Statistical Decision Methods in Hidden Information Detection

Cathel Zitzmann, Rémi Cogranne, Florent Retraint, Igor Nikiforov, Lionel Fillatre, and Philippe Cornu*

ICD - LM2S - Université de Technologie de Troyes - UMR STMR CNRS 6279
12, rue Marie Curie - B.P. 2060 - 10010 Troyes cedex - France
name.surname@utt.fr

Abstract. The goal of this paper is to show how the statistical decision theory based on the parametric statistical model of the cover media can be useful in theory and practice of hidden information detection.

1 Introduction and Contribution

It is an important and useful challenge for security forces to reliably detect in a huge set of files (image, audio, and video) which of these files contain the hidden information (like a text, an image, or an audio or a video record). An efficient statistical test should be able to detect the presence of hidden information embedded in the cover media. It is assumed that the embedding scheme is a priori unknown but it belongs to a commonly used family of steganographic LSB replacement based algorithms. Certainly, such steganographic algorithms are not extremely efficient but they are simple, popular, and downloadable on the Internet and can be easily applied by any person.

In such an operational context, the most important challenge is to get the hidden information detection algorithms with analytically predictable probabilities of false alarm and non detection. These algorithms should be immediately applicable without any supervised learning methods using sets of training examples (SVM-based algorithms). On the contrary, the capacity of a hidden information detection algorithm to detect a very sophisticated but not frequently used embedding algorithm with a low embedding rate is not very important in the framework of the above mentioned scenario.

The recently proposed steganalysers [7,8,9] are certainly very interesting and efficient but these *ad hoc* algorithms have been designed with a limited exploitation of cover media statistical model and hypothesis testing theory. Moreover, the only solution to get the statistical properties of these *ad hoc* algorithms is the statistical simulation by using large databases of cover media.

An alternative approach is to use the hypothesis testing theory with a parametric model of cover media. The first step in the direction of hypothesis testing has been done in [14].

* This work is supported by French National Agency (ANR) through ANR-CSOSG Program (Project ANR-07-SECU-004).

T. Filler et al. (Eds.): IH 2011, LNCS 6958, pp. 163–177, 2011.

In the actual paper, the direction started in [14] is extended to take into account two new phenomena :

- an impact of data quantization on the statistical decision;
- benefits from using a parametric statistical model of cover media.

This paper is mainly, but not exclusively, devoted to the situation when the cover media is represented by a natural image produced by a digital camera. This fact defines the above mentioned points of our interest. The advantages of a parametric statistical model are well known. The hypothesis testing theory is relatively well developed for such models. We are especially interested in the asymptotic decision theory and in dealing with non informative (nuisance) parameters of the cover media model. Both directions are interesting because the number of bytes (or pixels) is typically very large for modern cover media and the nuisance parameters of statistical model are only partially known.

Natural images are obtained by using a digital camera which obligatory includes a quantization. The parameters of statistical model are related to several factors (the scene, the amount of light, the focus, the exposure, the objective lens, CCD,...). Physically these factors define a continuous state space model but the decision should be done by using the quantized output of digital camera. More profound discussion of a parametric statistical model of natural images is in the companion paper [2].

The goal of this paper is threefold :

1. define the statistical framework of hidden information detection based on a parametric model of cover media by using the quantized observations;
2. design optimal statistical tests and to study their statistical properties and the impact of quantized observations on the quality of these tests;
3. theoretically compare the (almost) optimal statistical tests with the WS steganalysers, recently developed and commonly used in hidden information detection.

The paper is organized as follows. The problem of statistical decision based on quantized observations is stated in Section 2. The case of a known embedding rate is discussed. Section 3 is devoted to the problem of quantization. Its impact on the quality of statistical tests (steganalysers) is also studied here. A more general and realistic case of unknown embedding rate is discussed in Section 4. A solution to this case based on the local asymptotic approach is presented in Section 5. Finally, the proposed (almost optimal) detection algorithm is theoretically compared with the WS steganalysers, commonly used in hidden information detection in Section 6. Some conclusions are drawn in Section 7.

2 Statistical Decision Based on Quantized Observations

2.1 Model of Quantized Cover Media

Let us assume that the observation vector $C_n = (c_1, \ldots, c_n)^T$ which characterizes a cover media is defined in the following manner :

$$C_n = Q_1[Y_n], \quad Y_n \sim P_\theta, \tag{1}$$

where $Q_1[y_i] = \lfloor y_i \rfloor$ is the operation of uniform quantization (integer part of y_i) and the vector $Y_n = (y_1, \ldots, y_n)^T$ follows the distribution P_θ parameterized by the parametric vector θ. The binary representation of c (the index is omitted to seek simplicity) is

$$c = Q_1[y] = \sum_{i=0}^{q-1} b_i 2^i, \text{ where } b_i \in \{0,1\}, \quad c \in \{0,1,2,\ldots,2^q-1\}. \tag{2}$$

A simplified model of quantization (1) is used in this paper. It is assumed that the saturation is absent, i.e. the probability of the excess over the boundary 0 or $2^q - 1$ for the observation y is negligible.

2.2 Problem Statement: Test between Two Hypotheses

First, let us define two alternative hypotheses for one quantized observation z (seeking simplicity) :

$$\mathcal{H}_0 \ : \ z = c = Q_1[y] \sim Q_{Q_1} = [q_0, \ldots, q_{2^q-1}] \tag{3}$$

and

$$\mathcal{H}_1 \ : z = \begin{cases} Q_2[y] + z_s \text{ with probability } R \\ c = Q_1[y] \text{ with probability } 1-R, \end{cases} \tag{4}$$

where R is the embedding rate, $Q_2[y] = \sum_{i=1}^{q-1} b_i 2^i$, is a uniform quantization by using 2^{q-1} thresholds, $Q_2[y] \sim Q_{Q_2}$, $z_s \sim Q_s = \mathrm{B}(1,p)$ is the Bernoulli distribution which defines the hidden information (usually $p = 0.5$). In other words, to get the double quantization $Q_2[y]$ from $z = Q_1[y]$ the LSB is deleted, i.e. $b_0 \equiv 0$. Hence, under hypothesis $\mathcal{H}_1$, the LSB is used as a container of hidden information. In the rest of the paper it is assumed that $Q_2[z] = Q_2[y]$.

