2.2.3 of I.Cox et al book,[5] is that maximum robustness is targeted as the payload is reduced to the minimum. Here are two application scenarios where zero-bit watermarking might be sufficient, i.e. it is not necessary to hide a message, but just a presence of a mark.

Some copy protection platforms[6] use watermark as a flag whose presence warns compliant devices that the piece of content they are dealing with, is a copyrighted material. Content access and copy protection are tackled by cryptographic primitives. Watermarking just prevents the 'analog hole'.[7–9] In other words, compliant devices expect three kinds of content: commercial content which are encrypted and watermarked, free content which are in the clear and not watermarked, and pirated content through the 'analog hole' which are in the clear but watermarked. Although some DRM systems hide a message as the copy status, we have seen here that the presence of a mark is indeed sufficient.

Copyright protection is the most famous application of watermarking. However, hiding the name of the author in his work is not a legal proof. In Europe, the only legal way is the following: first, the author must be a member of an author society, then he registers his work. The only legal proof is to bring evidence that the suspicious image is indeed a version of a work belonging to the author society's database. Consequently, this is a yes/no question, which can be solved by detecting the presence or absence of a watermark previously embedded by this author society.

Further author information: (Send correspondence to T.F.)
T.F.: E-mail: teddy.furon@irisa.fr

In these two scenarios, we believe that the presence of a watermark is not a secret. The attacker wanting to remove this mark, obviously knows which content is watermarked. In the copy protection application, for instance, there is no point in attacking a personal video which is a 'free copy' content, not protected neither by encryption nor by watermarking.

1.2. Motivations from the scientific side

Zero-bit watermarking is closely related to detection of weak signals in noisy environment: the watermark signal is embedded in a host signal, unknown to the detector. Its power is very weak compared the one of the host. Watermarkers resorted to elements of detection theory (or binary hypothesis testing) very early. This includes the use of Neyman-Pearson and Pitman-Noether theorems, calculus of efficacy, LMP tests (Locally Most Powerful),[10] and robust statistics.[11]

The priority was at these times to design a better detector than the classical correlation, which is only optimal for white gaussian host signals. To name a few, this includes the works of teams such as Q. Cheng and T. Huang,[12] A. Briassouli and M. Strinzis,[13] M. Barni et al.[14] They assumed that the host signals follow a known pdf (probability density function), and they applied classical elements of detection theory above-mentioned. X. Huang and B. Zhang relaxed this implicit assumption and set that the 'real' pdf of the host belongs to a given family of functions.[15] The test should be designed to fairly perform for the entire family. This allows to encompass attacks modifying this pdf into this family.

Another track is to see the host signal as a side information only available at the embedding. Side information brings huge improvements in watermark decoding. However, its use for zero-bit watermarking has received less interest. Pioneer works are mostly heuristic approaches.[2, 16] More recent works use the binning principle to achieve zero-bit watermarking,[4, 17] although J. Eggers noticed that SCS is less efficient for zero-bit than positive rate watermarking scheme (See Sect. 3.6 of his book[18]). Indeed, Erez *et al.* proved the optimality of Lattice QIM for strictly positive rate data hiding as far as an additive white gaussian noise attack is considered.[19] In the case of zero-rate watermarking, P. Moulin *et al.* reasonably conjecture that sparse Lattice QIM is optimal.[20] For zero-bit watermarking, Lattice QIM achieves high performances showing some host interference rejection.[4] However, there is a loss of efficacy compared to the private setup where the side information is also available at the detector.

1.3. Strategy of this paper

N. Merhav mentioned during the WaCha'05 workshop in Barcelona, that zero-bit watermarking is a hard problem whose optimal solution is not known for the moment.[1] Especially, up to now, there is no reason why the binning principle should be optimal, even if it has the best performances against an AWGN attack. Moreover, QIM schemes are known to be weak against scale gain attack.

We would like to follow a different track, closer to the theory of weak signal detection but taking into account the side information at the embedding. Our goal is not to work on an accurate statistical model of the host signal as done in prior wroks. On contrary, we will use very basic assumptions (gaussian distribution or flat-host assumption) in order to stress how side information increases performances.

2. BOUNDS

The ambition of this section is extremely small. It is only a pastiche of M. Costa's article but formulated in detection theoretical terms rather than with mutual information, capacity, and so on. Our motivation is to illustrate that decoding one bit is strongly different from detecting whether a content has been watermarked or not, although many authors in watermarking literature have been confusing these two topics.

2.1. Mathematical model

We wish to detect the presence of a watermark signal in a digital content. As depicted in Fig. 1, the embedder transforms an original host signal $\mathbf{S}$ into a watermarked content $f(\mathbf{S}) = \mathbf{S} + \mathbf{X}$. The host signal or channel state $\mathbf{S}$ in composed of some components of the original content and is assumed to be a sequence of n independent identically distributed (i.i.d.) $\mathcal{N}(0, Q)$ random variables. The watermark signal must not bring any annoying perceptual artefacts so that, in our simple model, f must satisfy the following power constraint:

$$\frac{1}{n}\mathrm{E}\{\|f(\mathbf{S}) - \mathbf{S}\|^2\} \leq P, \tag{1}$$

where E is the mathematical expectation. In real application, the power P of the watermark signal is indeed very weak compared to Q for invisibility reason.

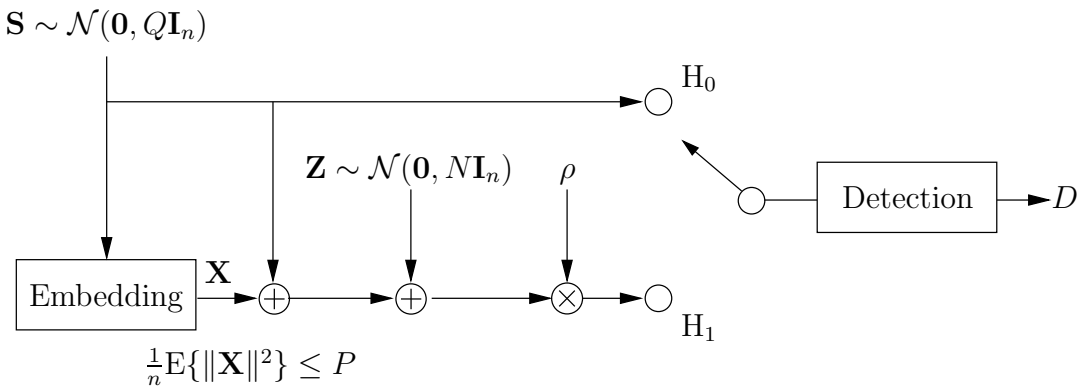

Figure 1. Framework for watermark detection

The channel output is given by $\mathbf{R}_1 = \rho(\mathbf{S} + \mathbf{X} + \mathbf{Z})$, where the channel noise $\mathbf{Z}$ which represents the impact of an attack, is assumed to be distributed according to $\mathcal{N}(0, N\mathbf{I}_n)$ ($\mathbf{I}_n$ is the $n \times n$ identity matrix). Scaling factor $\rho = \sqrt{Q/(Q+N)}$ renders the power of $\mathbf{R}_1$ (we approximate $P + Q \sim Q$) equal to the power of $\mathbf{S}$ while keeping a watermark to noise ratio P/N.

Upon receipt of $\mathbf{R}$ the detector makes a binary decision D: $d = 1$ ($d = 0$) means that, according to the detector, the analysed piece of content is watermarked (resp. it has not been watermarked). There are two hypotheses: Under hypothesis H_0, the detector receives an original content $\mathbf{R} = \mathbf{R}_0 = \mathbf{S}$ (see end of subsection 1.1 for justifications), whereas under hypothesis H_1, the detector receives a watermarked but attacked content $\mathbf{R} = \mathbf{R}_1$. Probability of false alarm P_{fa} and power of the test P_p are given by

$$P_{fa} = \Pr\{D = 1 | \mathrm{H}_0\} \quad ; \quad P_p = \Pr\{D = 1 | \mathrm{H}_1\}. \tag{2}$$

This is the standard watermark Gaussian model with power constraint P, where the embedder is informed of part of Gaussian additive noise sequence that will be added to his watermark signal. Unfortunately, in blind schemes, this information is not made available to the detector, who will have to base its decision D solely on received vector $\mathbf{R}$.

At first glance, it would seem that the problem of watermark detection is simpler than the decoding of hidden symbols, because the detection's output belongs to a message space which is bigger than the actual range $\mathbb{B} = \{0, 1\}$. In other words, whereas the watermark detection implies a simple binary hypotheses test, the decoding of watermark is a complex multiple hypotheses test.

Yet, no theoretical limit has been shown for watermark detection. In the decoding problem, M. Costa[21] first pointed out that the capacity $C^\star$ of a channel with side-information at the encoder is obviously in between $C(P/(Q+N))$, capacity of a channel without side information, and $C(P/N)$, capacity of a channel with side

information at the encoder and decoder side, where $C(x) = \frac{1}{2}\ln(1+x)$. Then, inventing an embedding scheme and thanks to the Gel'fand and Pinsker's formula, he has shown that the upper bound is achievable: $C^\star = C(P/N)$. The main insight is that the optimal capacity doesn't depend on the power of the original vector and it is equal to the capacity when the decoder is not blind.

In watermarking detection, no symbol is transmitted. Our problem is then fundamentally different from the communication of one bit because, under hypothesis H_0, no processing is applied and $\mathbf{S}$ is directly sent to the detector. The channel capacity is not relevant in this context. Our goal is to distinguish which of two probability density functions, $p_{\mathbf{R}_0}$ or $p_{\mathbf{R}_1}$, received vector $\mathbf{R}$ is drawn from. Whereas $p_{\mathbf{R}_0} = p_{\mathbf{S}}$ is imposed by the nature of the extracted components of the original content, function f turns it into a substentially different pdf $p_{\mathbf{R}_1}$. The discrimination between the two pdf plays the role of the channel capacity as it is useful for forming bounds on the detection performances. Thanks to the data processing theorem,[22] we have:

$$L(\mathbf{R}_0;\mathbf{R}_1) \geq L(D_0;D_1). \tag{3}$$

The discrimination $L(\mathbf{R}_0;\mathbf{R}_1)$ between pdfs $p_{\mathbf{R}_0}$ and $p_{\mathbf{R}_1}$ upper bounds discrimination $L(D_0;D_1)$ between $P(D|\mathrm{H}_0) = (1-P_{fa}, P_{fa})$ and $P(D|\mathrm{H}_1) = (1-P_p, P_p)$. For instance, suppose we have $p_{\mathbf{S}} \sim \mathcal{N}(\mathbf{0}, Q\mathbf{I}_n)$ and $p_{\mathbf{R}_1} \sim \mathcal{N}(\mathbf{a}, Q\mathbf{I}_n)$:

$$L(\mathbf{R}_0;\mathbf{R}_1) = \int_{\mathbb{R}^n} p_{\mathbf{R}_0}(\mathbf{r}) \ln \frac{p_{\mathbf{R}_0}(\mathbf{r})}{p_{\mathbf{R}_1}(\mathbf{r})} d\mathbf{r} = \frac{1}{2Q}\mathrm{E}_{\mathbf{R}_0}\{\|\mathbf{r}-\mathbf{a}\|^2 - \|\mathbf{r}\|^2\} = \frac{\|\mathbf{a}\|^2}{2Q}, \tag{4}$$

and

$$L(D_0;D_1) = (1-P_{fa})\ln\frac{1-P_{fa}}{1-P_p} + P_{fa}\ln\frac{P_{fa}}{P_p}. \tag{5}$$

$L(\mathbf{R}_0;\mathbf{R}_1)$ is constraining the receiver operating point (P_{fa}, P_p). A high discrimination is a necessary condition to have good detection performances. Finally, the watermark detection problem is equivalent to finding the embedding function f that maximises $L(\mathbf{R}_0;\mathbf{R}_1)$ under the power constraint P and the fact that an attack occurs on the way to the receiver. In the sequel, we give the bounds of $L(\mathbf{R}_0;\mathbf{R}_1)$.

2.2. Bounds

Contrary to the channel capacity, $L(\mathbf{R}_0;\mathbf{R}_1)$ is not a measure representing the nature of a channel, as it also depends on the chosen function f. For instance, the identity is a possible choice which leads to the equality $p_{\mathbf{R}_1} = p_{\mathbf{S}}$ (thanks to scaling factor ρ and the Gaussianity assumption), whence $L(\mathbf{R}_0;\mathbf{R}_1) = 0$. Denote $\mathcal{F}_P$ the set of functions fulfilling the power constraint (1). We define $\overline{L}(\mathbf{R}_0;\mathbf{R}_1)$ as:

$$\overline{L}(\mathbf{R}_0;\mathbf{R}_1) = \max_{f\in\mathcal{F}_P} L(\mathbf{R}_0;\mathbf{R}_1). \tag{6}$$

Copying the rationale from M. Costa, it is obvious that a lower bound of $\overline{L}(\mathbf{R}_0;\mathbf{R}_1)$ is $K(P/(Q+N))$, where $K(x) = nx/2$. This corresponds to the situation without any side information. Function f produces a signal $\mathbf{X}$ independent of $\mathbf{S}$ and with the maximum energy allowed $\sum_{i=1}^n X_i^2 = nP$. Consequently, $p_{\mathbf{R}_1} \sim \mathcal{N}(\rho\mathbf{X}, Q\mathbf{I}_n)$ and Eq. (4) yields the result.