2.3 A Known Embedding Rate. Two Simple Hypotheses: Likelihood Ratio Test

Let us suppose that the distributions $Q_s(z_s) = 1/2$, $z_s \in \{0,1\}$, Q_{Q_1}, Q_{Q_2} and the embedding rate R are exactly known. In this case the LR for one observation is written as follows :

$$\Lambda_R(z) = R\Lambda_1(z) + (1-R), \quad \Lambda_1(z) = \frac{Q_s(b_0) Q_{Q_2}(Q_2[z])}{Q_{Q_1}(z)} = \frac{Q_{Q_2}(Q_2[z])}{2 Q_{Q_1}(z)}. \tag{5}$$

where b_0 is the LSB of z. The most powerful (MP) Neyman-Pearson test over the class

$$\mathcal{K}_{\alpha_0} = \{\delta : \mathbb{P}_0(\delta(Z_n) = \mathcal{H}_1) \le \alpha_0\}, \tag{6}$$

where $\mathbb{P}_i(\ldots)$ denotes the probability under hypothesis $\mathcal{H}_i$, $i = 0, 1$, is given by the following decision rule :

$$\delta_R(Z_n) = \begin{cases} \mathcal{H}_0 \text{ if } \Lambda_R(Z_n) = \prod_{i=1}^{n} \Lambda_R(z_i) < h \\ \mathcal{H}_1 \text{ if } \Lambda_R(Z_n) = \prod_{i=1}^{n} \Lambda_R(z_i) \ge h \end{cases}, \tag{7}$$

where the threshold h is the solution of the following equation $\mathbb{P}_0(\Lambda_R(Z_n) \geq h) = \alpha_0$. The MP test $\delta_R(Z_n)$ maximizes the power

$$\beta_{\delta_R} = 1 - \mathbb{P}_1(\delta_R(Z_n) = \mathcal{H}_0) = 1 - \alpha_1 \tag{8}$$

over the class $\mathcal{K}_{\alpha_0}$.

3 Simple Model of Cover Media

3.1 Exact and Approximate Likelihood Ratio

Let us assume an independent random sequence $y_1, \ldots, y_n$, $y_i \sim \mathcal{N}(\theta, \sigma^2)$. The quantized variable z_i follows a "discrete" normal distribution i.e. :

$$z_i = Q_1[y_i] \sim Q_{Q_1} = [q_0, \ldots, q_{2^q-1}], \quad z \in [0, 1, 2, \ldots, 2^q - 1], \tag{9}$$

where the coefficients q_i are computed in the following manner

$$q_i = \int_i^{i+1} \varphi(x)dx = \Phi(i+1) - \Phi(i), \quad \varphi(x) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left\{-\frac{(x-\theta)^2}{2\sigma^2}\right\}, \tag{10}$$

where $\Phi(x) = \int_{-\infty}^{x} \varphi(u)du$. It is easy to see that for any R the LR given by equation (5) depends on the observations through the LR ratio $\Lambda_1(z)$ computed under assumption that $R = 1$. The exact equation of this log LR is given by :

$$\begin{aligned} \log \Lambda_1(Z_n) &= n \log \frac{1}{2} + \sum_{i=1}^{n} \log Q_{Q_2}\left(Q_2[z_i]\right) - \sum_{i=1}^{n} \log Q_{Q_1}\left(z_i\right) \\ &= \sum_{i=1}^{n} \frac{1}{2\sigma^2}\Big[-\left(Q_2[z_i] + 1 + \delta_{2,i} - \theta\right)^2 + \left(z_i + 0.5 + \delta_{1,i} - \theta\right)^2\Big]. \end{aligned} \tag{11}$$

The approximate equation of the log LR is

$$\log \Lambda_1(Z_n) \simeq \log \widetilde{\Lambda}_1(Z_n) = \sum_{i=1}^{n} \frac{1}{2\sigma^2}\Big[-\left(Q_2[z_i] + 1 - \theta\right)^2 + \left(z_i + 0.5 - \theta\right)^2\Big]. \tag{12}$$

The corrective terms due to quantization $\delta_{1,i}$ and $\delta_{2,i}$ are omitted in the last equation and in the rest of this section.

3.2 The Moments of Approximate Log Likelihood Ratio

It follows from the central limit theorem [17] that the fraction

$$\frac{\log \widetilde{\Lambda}_1(Z_n) - n\mathbb{E}\left(\log \widetilde{\Lambda}_1(z)\right)}{\sigma\sqrt{n}} \underset{n\to\infty}{\rightsquigarrow} \mathcal{N}(0, 1), \tag{13}$$

where $\sigma^2 = \mathrm{Var}\left(\log \widetilde{\Lambda}_1(z)\right)$, $\rightsquigarrow$ is the weak convergence and $\log \widetilde{\Lambda}_1(Z_n)$ is the approximate log LR given by (12), will converge in distribution to the standard normal distribution as n goes to infinity. The expectation and variance

are denoted by $\mathbb{E}(\ldots)$ and $\mathrm{Var}(\ldots)$ respectively. Hence, to compute the error probabilities it is necessary to get the expectations and variances of the approximate log LR. Under hypothesis $\mathcal{H}_0$, the approximate log LR can be re-written as follows

$$\log \widetilde{\Lambda}_1(Z_n) = \sum_{i=1}^{n} \left[\frac{\zeta_i(b_{0,i} - 0.5)}{\sigma^2} - \frac{(b_{0,i} - 0.5)^2}{2\sigma^2} \right] = \sum_{i=1}^{n} \left[\frac{\zeta_i(b_{0,i} - 0.5)}{\sigma^2} - \frac{1}{8\sigma^2} \right], \quad (14)$$

where $\zeta_i = z_i + 0.5 - \theta$, $b_{0,i} = \mathrm{LSB}(z_i)$ and under hypothesis $\mathcal{H}_1$ is

$$\log \widetilde{\Lambda}_1(Z_n) = \sum_{i=1}^{n} \left[\frac{\xi_i(b_{0,i} - 0.5)}{\sigma^2} + \frac{1}{8\sigma^2} \right], \quad (15)$$