The upper bound is a little more complicated to find out. If we apply the rationale of M. Costa, this latter is given assuming the embedder and the detector both know channel state $\mathbf{S}$. As the expected discrimination is nondecreasing under conditioning,[22] we have*: $\overline{L}(\mathbf{R}_0;\mathbf{R}_1) \leq \overline{L}(\mathbf{R}_0;\mathbf{R}_1|\mathbf{S})$. A perfect detector is then possible. It outputs $d=1$ if $\mathbf{R} \neq \mathbf{S}$, $d=0$ if $\mathbf{R} = \mathbf{S}$. We are sure that $L(\mathbf{R}_0;\mathbf{R}_1) = +\infty$ as $(P_{fa}, P_p) = (0,1)$ implies $L(D_0;D_1) = +\infty$. Moreover, it is still true when $P \to 0^+$. In conclusion, whereas this rationale led to a useful bound in watermark decoding, we don't learn anything in watermarking detection.

To discover a closer upper bound, we change our framework to an equivalent problem depicted in Fig. 2. The attack is reproduced even on original content, i.e. under hypothesis H_0, $\mathbf{R}_0 = \rho(\mathbf{S}+\mathbf{Z})$. This has absolutely no

*The expected discrimination is defined on expectation across the randomness of $\mathbf{S}$, and not for a specific $\mathbf{S} = \mathbf{s}$: $L(\mathbf{R}_0;\mathbf{R}_1|\mathbf{S}) = \int L(\mathbf{R}_0;\mathbf{R}_1|\mathbf{S}=\mathbf{s})p_{\mathbf{S}}(\mathbf{s})d\mathbf{s}$.

signification in real life. An attacker has no interest in pirating an original content which contains no watermark signal, as discussed in subsection 1.1. Yet, from an information theory point of view, the two frameworks are equivalent as $p_{\mathbf{R}_0}$ is still distributed as $\mathcal{N}(0, Q\mathbf{I}_n)$. The detector is doing the same task in both frameworks. The function f which maximises $L(\mathbf{R}_0; \mathbf{R}_1)$ in the second case produces the same distance in our first framework, and vice versa. Hence, both frameworks share the same maximum discrimination $\overline{L}(\mathbf{R}_0; \mathbf{R}_1)$.

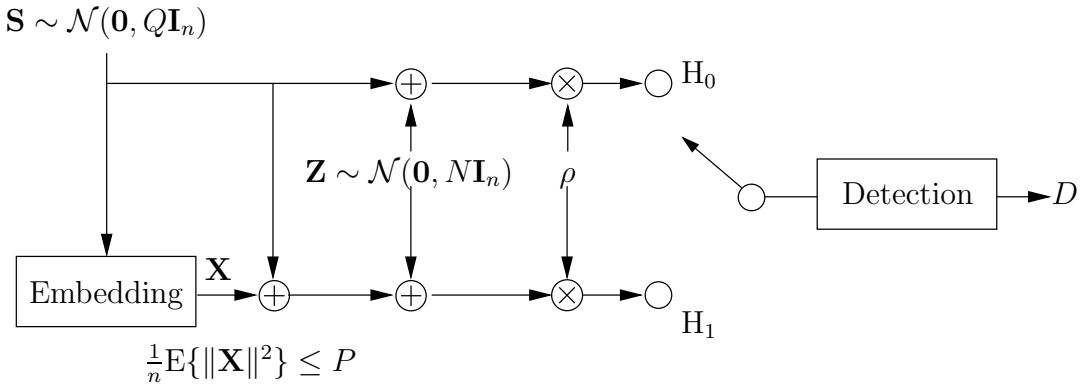

Figure 2. Equivalent framework

Let us now apply Costa's rationale on the second framework: the upper bound is given when the channel state is available at the detection side. The detector has to make a distinction between $\mathbf{R}_1 = \rho(\mathbf{X} + \mathbf{S} + \mathbf{Z})$ and $\mathbf{R}_0 = \rho(\mathbf{S} + \mathbf{Z})$ knowing the channel state $\mathbf{S}$. Hence $\mathbf{R}_0$ is distributed as $\mathcal{N}(\rho\mathbf{S}, \rho^2 N\mathbf{I})$, whereas the pdf of $\mathbf{R}_1$ is $\mathcal{N}(\rho(\mathbf{S} + \mathbf{X}), \rho^2 N\mathbf{I})$. This produces the following discrimination:

$$\overline{L}(\mathbf{R}_0; \mathbf{R}_1|\mathbf{S}) = \frac{nP}{2N} = K(P/N). \tag{7}$$

The conclusion of this short study is the following inequality:

$$K\left(\frac{P}{N+Q}\right) \leq \overline{L}(\mathbf{R}_0; \mathbf{R}_1) \leq K\left(\frac{P}{N}\right). \tag{8}$$

2.3. Comparison to the upper bound

This section compares the discrimination induced by embedding functions from classical zero-bit watermarking schemes to the upper bound. For this matter, we compute the ratio $\kappa = L(\mathbf{R}_0; \mathbf{R}_1)/K(P/N)$.

Before, we analyse the special case $N = 0$ where the upper bound goes to $+\infty$. Let f be a quantizer q inducing a distortion energy lower than nP. It means that $\mathbf{X}$ is indeed the quantization error $q(\mathbf{S}) - \mathbf{S}$. This process transforms the pdf $p_{\mathbf{S}}$ into a probability mass function $P_{\mathbf{R}_1}$. $\mathbf{R}_0$ is a continuous random vector, whereas $\mathbf{R}_1$ is a discrete random variable belonging to the set $\mathcal{Q}$ of codewords. A perfect test with $(P_{fa}, P_p) = (0, 1)$ is possible. It outputs $d = 1$ if $\mathbf{r} \in \mathcal{Q}$, $d = 0$ else. As the probability that the continuous random variable $\mathbf{S}$ exactly equals a codeword is null, then $P_{fa} = 0$. $L(D_0; D_1) = +\infty$ and consequently $L(\mathbf{R}_0; \mathbf{R}_1) = +\infty$.

ISS is a watermarking scheme proposed by H. Malvar and D. Florêncio.[23] The embedding function is defined as:

$$f(\mathbf{S}) = \mathbf{S} + (\alpha - \lambda \mathbf{S}^t \mathbf{U})\mathbf{U}. \tag{9}$$

where $\mathbf{U}$ is a vector with unity norm known at the embedding and the detection sides, $\alpha \in \mathbb{R}^+$ and $\lambda \in [0, 1]$ are two parameters such that $nP = \alpha^2 + \lambda^2 Q$ to fulfil power constraint (1). If $\lambda = 0$, f is indeed the very well known direct sequence spread spectrum watermarking technique. If $\lambda = 1$, f corresponds to the fixed normalized correlation embedding strategy explained in I.Cox et al book.[5] M. Costa named it the 'fight and cancel' strategy

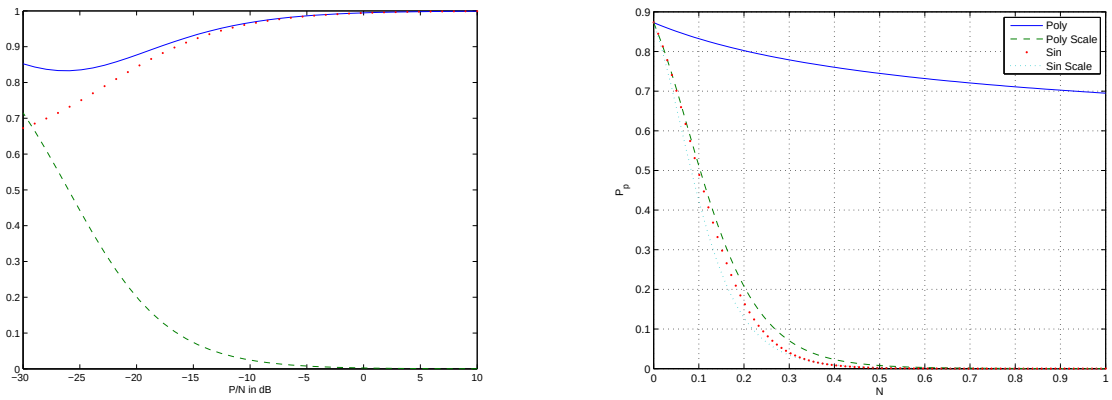

Figure 3. a) Graph of $\kappa(P/N)$ for $n = 1024$, $Q = 1$, $P/Q = -26$dB. Dashed line: $\lambda = 0$, this corresponds to DSSS but also to the lower bound $\kappa^{DSSS}(P/N) = K(P/(Q+N))/K(P/N)$. Dotted line: $\lambda = 1$, this corresponds to the 'erase and set' strategy. Plain line: $\lambda = \lambda^\star$, this is $\kappa^{ISS}(P/N)$. b) Power of polynomial and sinusoidal schemes.

where part of the watermark power is used to cancel the impact of the channel state. This is only possible with ISS if $nP \geq Q$. After some calculus, we get:

$$\kappa^{ISS}(\lambda) = \frac{N}{nP}\left(\frac{nP - \lambda^2 Q + Q/\rho^2}{(1-\lambda)^2 Q + N} - 1 + \ln\frac{\rho^2((1-\lambda)^2 Q + N)}{Q}\right), \tag{10}$$

which is maximal for $\lambda = \lambda^\star$, solution of the following equation:

$$\pi(\lambda) = -\lambda^3 + 2\lambda^2 + \frac{nP + N - Q}{Q}\lambda - \frac{nP}{Q} = 0. \tag{11}$$

Note that we are sure to find $\lambda^\star \in [0,1]$ as π is a continuous function and $\pi(0) = -nP/Q$ and $\pi(1) = N/Q$.

Asymptotically, when $n \to +\infty$, $\lambda^\star \to 1$ and

$$\lim_{n\to+\infty} \kappa^{ISS}(\lambda^\star) = 1. \tag{12}$$

Hence, asymptotically, $\overline{L}(\mathbf{R}_0;\mathbf{R}_1)$ equals $K(P/N)$. ISS achieves the upper bound for long sequences. Note that, for a finite n such that $nP \geq Q$, it is also the case when $N \to 0$. Figure 3 plots ratio κ against the watermark to noise power ratio in dB. We have chosen $n = 1024$, $Q = 1$ and $P/Q = -26$dB. The ISS embedder is linear, thus, according to Eq. (18) of N. Merhav paper,[1] it is not the optimal embedder. However, our purpose is absolutely not to propose the optimal (once again, this is a hard problem[1]), but to illustrate with a well known scheme (but only asymptotically) that $\overline{L}(\mathbf{R}_0;\mathbf{R}_1) = K\left(\frac{P}{N}\right)$. It has been shown that the discrimination of a watermarking detection framework with additive Gaussian noise followed by Wiener filtering and power constrained embedding is not affected by the cover signal as long as knowledge of this sequence is given to the embedder.

It is quite important to outline the limitation of this section. Our rationale only works with one type of attack (addition of white gaussian noise and Wiener filtering) and one type of pdf, i.e. white gaussian noise. The upper bound is extremely important from a theoretical point of view, but practical limitations may spoil a high $L(\mathbf{R}_0;\mathbf{R}_1)$. The Neyman-Pearson theorem states that the detector first calculates a statistic $T \in \mathbb{R}$ whose thresholding yields binary decision $D \in \mathbb{B}$. Sufficient statistic $T(\mathbf{R}) = \ln p(\mathbf{R}|\mathrm{H}_1)/p(\mathbf{R}|\mathrm{H}_0)$ insures that there is no loss of information, i.e. $L(T_0;T_1) = L(\mathbf{R}_0;\mathbf{R}_1)$. Yet, it may be impossible to calculate this sufficient statistic. For instance, the exact pdf $p_{\mathbf{S}}$, the embedding power P and the attack really undergone might depend from a content to another. In real life application, watermarking detectors are only Locally Most Powerful tests.

2.4. Digression

T. Liu and P. Moulin worked on a third framework where $\mathbf{R}_0 = \mathbf{S} + \mathbf{Z}$ and $\mathbf{R}_1 = \mathbf{X} + \mathbf{S} + \mathbf{Z}$. There is no scaling factor ρ. With the Gaussianity assumption, it happens that this framework has same discrimination bound: $K(P/N)$. It means, that theoretically, this third framework poses a problem as difficult as the first and second ones. However, these authors proposed a practical solution based on the binning strategy, which may not be efficient for the first two frameworks. The scaling factor, unknown at the detection side (and also N), as a collapsing effect on the performances at low watermark to noise power ratio.

3. DETECTION OF WEAK SIGNAL DEPENDENT ON SIDE INFORMATION

This section gives expression for best detectors and best embedding functions, when no attack is lead. From the above section, we know that a quantizer embedding function is optimal. Yet, its performances will collapse with the SAWGN attack. This is the reason why we look for a embedding function as $f(\mathbf{s}, \theta) = \mathbf{s} + \theta\mathbf{x}(\mathbf{s})$ where $\mathbf{x}(.)$ is a smooth function from $\mathbb{R}^n$ to $\mathbb{R}^n$, with the constraint that $\mathrm{E}(\|\mathbf{x}(\mathbf{s})\|^2) = n$. Therefore, $\theta = \sqrt{P}$.

3.1. Best detectors for a given embedding function

We assume that the detector has the structure of a Neyman-Pearson test. First, it applies a function $t(\mathbf{r})$ mapping from $\mathbb{R}^n$ to $\mathbb{R}$. Then, this scalar is compared to a threshold τ: $d = (t(\mathbf{r}) > \tau)$.