where $\xi_i = Q_2[z_i] + 1 - \theta$ and $b_{0,i} = z_{s,i}$. Under hypothesis $\mathcal{H}_0$, the expectation of the approximate log LR is given by the following expression

$$m_0 = \mathbb{E}_0 \left[\log \widetilde{\Lambda}_1(z) \right] = -\frac{1}{8\sigma^2} + \frac{\varepsilon}{\sigma^2}, \quad (16)$$

where the coefficient ε defines the impact of the quantization. This coefficient is given by

$$\varepsilon = \mathbb{E}_0 \left[\zeta(b_0 - 0.5) \right] = \sum_{m=-\infty}^{\infty} \left[\Phi\left(\frac{2m+2-\theta}{\sigma} \right) - \Phi\left(\frac{2m+1-\theta}{\sigma} \right) \right] \frac{(2m+1.5-\theta)}{2}$$
$$- \sum_{m=-\infty}^{\infty} \left[\Phi\left(\frac{2m+1-\theta}{\sigma} \right) - \Phi\left(\frac{2m-\theta}{\sigma} \right) \right] \frac{(2m+0.5-\theta)}{2}. \quad (17)$$

Finally, the variance is given by

$$\sigma_0^2 = \mathrm{Var}_0 \left[\log \widetilde{\Lambda}_1(z) \right] = \frac{1}{\sigma^4} \left\{ \mathbb{E}_0 \left[\zeta^2 (b_0 - 0.5)^2 \right] - \left[\mathbb{E}_0 \left(\zeta(b_0 - 0.5) \right) \right]^2 \right\} = \frac{\mathbb{E}_0 \left[\zeta^2 \right] - 4\varepsilon^2}{4\sigma^4}, \quad (18)$$

where

$$\mathbb{E}_0 \left[\zeta^2 \right] = \sum_{m=-\infty}^{\infty} \left[\Phi\left(\frac{m+1-\theta}{\sigma} \right) - \Phi\left(\frac{m-\theta}{\sigma} \right) \right] (m+0.5-\theta)^2. \quad (19)$$

Under hypothesis $\mathcal{H}_1$, the expectation and variance of the approximate log LR are given by the following expressions

$$m_1 = \mathbb{E}_1 \left[\log \widetilde{\Lambda}_1(z) \right] = \frac{1}{8\sigma^2}, \quad (20)$$

$$\sigma_1^2 = \mathrm{Var}_1 \left[\log \widetilde{\Lambda}_1(z) \right] = \mathrm{Var}_1 \left[\frac{\xi(b_0 - 0.5)}{\sigma^2} \right] = \frac{1}{4\sigma^4} \mathbb{E}_1 \left[\xi^2 \right], \quad (21)$$

where

$$\mathbb{E}_1 \left[\xi^2 \right] = \sum_{m=-\infty}^{\infty} \left[\Phi\left(\frac{2m+2-\theta}{\sigma} \right) - \Phi\left(\frac{2m-\theta}{\sigma} \right) \right] (m+1-\theta)^2, \quad (22)$$

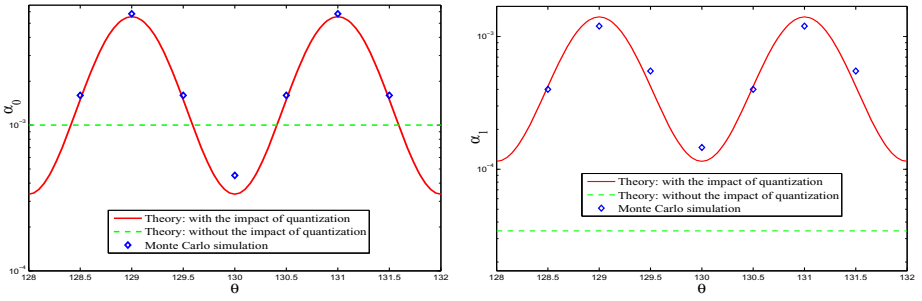

Fig. 1. The impact of the quantization on the probability of false alarm α_0 (left figure) and missed detection α_1 (right figure)

respectively. The following simplified equations can be proposed for the expectation and variance of the approximate log LR given by (12) without taking into account the impact of quantization

$$m_i = (-1)^{i+1}\frac{1}{8\sigma^2}, \quad \sigma_i^2 = \frac{1}{4\sigma^2}, \quad i = 0, 1. \tag{23}$$

Proposition 1. *Let us assume that the true embedding rate takes an arbitrary value* $\widetilde{R} \ : \ 0 < \widetilde{R} \leq 1$. *The power* β_{δ_1} *of the MP test (7) with the log LR* $\log \widetilde{\Lambda}_1(Z_n)$ *given by (12) can be approximated by*

$$\beta_{\delta_1} \simeq 1 - \Phi\left(\Phi^{-1}(1-\alpha_0)\frac{\sigma_0}{\sigma_{\widetilde{R}}} - \frac{(m_1 - m_0)\widetilde{R}\sqrt{n}}{\sigma_{\widetilde{R}}}\right) \tag{24}$$

for large n. *The expectations* m_i *and variance* σ_0^2 *are computed by using equations (16) - (22) (resp. (23)) with (resp. without) taking into account the impact of quantization. The variance* $\sigma_{\widetilde{R}}^2$ *is also computed with taking into account the impact of quantization*

$$\sigma_{\widetilde{R}}^2 = \frac{1}{4\sigma^2}\left[\left(\mathbb{E}_1\left[\xi^2\right] + \frac{1}{16}\right)\widetilde{R} + \left(\mathbb{E}_0\left[\zeta^2\right] + \frac{1}{16} - \varepsilon\right)(1-\widetilde{R})\right] - \left[m_1\widetilde{R} + m_0(1-\widetilde{R})\right]^2 \tag{25}$$

or without taking into account the impact of quantization

$$\sigma_{\widetilde{R}}^2 = \frac{1 + \widetilde{R} - \widetilde{R}^2}{4\sigma^2}. \tag{26}$$

It is worth noting that the explicit for form of the power function β_{δ_1} given in Proposition 1 conforms with the fact established in [10] that the "secure" steganographic capacity is proportional only to the square root of the number of covers n.