The issue is whether the problem is a simple hypothesis test (θ is fixed) or composite one sided hypothesis test ($\theta > 0$). Although we presented it as simple hypothesis test in the previous theoretical section, in practice, pieces of content might bear different watermarking power. Even within a content, the embedding gain might depend on a perceptual adaptation. In this case, θ should be considered as the average embedding gain. In the sequel, we will adapt the value of θ to $\mathbf{s}$. Finally, the watermark signal is weak. For all these reasons, a classical element of detection theory states that the optimal detection function is the Local Most Powerful test in $\theta \sim 0$:

$$t(\mathbf{r}) = k_t \frac{1}{p(\mathbf{r}|H_0)} \left.\frac{\partial p(\mathbf{r}|H_1)}{\partial \theta}\right|_{\theta=0}, \tag{13}$$

with $p(\mathbf{r}|H_0) = p_{\mathbf{S}}(\mathbf{r})$ and $p(\mathbf{r}|H_1) = p_{\mathbf{R}}(\mathbf{r})$. The role of k_t is explained below.

We assume function $f(\mathbf{s}, \theta)$ is invertible: $\mathbf{s} = f^{-1}(\mathbf{r}, \theta)$. This allows to write $p_R(\mathbf{r}) = p_{\mathbf{S}}(f^{-1}(\mathbf{r}, \theta))|J_{f^{-1}}(\mathbf{r}, \theta)|$, with the last term being the Jacobian of f^{-1} taken at $(\mathbf{r}, \theta)$. Developing this last equation, we finally get this expression:

$$t(\mathbf{r}) = -k_t \frac{\mathrm{div}(p_{\mathbf{S}}(r)\mathbf{x}(\mathbf{r}))}{p_{\mathbf{S}}(\mathbf{r})} = -k_t \frac{\nabla p_{\mathbf{S}}(\mathbf{r})^T}{p_{\mathbf{S}}(\mathbf{r})}\mathbf{x}(\mathbf{r}) - k_t \mathrm{div}(\mathbf{x}(\mathbf{r})). \tag{14}$$

The first term corresponds to the regular LMP test, whereas the second term is not null whenever side information is enabled at the embedding side.

According to the Pitman-Noether theorem, a good way to compare tests is to calculate their efficacy R, defined in our case by:

$$R = \left[\left.\frac{\partial \psi(\theta)}{\partial \theta}\right|_{\theta=0}\right]^2 . \frac{1}{{\sigma_{t|\mathsf{H}_0}}^2}, \text{ with } \psi(\theta) = \mu_{t|\mathsf{H}_1}(\theta) - \mu_{t|\mathsf{H}_0} \text{ and } {\sigma_{t|\mathsf{H}_0}}^2 = \mathrm{Var}(t|\mathrm{H}_0). \tag{15}$$

With no loss of generality, we assume that $t(.)$ is such that $\mu_{t|\mathsf{H}_0} = 0$ and $\sigma_{t|\mathsf{H}_0} = 1$ (otherwise, it is easy to work with $(t(.) - \mu_{t|\mathsf{H}_0})/\sigma_{t|\mathsf{H}_0}$). For this reason, the multiplicative constant k_t is introduced in (13).

Mixing (13) and (15), it appears that:

$$R = k_t^{-2} = \int \left(\left.\frac{\partial p_{\mathbf{R}}(\mathbf{r})}{\partial \theta}\right|_{\theta=0}\right)^2 p_{\mathbf{S}}(\mathbf{r})^{-1} d\mathbf{r} \tag{16}$$

3.2. Best embedding function for a given detection function

The detection function being given, the only way to increase R is to work on $\mu_{t|\mathrm{H}_1}(\theta)$:

$$\left.\frac{\partial\psi(\theta)}{\partial\theta}\right|_{\theta=0} = \left.\frac{\partial}{\partial\theta}\mathrm{E}(t(\mathbf{r})|\mathrm{H}_1)\right|_{\theta=0} \tag{17}$$

$$= \mathrm{E}\left(\left.\frac{\partial}{\partial\theta}t(\mathbf{s}+\theta\mathbf{x}(\mathbf{s}))\right|_{\theta=0}\right) = \mathrm{E}(\mathbf{x}(\mathbf{s})^T\nabla t(\mathbf{s})). \tag{18}$$

It appears that, for a given $t(.)$, the embedding strategy maximizing R is to have :

$$\mathbf{x}(\mathbf{s}) = k_x\nabla t(\mathbf{s}) \quad \forall\mathbf{s}\in\mathbb{R}^n. \tag{19}$$

where k_x is a normalizing constant to achieve $\mathrm{E}(\|\mathbf{x}(\mathbf{s})\|^2) = n$, equalling $k_x = \sqrt{n/\mathrm{E}(\|\nabla t(\mathbf{s})\|^2)}$. The efficacy is then equal to:

$$R = n^2k_x^{-2} = n\mathrm{E}(\|\nabla t(\mathbf{s})\|^2). \tag{20}$$

3.3. Synthesis

We know how to design the best embedding function for a given detection function, and how to design the best detection function for a given embedding function. This remembers the Lloyd-Max algorithm in quantization. However, we can insert (19) in (14) yielding a differential equation, that we loosely name 'fundamental equation of zero-bit watermarking':

$$p_{\mathbf{S}}(\mathbf{r})t(\mathbf{r}) + k_tk_x.\mathrm{div}(p_{\mathbf{S}}(\mathbf{r})\nabla t(\mathbf{r})) = 0 \quad \forall\mathbf{r}\in\mathbb{R}^n. \tag{21}$$

Hence, the best couple of detection/embedding functions $\{t(.), \mathbf{x}(.)\}$ is $\{t^\star(.), k_x\nabla t^\star(.)\}$, with $t^\star(.)$ solution of (21). Note that Eq. (16) and (20) are still valid. Therefore, it is possible to build a scheme of a given R (as high as possible), provided (21) admits a solution with $k_xk_t = nR^{-1}$.

This equation can also be written as:

$$\frac{R}{n}t(\mathbf{r}) + \frac{\nabla p_{\mathbf{S}}(\mathbf{r})^T}{p_{\mathbf{S}}(\mathbf{r})}\nabla t(\mathbf{r}) + \nabla^2 t(\mathbf{r}) = 0,$$

$\nabla^2 t(\mathbf{r})$ being the Laplacian of $t(\mathbf{r})$.

4. SOME SOLUTIONS OF THE FUNDAMENTAL EQUATION OF ZERO-BIT WATERMARKING

We are not able to provide a general expression of the class of solutions. However, in some cases, we show some examples of solutions.