To illustrate the impact of the quantization, let us assume the following parameters of the Gaussian cover media model : $\widetilde{R} = 1$, $\theta \in [128; 132]$, $\sigma = 1$ and

$n = 200$. The comparison of theoretical equations for α_0 and α_1 with the Monte Carlo simulation (10^6 repetitions) are presented in Figure 1. The left figure shows the probability of false alarm α_0 calculated with (solid line) and without (dashed line) taking into account the impact of quantization. Here, the required probability of false alarm is $\alpha_0 = 10^{-3}$. First, the threshold h for the MP test $\delta_1(Z_n)$ given by (7) is computed by using equations (23) and (24). Next, the probability of false alarm $\alpha_0 = \alpha_0(h)$ is computed as a function of this threshold by using the corrected equations for the expectations and variances of the log LR, i.e. (16) - (21) and (24) (with taking into account the impact of quantization). The right figure shows the probability of missed detection α_1 calculated with (solid line) and without (dashed line) taking into account the impact of quantization for the prescribed significance level $\alpha_0 = 10^{-3}$. As it follows from Figure 1, the impact of quantization on the probability of false alarm α_0 and missed detection α_1 is significant.

4 An Unknown Embedding Rate: Two Composite Hypotheses

Let us assume that the previously defined distributions are known, but the embedding rate R is unknown. The following alternative composite hypotheses have to be tested by using n observations Z_n representing the cover media :

$$\mathcal{H}_0 = \{R \le r^*\} \text{ against } \mathcal{H}_1 = \{R > r^*\}, \tag{27}$$

where r^* denotes the "frontier" value of embedding rate separating $\mathcal{H}_0$ and $\mathcal{H}_1$. Hence, the LR (5) becomes

$$\Lambda_{R_0,R_1}(Z_n) = \prod_{i=1}^{n} \frac{R_1\Lambda_1(z_i) + (1 - R_1)}{R_0\Lambda_1(z_i) + (1 - R_0)}, \;\; \Lambda_1(z_i) = \frac{Q_{Q_2}\left(Q_2[z_i]\right)}{2Q_{Q_1}\left(z_i\right)} \tag{28}$$

where $R_0 \le r^* < R_1$. The main difficulty is that the values of acceptable R_0 and unacceptable R_1 embedding rates are unknown. The ultimate challenge for anyone in the case of two composite hypotheses is to get a uniformly MP (UMP) test δ which maximises the power function

$$\beta(R) = 1 - \mathbb{P}_R(\delta(Z_n) = \mathcal{H}_0) \tag{29}$$

for any $R > r^*$ over the class

$$\mathcal{K}_{\alpha_0} = \left\{\delta : \sup_{R \le r^*} \mathbb{P}_R(\delta(Z_n) = \mathcal{H}_1) \le \alpha_0\right\} \tag{30}$$

The above mentioned hypothesis testing problem can be efficiently solved by a UMP test only if for any $R_0 < R_1$ the LR given by (28) is a monotonic function of a certain statistics $T = T(Z_n)$, see detailed description of UMP tests in [1,13]. Unfortunately, this is not the case for the LR given by (28) and, hence, the existence of a UMP test is compromised.

5 Local Asymptotic Approach

Let us continue the discussion of the case of random embedding. An efficient solution is based on the asymptotic local approach proposed by L. Le Cam [1,12,11,15]. The idea of this approach is that the "distance" between alternative hypotheses depends on the sample size n in such a way that the two hypotheses get closer to each other when n tends to infinity. By using an asymptotic expansion of the log LR, a particular hypothesis testing problem can be locally reduced to a relatively simple UMP hypothesis testing problem between two Gaussian scalar means [1,11,12,15]. This approach is applied to the following model

$$Z_n \sim Q_R = \prod_{i=1}^{n} R\frac{1}{2}Q_{Q_2}\left(Q_2[z_i]\right) + (1-R)Q_{Q_1}\left(z_i\right). \tag{31}$$

Let us consider two converging sequences of hypotheses $\mathcal{H}_j(n) = \{R \in \mathbb{R}_j(n)\}$ $(j = 0, 1)$. The sets $\mathbb{R}_j(n)$ are of the form $\mathbb{R}_j(n) = r^* + \frac{1}{\sqrt{n}}\delta_r$. If the Fisher information $\mathcal{F}(r)$ for the observation z_i is bounded and positively defined for any $R \in]0;1[$, the log LR

$$\log \Lambda_{r^*}\left(Z_n; \frac{\delta_r}{\sqrt{n}}\right) \stackrel{\text{def.}}{=} \log Q_{r^*+\frac{1}{\sqrt{n}}\delta_r}\left(Z_n\right) - \log Q_{r^*}\left(Z_n\right) \tag{32}$$

possesses the following asymptotic expansion (see details in [1,11,12,15]) :

$$\log\Lambda_{r^*}\left(Z_n; \frac{\delta_r}{\sqrt{n}}\right) \simeq \frac{\delta_r}{\sqrt{n}}\zeta_n(Z_n; r^*) - \frac{\delta_r^2\mathcal{F}(r^*)}{2},\ \zeta_n(Z_n; r^*) = \sum_{i=1}^{n} \left.\frac{\partial \log Q_R(z_i)}{\partial R}\right|_{R=r^*} \tag{33}$$

Moreover, the distribution of the efficient score weakly converges to the normal law

$$\mathcal{L}\left(\frac{1}{\sqrt{n}}\zeta_n(Z_n; r^*)\right) \underset{n\to\infty}{\rightsquigarrow} \begin{cases} \mathcal{N}(0, \mathcal{F}(r^*)) & \text{under } z_i \sim Q_{r^*} \\ \mathcal{N}(\mathcal{F}(r^*)\delta_r, \mathcal{F}(r^*)) & \text{under } z_i \sim Q_{r^*+\frac{\delta_r}{\sqrt{n}}} \end{cases} \tag{34}$$

It can be shown that the efficient score is given by

$$\zeta_n(Z_n; r^*) = \sum_{i=1}^{n} \zeta(z_i; r^*) = \sum_{i=1}^{n} \frac{\Lambda_1(z_i) - 1}{r^*\Lambda_1(z_i) + (1 - r^*)} \tag{35}$$

and the Fisher information $\mathcal{F}(R)$ is

$$\mathcal{F}(R) = \mathbb{E}_R\left[\frac{\Lambda_1(z) - 1}{R\Lambda_1(z) + (1-R)}\right]^2. \tag{36}$$

Therefore, the following decision rule

$$\delta_{r^*}(Z_n) = \begin{cases} \mathcal{H}_0 \text{ if } \zeta_n(Z_n; r^*) < h \\ \mathcal{H}_1 \text{ if } \zeta_n(Z_n; r^*) \geq h \end{cases}. \tag{37}$$

defines a local MP test designed to choose between two alternatives (27). The threshold h is the solution of the equation $\sup_{R \leq r^*} \mathbb{P}_R(\zeta_n(Z_n; r^*) \geq h) = \alpha_0$.