4.1. The scalar case

We suppose here that the host samples are i.i.d. such that $p_{\mathbf{S}}(\mathbf{s}) = \prod_{i=1}^n p_S(s_i)$. Moreover, our strategy is to maintain this statistical independence while embedding the watermark: $\mathbf{x}(\mathbf{s}) = (\epsilon_1x(s_1), \ldots, \epsilon_nx(s_n))^T$, where $\boldsymbol{\epsilon}$ is a secret vector, with for instance, $\epsilon_i = \pm1\,\forall i \in \{0, \ldots, n\}$. (14) shows that $t(\mathbf{r}) = \sum_{i=1}^n \epsilon_i t(r_i)$. Denote $R = n\bar{R}$. Finally, (21) boils down to a scalar second-order ordinary differential equation with non constant coefficient:

$$\bar{R}t(r) + \frac{p_S'(r)}{p_S(r)}t'(r) + t''(r) = 0. \tag{22}$$

4.1.1. Gaussian case

We assume that $s \sim \mathcal{N}(0,1)$. (21) becomes even simpler: $\bar{R}t(r) - rt'(r) + t''(r) = 0$. Yet, the solution is not trivial. It is a linear combination of two 'independent' (their Wronskian is not null) confluent hypergeometric functions of the first kind taken in $r^2/2$:

$$t_1(r) = a_1 \, {}_1F_1\left(-\frac{\bar{R}}{2}, \frac{1}{2}, \frac{r^2}{2}\right) + b_1, \tag{23}$$

$$t_2(r) = a_2 r \, {}_1F_1\left(\frac{1-\bar{R}}{2}, \frac{3}{2}, \frac{r^2}{2}\right) + b_2. \tag{24}$$

Constants (a_i, b_i) must be chosen such that $(\mu_{t|\mathsf{H}_0}, \sigma_{t|\mathsf{H}_0}) = (0,1)$. If $\bar{R}$ is an even integer, $t_1(.)$ is a polynomial function. If $\bar{R}$ is a odd integer, $t_2(.)$ is a polynomial function. Table 1 gives the expressions of these polynomial solutions and their associated embedding function. The first line of this Table is the well known direct spread

$\bar{R}$	$x(s)$	$t(r)$	$\frac{\sigma_1^2-\sigma_0^2}{\sigma_0^2}$
1	1	r	0
2	s	$\frac{-1+r^2}{\sqrt{2}}$	$6\theta^2$
3	$\frac{-1+s^2}{\sqrt{2}}$	$\frac{-3r+r^3}{\sqrt{6}}$	$66\theta^2$
4	$\frac{-3s+s^3}{\sqrt{6}}$	$\frac{3-6r^2+r^4}{2\sqrt{6}}$	$608\theta^2$
5	$\frac{3-6s^2+s^4}{2\sqrt{6}}$	$\frac{15r-10r^3+r^5}{2\sqrt{30}}$	$5470\theta^2$
6	$\frac{15s-10s^3+s^5}{2\sqrt{30}}$	$\frac{-15+45r^2-15r^4+r^6}{12\sqrt{5}}$	$49122\theta^2$
7	$\frac{-15+45s^2-15s^4+s^6}{12\sqrt{5}}$	$\frac{-105r+105r^3-21r^5+r^7}{12\sqrt{35}}$	$441392\theta^2$

Table 1. Polynomial solutions of the scalar Gaussian case.

spectrum scheme with a linear correlator, optimal detector in the Gaussian i.i.d. case. The second line is known as the proportional embedding.

4.1.2. Uniform case

We were surprised to find solutions which were very different from the binning principle. The classical 'flat-host' assumption used in QIM scheme states that the host pdf is a piecewise constant function. In this case, (21) defined almost everywhere, is a lot simpler: $\bar{R}t(r) + t''(r) = 0$, whose obvious solutions is $t_1(r) = a_1 \cos(\bar{R}r)$, $t_2(r) = a_2 \sin(\sqrt{\bar{R}}r)$, and hence, $w_1(s) = -\sqrt{2}\sin(\sqrt{\bar{R}}s)$, $w_2(s) = \sqrt{2}\cos(\sqrt{\bar{R}}s)$.

Although these are not exactly the embedding function of the scalar QIM (aka SCS), they look like it at least for their periodic character.

4.2. The vector case

We assume here that $\mathbf{S} \sim \mathcal{N}(\mathbf{0}, \mathbf{I}_n)$. Then, $\nabla p_{\mathbf{S}}(\mathbf{r}) = -p_{\mathbf{S}}(\mathbf{r})\mathbf{r}$, and (21) becomes $\bar{R}t(\mathbf{r}) - \mathbf{r}^T\nabla t(\mathbf{r}) + \nabla^2 t(\mathbf{r}) = 0$.

4.2.1. JANIS is a solution for the Gaussian case

We are not able to find a general solution. However JANIS, a zero-bit watermarking scheme invented heuristically some years ago,[3, 16] is a solution. The detection function is the following one:

$$t(\mathbf{r}) = \sqrt{\frac{p}{n}} \sum_{i=1}^{n/p} \prod_{j=1}^{p} r_{j_i}.$$

Indices j_i are such that r_k appears only once in the detection function, $\forall k \in \{1, \ldots, n\}$. It is easy to see that $\mathbf{r}^T\nabla t(\mathbf{r}) = pt(\mathbf{r})$ and $\nabla^2 t(\mathbf{r}) = 0$. Thus, JANIS with order p is a solution to (21) with $\bar{R} = p$. This theoretical framework proves the optimality of the JANIS scheme.

4.3. Uniform case

(21) reduces to the well known Helmholtz equation: $\bar{R}t(\mathbf{r}) + \nabla^2 t(\mathbf{r}) = 0$, which is usually solved by separation of variables method.

4.4. Additional comments

4.4.1. About the Pitman Noether theorem

As seen in the subsection 3.2, we are able to build schemes whose efficacy R is controlled. It means that, asymptotically, hypothesis H_1 gives a random variable $t(\mathbf{R})$ which is distributed as $\mathcal{N}(\sqrt{R}\theta, 1 + o(\theta))$ (if θ were fixed), whereas, under H_0, $t(\mathbf{R}) \sim \mathcal{N}(0, 1)$. These tests are sometimes called symmetric as both hypothesis yield Gaussian distribution with the same variance, at least to the first order. However, as shown in Table 1, the difference between the two variances gets bigger as $\bar{R}$ increases. For this reason, high efficacy schemes work only for small embedding power P or embedding gain θ: the amplification of the efficacy R is spoiled by a big variance ${\sigma_{t|\mathsf{H}_1}}^2$.

4.4.2. Asymmetric tests

Let us focus more on the variance ${\sigma_{t|\mathsf{H}_1}}^2$. As H. Malvar and D. Florencio did for zero-rate watermarking,[23] we would like to control the value of ${\sigma_{t|\mathsf{H}_1}}^2$, achieving so-called asymmetric tests.