6 Tractable Algorithm and Its Relation with Known Steganalysers

6.1 Tractable Likelihood Ratio

As it follows from the previous sections, in the case of arbitrary embedding rate R, an optimal solution is based on the log LR given by (28) if R_0 and R_1 are known or on the efficient score given by (35) if they are unknown but the value r^* is known. It is easy to see that in both cases the useful information obtained from observations Z_n of cover media (with or without a secret message) is concentrated in $\Lambda_1(z)$ or equivalently in $\log \Lambda_1(z)$. Let us denote $y \stackrel{\text{def.}}{=} \zeta(z; r^*)$, hence

$$y = f(x; r^*) \stackrel{\text{def.}}{=} \frac{e^x - 1}{r^* e^x + 1 - r^*} \quad \text{with} \quad x \stackrel{\text{def.}}{=} \log \Lambda_1(z). \tag{38}$$

This function is represented in Figure 2 for different values of r^*. Typical densities of $x = \log \Lambda_1(z)$ under alternative hypotheses $\mathcal{H}_0$ and $\mathcal{H}_1$ are also shown in Figure 2 for the case of $\sigma = 1.5$. The asymptotic normality of $\zeta_n(Z_n; r^*) = \sum_{i=1}^n \zeta(z_i; r^*)$ is warranted due to Le Cam expansion (see equation (34)). Hence, it is sufficient to compute the expectations and variances of $f(\Lambda_1(z); r^*)$ under alternative hypotheses $\mathcal{H}_0$ and $\mathcal{H}_1$. It follows from (14) that the efficient score for one observation is

$$y = g(\zeta_i, (b_{0,i} - 0.5)) \stackrel{\text{def.}}{=} f(x; r^*) \quad \text{with} \quad x = \frac{\zeta_i (b_{0,i} - 0.5)}{\sigma^2} - \frac{1}{8\sigma^2} \tag{39}$$

under $\mathcal{H}_0$ and, hence, two first moments ($k = 1, 2$) are given by

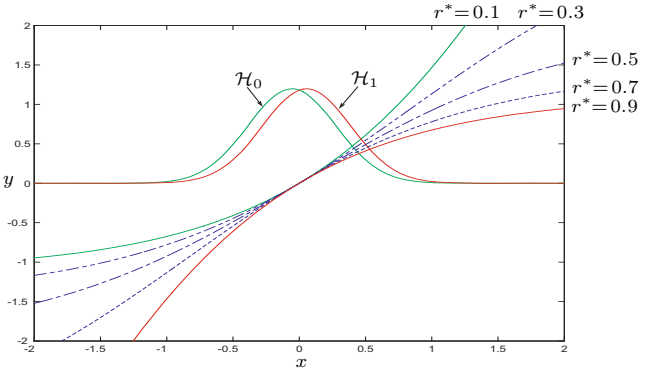

Fig. 2. The efficient score $y = f(x; r^*)$ as a function of $x = \log \Lambda_1(z)$ for $r^* = 0.1, 0.3, 0.5, 0.7, 0.9$

$$\mathbb{E}_0\left[g^k(\zeta_i,(b_{0,i}-0.5))\right]=\sum_{m=-\infty}^{\infty}\left[\Phi\left(\frac{2m+2-\theta}{\sigma}\right)-\Phi\left(\frac{2m+1-\theta}{\sigma}\right)\right]g^k\left(2m+\frac{3}{2}-\theta,\frac{1}{2}\right)$$
$$+\sum_{m=-\infty}^{\infty}\left[\Phi\left(\frac{2m+1-\theta}{\sigma}\right)-\Phi\left(\frac{2m-\theta}{\sigma}\right)\right]g^k\left(2m+\frac{1}{2}-\theta,-\frac{1}{2}\right). \quad (40)$$

It follows from (15) that the efficient score for one observation is

$$y=g(\xi_i,(b_{0,i}-0.5))\overset{\text{def.}}{=}f(x;r^*)\ \text{ with }\ x=\frac{\xi_i(b_{0,i}-0.5)}{\sigma^2}+\frac{1}{8\sigma^2} \quad (41)$$

under $\mathcal{H}_1$ and, hence, two first moments are given by

$$\mathbb{E}_1\left[g^k(\xi_i,(b_{0,i}-0.5))\right]=\frac{1}{2}\mathbb{E}_1\left[g^k(\xi_i,(b_{0,i}-0.5))|b_{0,i}=1\right]+$$
$$\frac{1}{2}\mathbb{E}_1\left[g^k(\xi_i,(b_{0,i}-0.5))|b_{0,i}=0\right]. \quad (42)$$

To compute the loss of optimality of the MP test based on $\log\Lambda_1(Z_n)$ given by (7) and designed for $R=1$ against the local MP test given by (37) with $r^*=0.05$ and the MP test based on $\log\Lambda_{\widetilde{R}}(Z_n)$ when the true embedding rate is $\widetilde{R}=0.1$, let us consider the following Gaussian cover media model : $\theta=129$,