For this purpose, we adapt the gain factor θ to $\mathbf{s}$, such that $\mathrm{E}\{\theta(\mathbf{s})^2\|\mathbf{x}(\mathbf{s})\|^2\} = nP$. Moreover, we still maintain $\mathrm{E}\{\|\mathbf{x}(\mathbf{s})\|^2\} = n$ and the embedding strategy. The idea is that the amplitude of the watermark signal is a very small value so that a Taylor expansion is reasonable around $\theta(\mathbf{s}) = 0$.

$$\begin{aligned}
{\sigma_{t|\mathsf{H}_1}}^2 &= \mathrm{E}\{(t(\mathbf{S} + \theta(\mathbf{S})\mathbf{X}(\mathbf{S})) - \mu_{t|\mathsf{H}_1})^2\} \\
&= \mathrm{E}\{(t(\mathbf{S}) + \theta(\mathbf{S})\nabla t(\mathbf{S})^T\mathbf{X}(\mathbf{S}) - \mu_{t|\mathsf{H}_1} + o(|\theta(\mathbf{s})|))^2\} \\
&= \mathrm{E}\{(t(\mathbf{S}) + k\theta(\mathbf{S})\|\nabla t(\mathbf{S})\|^2 - k\mathrm{E}\{\theta(\mathbf{S})\|\nabla t(\mathbf{S})\|^2\})^2\} + o(nP). \qquad (25)
\end{aligned}$$

Define $\nu(\mathbf{S}) = k\theta(\mathbf{S})\|\nabla t(\mathbf{S})\|^2$, and $\tilde{\nu}(\mathbf{S}) = \nu(\mathbf{S}) - \mathrm{E}\nu(\mathbf{S})$. We then get:

$${\sigma_{t|\mathsf{H}_1}}^2 = 1 + \mathrm{Var}(\tilde{\nu}(\mathbf{S})) + 2\mathrm{E}\{t(\mathbf{S})\tilde{\nu}(\mathbf{S})\}.$$

In order to decrease $\sigma_{t|\mathsf{H}_1}$ in the most efficient way, we impose $\tilde{\nu}(\mathbf{S}) = -c.t(\mathbf{S})$, with constant $1 \geq c \geq 0$:

$${\sigma_{t|\mathsf{H}_1}}^2 = 1 + \mathrm{Var}(ct(\mathbf{S})) - 2c\mathrm{E}\{t(\mathbf{S})^2\} = (1 - c)^2. \qquad (26)$$

Hence, we achieve to reduce $\sigma_{t|\mathsf{H}_1}$. However, this strategy consumes embedding distortion:

$$\begin{aligned}
nP &= \mathrm{E}\{\nu(\mathbf{S})^2/\|\nabla t(\mathbf{S})\|^2\} = \mathrm{E}\{(\mu_{t|\mathsf{H}_1} - c.t(\mathbf{S}))^2/\|\nabla t(\mathbf{S})\|^2\} \\
&= {\mu_{t|\mathsf{H}_1}}^2\mathrm{E}\{\|\nabla t(\mathbf{S})\|^{-2}\} + c^2\mathrm{E}\{t(\mathbf{S})^2\|\nabla t(\mathbf{S})\|^{-2}\} - 2c\mu_{t|\mathsf{H}_1}\mathrm{E}\{t(\mathbf{S})\|\nabla t(\mathbf{S})\|^{-2}\}. \qquad (27)
\end{aligned}$$

For the simple cases explored in this paper, we have a symmetry in $t(.)$ and $p_{\mathbf{S}}(.)$, that imposes a third null term $\mathrm{E}\{t(\mathbf{S})\|\nabla t(\mathbf{S})\|^{-2}\} = 0$. Denote $a = \mathrm{E}\{\|\nabla t(\mathbf{S})\|^{-2}\}$ and $b = \mathrm{E}\{t(\mathbf{S})^2\|\nabla t(\mathbf{S})\|^{-2}\}$. Finally, asymptotically and if P is small or with a power $P_n = P/n$ (see the conditions of Pitman Noether theorem), the receiver operating curve tends to $P_p = 1 - \Phi(\zeta(c))$, with

$$\zeta(c) = \frac{\Phi^{-1}(1 - P_{fa}) - \sqrt{(nP_n - bc^2)/a}}{|1 - c|}. \qquad (28)$$

Basically, a higher c decreases $\sigma_{t|\mathsf{H}_1} = |1-c|$ but also $\mu_{t|\mathsf{H}_1} = \sqrt{(nP_n - bc^2)/a}$ due to the distortion constraint (27). We have to find the best c such that $\zeta(c)$ is minimized.

5. ATTACK NOISE

The attack produces $\mathbf{R}_1 = \rho(\mathbf{S} + \mathbf{X}(\mathbf{S}) + \mathbf{Z})$ with $\mathbf{Z} \sim \mathcal{N}(\mathbf{0}, N\mathbf{I}_n)$. The strength of the attack, represented by power N, is not known at the detection side. We express the efficacy as a function of ρ. We now have :

$$\psi(\theta) = \int\int t(\rho(\mathbf{s} + \theta\mathbf{x}(\mathbf{s}) + \mathbf{z}))p_{\mathbf{S}}(\mathbf{s})p_{\mathbf{Z}}(\mathbf{z})d\mathbf{s}d\mathbf{z} \tag{29}$$

$$\left.\frac{\partial\psi(\theta)}{\partial\theta}\right|_{\theta=0} = \int \rho\mathbf{x}(\mathbf{s})^T \left(\int \nabla t(\rho(\mathbf{s} + \mathbf{z}))p_{\mathbf{Z}}(\mathbf{z})d\mathbf{z}\right) p_{\mathbf{S}}(\mathbf{s})d\mathbf{s}, \tag{30}$$

such that finally $R(\rho) = \rho^2 R(1)\mathrm{E}_{\mathbf{S}}\{\mathbf{x}(\mathbf{s})^T\mathrm{E}_{\mathbf{Z}}\{\mathbf{x}(\rho(\mathbf{s} + \mathbf{z}))\}\}^2$.

5.1. polynomial solutions

Assume first that $\rho = 1$ (no scaling). Then, the efficacy is not modified, however, the variance ${\sigma_{t|\mathsf{H}_1}}^2$ increases. We have:

$$\mu_{t|\mathsf{H}_1} = \sqrt{R(1)}\theta + O(\theta^2) \qquad {\sigma_{t|\mathsf{H}_1}}^2 = {\sigma_{t|\mathsf{H}_0}}^2 + R(1)N + O(N^2) \tag{31}$$

Assuming $\rho = \sqrt{Q/(Q+N)}$ (scaling), the efficacy is clearly modified: $R(\rho) = R(1)\rho^{2\bar{R}}$. However, the situation is better described by the following data:

$$\mu_{t|\mathsf{H}_1} = \sqrt{R(\rho)}\theta + O(\theta^2) \qquad {\sigma_{t|\mathsf{H}_1}}^2 = 1 + O(\theta^2) \tag{32}$$

5.2. sinusoidal solutions

Even knowing that the host is gaussian distributed, we select a scalar solution optimal in the uniform case. In other words, we assume the flat-host assumption. In this case,

$$(x(s), t(r)) = \left(\frac{e^{\frac{\omega^2}{2}}}{\sqrt{\cosh(\omega^2)}}\cos(\omega s), \frac{e^{\frac{\omega^2}{2}}}{\sqrt{\sinh(\omega^2)}}\sin(\omega r)\right).$$

This yields an efficacy $R(1) = n\omega^2\coth(\omega^2)$ when no attack is performed.

When no scaling is performed during the attack, we have the following mean and variance:

$$\mu_{t|\mathsf{H}_1} = \sqrt{R(1)}\theta e^{-\frac{\omega^2 N}{2}} \qquad {\sigma_{t|\mathsf{H}_1}}^2 = e^{-\omega^2 N}\frac{\sinh(\omega^2(1+N))}{\sinh(\omega)}. \tag{33}$$

In case of noise addition plus scaling attack, we have $R(\rho) = R(1)\rho^2\frac{\cosh(\omega^2\rho)^2}{\cosh(\omega^2)^2}$. However, the situation is better described by the following data:

$$\mu_{t|\mathsf{H}_1} = \sqrt{R(\rho)}\theta + O(\theta^2) \qquad {\sigma_{t|\mathsf{H}_1}}^2 = 1 + O(\theta^2). \tag{34}$$

5.3. comparison

Host vectors are white Gaussian noise with length $n = 2048$. The probability of false alarm is set to $P_{fa} = 10^{-4}$ giving a threshold $\tau = 3,719$. The embedding distortion is fixed to -26dB, $\theta = 0.05$. Fig.(**??**) shows the power of the polynomial and sinusoidal tests for the AWGN and SAWGN attacks. These schemes have the same efficacy ($\bar{R} = 4$) when no attack is lead. Polynomial solutions are far more robust in the non-scaling attack, and they perform slightly better in the scaling scenario.

6. CONCLUSION

Our future work is to build better schemes with the idea of mixing different detector functions. We will also look for the worst case attack. This implies that there is a game between the attacker and the embedder. Another interesting point will be to adapt the 'Robust statistics'[11] theory to side information embedding.

REFERENCES

1. N. Merhav, "An information-theoretic view of watermarking embedding-detection and geometric attacks." presented at WaCha05, available at `www.ee.technion.ac.il/people/merhav/`, jun 2005.
2. M. Miller, I. Cox, and J. Bloom, "Informed embedding: exploiting image and detector information during watermark insertion," in *Proc. of Int. Conf. on Image Processing*, IEEE, (Vancouver, Canada), September 2000.
3. J. Delhumeau, T. Furon, N. Hurley, and G. Silvestre, "Improved polynomial detectors for side-informed watermarking," in *Security and Watermarking of Multimedia Contents IV*, pp. 311–321, SPIE Electronic Imaging, (Santa Clara, Cal., USA), January 2003.
4. T. Liu and P. Moulin, "Error exponents for one-bit watermarking," in *Proc. of ICASSP*, (Hong-Kong), apr 2003.
5. I. Cox, M. Miller, and J. Bloom, *Digital Watermarking*, Morgan Kaufmann Publisher, 2001.
6. J. Andreaux, A. Durand, T. Furon, and E. Diehl, "Copy protection system for digital home networks," *IEEE Signal Processing Magazine* **21**, pp. 100–108, March 2004. Special Issue on Digital Right Management.
7. 2004.
8. E. Diehl and T. Furon, "Closing the analog hole," in *Proc. of Int. Consumer Electronics*, IEEE, ed., pp. 52–53, 2003.
9. E. Lin, A. Eskicioğlu, R. Lagendijk, and E. Delp, "Advances in digital video content protection," *Proc. of IEEE* **93**, pp. 171–183, jan 2005.
10. H. V. Poor, *An introduction to signal detection and estimation*, vol. 2nd edition, Springer, 1994.
11. P. Huber, *Robust statistics*, J. Wiley and Sons, 1991.
12. Q. Cheng and T. Huang, "Robust optimum detection of transform domain multiplicative watermarks," *IEEE Trans. Sig. Processing* **51**, pp. 906–924, apr 2003.
13. A. Briassouli and M. Strinzis, "Locally optimum nonlinearities for DCT watermarking detection," *IEEE Trans. Image Processing* **13**, pp. 1604–16017, dec 2004.
14. M. Barni, F. Bartolini, A. de Rosa, and A. Piva, "Optimum decoding and detection of multiplicative watermarks," *IEEE Trans. Signal Processing* **51**, pp. 1118–1123, apr 2003.
15. X. Huang and B. Zhang, "Robust detection of transform domain additive watermarks," in *Proc. of Int. Work. on Digital Watermarking*, M. Barni, ed., *LNCS* **3710**, pp. 124–138, Springer, (Siena, Italy), sep 2005.
16. T. Furon, G. Silvestre, and N. Hurley, "JANIS: Just Another N-order side-Informed Scheme," in *Proc. of Int. Conf. on Image Processing ICIP'02*, **2**, pp. 153–156, (Rochester, NY, USA), September 2002.
17. L. Pérez-Freire, P. C. na, and F. Pérez-González, "Detection in quantization-based watermarking: performances and security issues," in *Security, Steganography, and Watermarking of multimedia contents VII*, E. Delp and P. W. Wong, eds., *Proc. of SPIE-IS&T Electronic Imaging* **5681**, pp. 721–733, (San jose, CA, USA), jan 2005.
18. J. Eggers and B. Girod, *Informed Watermarking*, Kluwer Academic Publishers, 2002.
19. U. Erez and R. Zamir, "Achieving $0.5 \log 1 + SNR$ on additive white gaussian noise channel with lattice encoding and decoding," *IEEE Tran. on IT* , pp. 2293–2314, oct 2004.
20. P. Moulin, A. Goteti, and R. Koetter, "Optimal sparse-QIM codes for zero-rate blind watermarking," in *Proc. of ICASSP*, (Montreal), may 2004.
21. M. Costa, "Writing on dirty paper," *IEEE Trans. on Information Theory* **29**, May 1983.
22. R. Blahut, *Principes and practice of information theory*, Addisson-Wesley, 1987.
23. H. Malvar and D.A.F. Florêncio, "Improved spread spectrum: A new modulation technique for robust watermarking," *IEEE Trans. on Signal Processing* **51**, pp. 868–905, April 2003. Special Issue on Signal Processing for Data Hiding in Digital Media and Secure Content Delivery & secure content delivery, IEEE Trans. on Signal Processing.