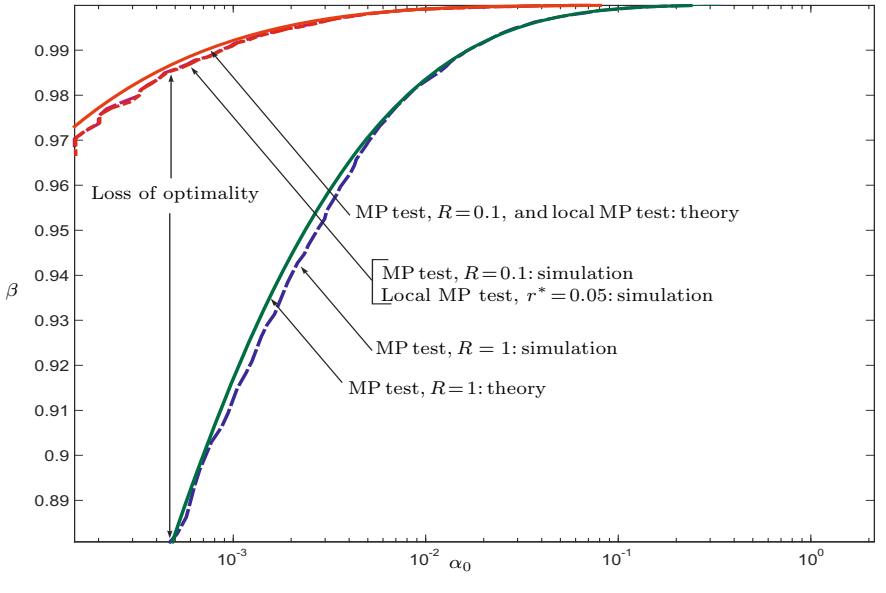

Fig. 3. The power function $\beta=\beta(\alpha_0)$ for the MP tests designed for $R=1$ and $R=0.1$ and for the local MP test designed for $r^*=0.05$: theory and simulation

$\sigma = 1$ and $n = 10^4$. The comparison of the theoretical power $\beta = \beta(\alpha_0)$ as a function of the false alarm rate α_0 for these tests with the Monte Carlo simulation (10^5 repetitions) are presented in Figure 3. These curves reflet the worst case situation, i.e. the augmentation of σ or $\widetilde{R}$ leads to the smaller difference between the above mentioned tests.

6.2 A More Realistic Model of Cover Media

As it follows from equation (24), the power β of an optimal steganalyser depends on the standard deviation σ of cover media pixels for a given rate of false alarm α_0. Hence, to increase the power β, someone has to reduce the standard deviation σ by using a parametric model of cover media. As it is motivated in the companion paper [2], the observation vector (pixels) extracted from the cover media file (digital image, for instance) by using a specially chosen segment or mask is characterized "block by block" by a regression model. Let us split the observation vector C in M statistically independent n dimensional sub-vectors C_j, i.e. $C^T = (C_1^T, \ldots, C_M^T)$. It is assumed that each segment C_j is approximated by :

$$C_j = Q_1[Y_j], \quad Y_j = Hx_j + \xi \sim \mathcal{N}(Hx_j, \sigma_j^2 I_n), \quad j = 1, \ldots, M, \tag{43}$$

where H is a known $[n \times l]$ full rank matrix, $n > l$, $x_j \in \mathbb{R}^l$ is a nuisance parameter (content of the image), I_n is an $(n \times n)$ identity matrix and σ_j^2 is the residual variance. The l columns of H span a column subspace $R(H)$ of the observation space $Y_j \in \mathbb{R}^n$. It is assumed that one column of H is obligatory formed of ones. Such a parametric model is an efficient method to reduce the standard deviation σ [2]. The new hypothesis testing problem with a parametric model of cover media consists in deciding between

$$\mathcal{H}_0 \ : \ Z = C = Q_1[Y], \tag{44}$$

and

$$\mathcal{H}_1 \colon z_i = \begin{cases} Q_2[y_i] + z_{s,i} \text{ with probability } R \\ c_i = Q_1[y_i] \ \text{ with probability } 1-R \end{cases}, \ i = 1, \ldots, Mn, \tag{45}$$

where $Y^T = (Y_1^T, \ldots, Y_M^T)$, $Y_j \sim \mathcal{N}(Hx_j, \sigma_j^2 I_n)$. It follows from the previous subsection that the tractable log LR $\log \Lambda_1(Z_j)$ in the case parametric model can be re-written as follows :

$$\log \Lambda_1(Z_j) = -\frac{1}{2\sigma_j^2} \left\| Q_2[Z_j] - Hx_j + \mathbf{1}_n + \Delta_2 \right\|_2^2 + \frac{1}{2\sigma_j^2} \left\| Z_j - Hx_j + 0.5 \cdot \mathbf{1}_n + \Delta_1 \right\|_2^2, \tag{46}$$

where $\mathbf{1}_n$ is an n-dimensional vector composed of ones, Δ_j is an n-dimensional vector composed of corrective terms due to quantization $\delta_{j,i}$, $j = 1, 2$. The "approximate" log LR is given by

$$\log \Lambda_1(Z_j) \simeq -\frac{1}{2\sigma_j^2} \left\| Q_2[Z_j] - Hx_j + \mathbf{1}_n \right\|_2^2 + \frac{1}{2\sigma_j^2} \left\| Z_j - Hx_j + 0.5 \cdot \mathbf{1}_n \right\|_2^2. \tag{47}$$

In practice, x_j and σ_j^2 are unknown. The theoretical aspects of dealing with nuisance parameters in the framework of statistical decision theory is discussed in [1,13]. An efficient approach to this problem is based on the theory of invariance in statistics. The optimal invariant tests and their properties in the context of image processing have been designed and studied in [4,5,6,16].

Let us first assume that σ_j^2 is known. The nuisance parameter x_j can be estimated (or more exactly rejected) by using $Q_2[Z_j] = Q_2[Y_j]$ which is free from the embedded information. To reject the nuisance parameters, the theory of invariance is usually used in the case non-quantized observations. The detailed description of theoretical and practical aspects (together with all necessary proofs) how to use the invariance principle in the case of regression model can be found in [4,5,6,16]. The idea of the invariant hypotheses testing approach is based on the existence of the natural invariance of the detection problem with respect to a certain group of transformation. Let us note that the above mentioned hypotheses testing problem given by (44) - (45) remains "almost" invariant under the group of translations $G = \{g : g(Y) = Y + Hx\}$, $x \in \mathbb{R}^l$. The word "almost" is due to the quantization $Q_j[y]$, $j = 1, 2$. Without the quantization, the invariance will be exact. In such a case, the statistical decision should be based on a maximal invariant to the group of translations G, i.e. all invariant tests with respect to G are functions of a maximal invariant statistics (see the definition in [3]). It is shown that the projection $\varepsilon = W^T Y$ of Y onto the left null space $R(H)^{\perp}$ of the matrix H is a maximal invariant. The matrix $W = (w_1, \ldots, w_{n-l})$ of size $n \times (n - l)$ is composed of eigenvectors $w_1, \ldots, w_{n-l}$ of the projection matrix $P_H^{\perp} = I_n - H(H^T H)^{-1} H^T$ corresponding to eigenvalue 1. The matrix W satisfies the following conditions: $W^T H = 0$, $WW^T = P_H^{\perp}$ and $W^T W = I_{n-l}$. In practice, the nuisance parameter rejection is usually done by using the matrix $P_H^{\perp}$, because $P_H^{\perp} H = 0$. Moreover, if the matrix H is full rank, then the invariant test is equivalent to the generalized LR (or GLR) test. The "approximate" log GLR (or "almost" invariant) is given by

$$\begin{aligned} \log \widehat{\Lambda}_1(Z_j) &\simeq -\frac{1}{2\sigma_j^2} \left\| Q_2[Z_j] - H\widehat{x} + \mathbf{1}_n \right\|_2^2 + \frac{1}{2\sigma_j^2} \left\| Z_j - H\widehat{x} + 0.5 \cdot \mathbf{1}_n \right\|_2^2 \\ &= \frac{1}{\sigma_j^2} \left[P_H^{\perp} Q_2[Z_j] \right]^T [B_0 - 0.5 \cdot \mathbf{1}_n] + \frac{n}{8\sigma_j^2}, \end{aligned} \tag{48}$$

where $B_0 = (b_{0,1}, \ldots, b_{0,n})^T$ and $\widehat{x} = (H^T H)^{-1} H^T Q_2[Z_j]$ is the ML estimate of the nuisance parameter x.

Under hypothesis $\mathcal{H}_0$, the expectation and variance of the "approximate" log GLR for the total observation vector Y are given by the following expressions :

$$m_0 = \mathbb{E}_0 \left[\sum_{j=1}^{M} \log \widehat{\Lambda}_1(Z_j) \right] \simeq \frac{M(2l - n)}{8\overline{\sigma}^2} \quad \text{with} \quad \frac{1}{\overline{\sigma}^2} = \frac{1}{M} \sum_{j=1}^{M} \frac{1}{\sigma_j^2} \tag{49}$$

and

$$\sigma_0^2 = \mathrm{Var}_0\left[\sum_{j=1}^{M}\log\widehat{\Lambda}_1(Z_j)\right] \simeq M(n-l)\left[\frac{1}{4\overline{\sigma}^2}+\frac{1}{16\overline{\sigma}^4}\right] \text{ with } \frac{1}{\overline{\sigma}^4}=\frac{1}{M}\sum_{j=1}^{M}\frac{1}{\sigma_j^4}. \quad (50)$$

Let us assume that the true embedding rate takes an arbitrary value $\widetilde{R}$: $0 < \widetilde{R} \leq 1$. Under hypothesis $\mathcal{H}_1$ with the true embedding rate $\widetilde{R}$, the expectation and variance of the "approximate" log GLR for the total observation vector Y are given by the following expressions :

$$m_{\widetilde{R}} = \mathbb{E}_{\widetilde{R}}\left[\sum_{j=1}^{M}\log\widehat{\Lambda}_1(Z_j)\right] \simeq \frac{M(2l-n+2\widetilde{R}(n-l))}{8\overline{\sigma}^2} \quad (51)$$

and

$$\sigma_{\widetilde{R}}^2 = \mathrm{Var}_{\widetilde{R}}\left[\sum_{j=1}^{M}\log\widehat{\Lambda}_1(Z_j)\right] \simeq \frac{M(n-l)}{4\overline{\sigma}^2} + \frac{M(n-l)(1-R)^2}{16\overline{\sigma}^4} \quad (52)$$

Proposition 2. *Let us assume that the Lindeberg's condition imposed on the log LR* $\log\widehat{\Lambda}_1(Z_j)$ *is satisfied. It follows from the central limit theorem that the following fraction*

$$\frac{\sum_{j=1}^{M}\log\widehat{\Lambda}_1(Z_j) - \mathbb{E}_{\widetilde{R}}\left[\sum_{j=1}^{M}\log\widehat{\Lambda}_1(Z_j)\right]}{\sqrt{\mathrm{Var}_{\widetilde{R}}\left[\sum_{j=1}^{M}\log\widehat{\Lambda}_1(Z_j)\right]}} \underset{M\to\infty}{\rightsquigarrow} \mathcal{N}(0,1) \quad (53)$$

weakly converges to the standard normal distribution [17]. For large M*, the power* β_{δ_1} *of the test (7) with the log LR* $\sum_{j=1}^{M}\log\widehat{\Lambda}_1(Z_j)$ *given by (48) can be approximated*

$$\beta_{\delta_1} \simeq 1 - \Phi\left(\Phi^{-1}(1-\alpha_0)\frac{\sigma_0}{\sigma_{\widetilde{R}}} - \frac{(m_{\widetilde{R}}-m_0)}{\sigma_{\widetilde{R}}}\right) \quad (54)$$

where m_0*,* $m_{\widetilde{R}}$*,* σ_0 *and* $\sigma_{\widetilde{R}}$ *are calculated by using equations (49) - (52).*

If the residual variance σ_j^2 is unknown, then the following GLR is used

$$\log\widehat{\Lambda}_1(Z_j) \simeq \frac{1}{\widehat{\sigma}_j^2}\left[P_H^{\perp}Q_2[Z_j]\right]^T\left[B_0 - 0.5\cdot\mathbf{1}_n\right] + \frac{n}{8\widehat{\sigma}_j^2}, \quad (55)$$

where $\widehat{\sigma}_j^2 = \frac{1}{n-l}\left\|P_H^{\perp}Q_2[Z_j]\right\|_2^2$.

The first right hand side term in equation (48) defines the sensitivity of the test because the second right hand side term $\frac{n}{8\widehat{\sigma}^2}$ does not depend on the embedded secret message. Nevertheless, the second right hand side term $\frac{n}{8\widehat{\sigma}^2}$ of (48) is also necessary to correctly calculate the threshold h in (7) by using the equation

$\mathbb{P}_0(\sum_{j=1}^{M} \log \widehat{\Lambda}_1(Z_j) \geq h) = \alpha_0$. The first right hand side term in equation (48) represents an inner product of the vector of "residuals" $\varepsilon = P_H^{\perp} Q_2[Z_j]$, i.e. the vector of projection of $Q_2[Z_j]$ on the orthogonal complement $R(H)^{\perp}$ of the column space $R(H)$, and the vector $[B_0 - 0.5 \cdot \mathbf{1}_n]$ composed of $\mathrm{LSB}(z_i) - 0.5$:

$$\frac{1}{\widehat{\sigma}^2}\left[P_H^{\perp} Q_2[Z_j]\right]^T [B_0 - 0.5 \cdot \mathbf{1}_n] = \sum_{i=1}^{n} \overbrace{\widehat{\sigma}^{-2}}^{=\text{"weight"}} \cdot \overbrace{(Q_2[z_i] - (H\widehat{x}_j)_i + 1)}^{=\text{"residual" } \varepsilon_i} \cdot \overbrace{(b_{0,i} - 0.5)}^{=\mathrm{LSB}(z_i)-0.5}, \quad (56)$$

where $(H\widehat{x}_j)_i$ is the i-th row of the vector $H\widehat{x}_j$. Let us now compare the last equation with the recently developed steganalysers [7,8,9]. These steganalysers are based on the following statistics [9] :

$$\sum_{i=1}^{n} \overbrace{w_i}^{=\text{"weight"}} \cdot \overbrace{(z_i - \mathcal{F}(z)_i)}^{=\text{"residual" } \varepsilon_i} \cdot \overbrace{(z_i - \overline{z}_i)}^{=2\cdot(\mathrm{LSB}(z_i)-0.5)}, \quad (57)$$

where $\mathcal{F}(s)$ denotes a "filter" dedicated to estimate the cover-image by filtering the stego-image, the weight w_i is chosen as $\frac{1}{1+\sigma_i^2}$, σ_i^2 is the "local" variance and $\overline{z}_i$ denotes the nonnegative integer z_i with the LSB flipped. As it follows from equations (56) - (57), the steganalysers developed in [7,8,9] coincide with the first term of the tractable log GLR (48).

7 Conclusions

The problem of hidden information detection has been addressed from a statistical point of view. Two new phenomena have been studied : *i)* the impact of observation quantization on the probabilities of false alarm and non detection; *ii)* the benefits from using a parametric statistical model of cover media. Some (almost) optimal statistical solutions have been designed and studied to solve the problem of hidden information detection. These solutions have been theoretically compared with the WS steganalysers algorithm recently developed [7,8,9]. Based on these theoretical findings, an efficient parametric model and hidden information detection algorithms have been developed and tested in the companion paper [2].

References

1. Borovkov, A.A.: Mathematical Statistics. Gordon and Breach Sciences Publishers, Amsterdam (1998)
2. Cogranne, R., Zitzmann, C., Fillatre, L., Retraint, F., Nikiforov, I., Cornu, P.: A cover image model for reliable steganalysis. In: Filler, T., et al. (eds.) IH 2011. LNCS, vol. 6958, pp. 178–192. Springer, Heidelberg (2011)
3. Ferguson, T.: Mathematical Statistics: A Decision Theoretic Approach. Academic Press, London (1967)

4. Fillatre, L., Nikiforov, I.: A statistical detection of an anomaly from a few noisy tomographic projections. Journal of Applied Signal Processing, Special issue on Advances in Intelligent Vision Systems: Methods and Applications-Part II 14, 2215–2228 (2005)
5. Fillatre, L., Nikiforov, I.: Non-bayesian detection and detectability of anomalies from a few noisy tomographic projections. IEEE Trans. Signal Processing 55(2), 401–413 (2007)
6. Fillatre, L., Nikiforov, I., Retraint, F.: ε-optimal non-bayesian anomaly detection for parametric tomography. IEEE Transactions on Image Processing 17(11), 1985–1999 (2008)
7. Fridrich, J., Goljan, M.: On estimation of secret message length in LSB steganography in spatial domain. In: Proc. of SPIE, pp. 23–34. Addison-Wesley, Reading (2004)
8. Ker, A.D.: Locating steganographic payload via WS residuals. In: Proceedings of the 10th ACM Workshop on Multimedia and Security, Oxford, September 22-23, pp. 27–31 (2008)
9. Ker, A.D., Böhme, R.: Revisiting weighted stego-image steganalysis. In: Delp, E.J., Wong, P.W. (eds.) Proceedings SPIE, Electronic Imaging, Security, Forensics, Steganography, and Watermarking of Multimedia Contents X, San Jose, CA, January 27-31, vol. 6819, pp. 51 – 517 (2008)
10. Ker, A.D., Pevný, T., Kodovský, J., Fridrich, J.: The square root law of steganographic capacity. In: MM&Sec 2008: Proceedings of the 10th ACM Workshop on Multimedia and Security, pp. 107–116. ACM, New York (2008), http://doi.acm.org/10.1145/1411328.1411349
11. Le Cam, L.: Asymptotic Methods in Statistical Decision Theory. Series in Statistics. Springer, New York (1986)
12. Le Cam, L., Yang, G.L.: Asymptotics in Statistics. Springer, Heidelberg (1990)
13. Lehmann, E.: Testing Statistical Hypotheses, 2nd edn. Chapman & Hall, Boca Raton (1986)
14. Dabeer, O., Sullivan, K., Madhow, U., Chandrasekaran, S.: Detection of hiding in the least significant bit. IEEE Trans. Signal Processing 52(10), 3047–3058 (2004)
15. Roussas, G.G.: Contiguity of Probability Measures, Some Applications in Statistics. Cambridge University Press, Mass (1972)
16. Scharf, L., Friedlander, B.: Matched subspace detectors. IEEE Trans. Signal Processing 42(8), 2146–2157 (1994)
17. Shiryaev, A.N.: Probability, 2nd edn. Springer, New York (1996)