Available online at www.sciencedirect.com

ScienceDirect

Digital Signal Processing 00 (2013) 1–20

Digital Signal Processing

Hidden Information Detection using Decision Theory and Quantized samples: Methodology, Difficulties and Results☆

Rémi Cogranne[a*], Florent Retraint[a], Cathel Zitzmann[a], Igor Nikiforov[a], Lionel Fillatre[b] and Philippe Cornu [a**]

[a] *ICD, LM2S, Université de Technologie de Troyes, UMR STMR CNRS, 12, rue Marie Curie, CS 42060, 10004 Troyes cedex, France*
[b] *Université de Nice Sophia-Antipolis, Laboratoire d'Informatique, Signaux et Systèmes de Sophia-Atipolis, 06900 Sophia Antipolis, France*

© 2013 Elsevier B.V. All rights reserved. Accepted version provided for non-commercial research and education use.
Final version published in Digital signal processing, Vol. 24, pp. 144 – 161, January 2014, is available at doi: 10.1016/j.dsp.2013.09.012.
This article appeared in a journal published by Elsevier. The attached copy is furnished to the author for internal non-commercial research and education use, including for instruction at the authors institution and sharing with colleagues. Other uses, including reproduction and distribution, or selling or licensing copies, or posting to personal, institutional or third party websites are prohibited.

Abstract

This paper studies the detection of Least Significant Bits (LSB) steganography in digital media by using hypothesis testing theory. The main goal is threefold: first, it is aimed to design a test whose statistical properties are known, this especially allows the guaranteeing of a false alarm probability. Second, the quantization of samples is studied throughout this paper. Lastly, the use of a linear parametric model of samples is used to estimate unknown parameters and design a test which can be used when no information on cover medium is available. To this end, the steganalysis problem is cast within the framework of hypothesis testing theory and digital media are considered as quantized signals. In a theoretical context where media parameters are assumed to be known, the Likelihood Ratio Test (LRT) is presented. Its statistical performances are analytically established; this highlights the impact of quantization on the most powerful steganalyzer. In a practical situation, when image parameters are unknown, a Generalized LRT (GLRT) is proposed based on a local linear parametric model of samples. The use of such model allows us to establish GLRT statistical properties in order to guarantee a prescribed false-alarm probability. Focusing on digital images, it is shown that the well-known WS (Weighted-Stego) is close to the proposed GLRT using a specific model of cover image. Finally, numerical results on natural images show the relevance of theoretical findings.

Keywords: Hypothesis testing theory, LSB steganalysis, Quantized data, Optimal steganalysis, Nuisance parameters.

1. Introduction

Information hiding concerns the transmission of a secret message buried in a host digital medium. It has recently received increasing interest driven by the large number of ensuing application such as watermark-based authentication and fingerprint tracing. Unfortunately, potential malicious uses, among which steganography, have also emerged. The "prisoners problem" [43] illustrates a typical scenario of steganography and steganalysis. Alice and Bob, two prisoners, communicate by embedding a secret binary message $\boldsymbol{M}$ into a cover-object $\boldsymbol{C}$ to obtain a stego-object $\boldsymbol{S}$ which is then sent through a public channel. Wendy, the warden, examines all their communications and tries to detect whether an inspected object $\mathbf{Z}$, either a cover object $\boldsymbol{C}$ or a stego-object $\boldsymbol{S}$, contains a secret message $\boldsymbol{M}$ without being able to extract $\boldsymbol{M}$.
With many tools available in the public domain, steganography

☆© 2013 Elsevier B.V. All rights reserved. Accepted version provided for non-commercial research and education use.
Final version published in Digital signal processing, Vol. 24, pp. 144 – 161, January 2014, is available at doi: 10.1016/j.dsp.2013.09.012.
This article appeared in a journal published by Elsevier. The attached copy is furnished to the author for internal non-commercial research and education use, including for instruction at the authors institution and sharing with colleagues. Other uses, including reproduction and distribution, or selling or licensing copies, or posting to personal, institutional or third party websites are prohibited.

*Corresponding author.

**With the financial support from the Prevention of and Fight against Crime Programme of the European Union European Commission - Directorate-General Home Affairs (2centre.eu project). Research funded, in part, by Troyes University of Technology (UTT) strategic program COLUMBO and by National Agency for Research (ANR) program (Project ANR-07-SECU-004).

Email address: `remi.cogranne@utt.fr` (Rémi Cogranne[a])
URL: `http://lm2s.utt.fr/fr/membres/cogrannr.html` (Rémi Cogranne[a])

is within the reach of anyone, for legitimate or malicious purpose; it is thus of a crucial interest to be able to efficiently detect steganographic content among a (possibly huge) set of media.

1.1. Reliable Detection of Hidden Bits as a Main Motivation

Many methods have recently been proposed to detect steganographic content [4, 12, 37] among which some are very efficient (see results of BOSS contest [2] for example). These methods can be roughly divided into four categories:

1. Only a few detectors rely on the hypothesis testing theory [7, 9, 13, 16, 32, 48]. The performance of these detectors can be expressed analytically which allows the guaranteeing of a prescribed detection-error probability. Unfortunately, these tests lack an accurate cover medium model and therefore exhibit rather poor performances.
2. Many detectors belong to the class of *structural detectors* [26] which aims at detecting specific modifications of bit replacement using local pixels' correlation. The Regular-Singular (RS) [21] the Sample Pair Analysis (SPA) [14, 34] and the triple/quadruple detectors [27] are, for instance, good representatives of this category. These methods usually achieve overall good performances but lack a statistical model of cover media which prevents the analytic calculation of detection performance.
3. The Weighted Stego-image (WS) analysis, initially proposed in [20] to estimate the payload size and deeply studied in [28, 29], forms a class apart which is known to have good detection performance. Similarly to the structural detectors, the WS detectors rely on a local autoregressive model of media. However, the statistical properties of WS algorithms remain unknown; therefore, probabilities of detection errors can only be measured empirically.
4. Lastly, *universal* or *blind* detectors aims at detecting any steganographic scheme in any kind of image using a set of selected features and supervised learning methods to train a classifier. As in all applications of supervised learning, a difficult problem is to choose an appropriate feature set which, for detection of hidden information, is usually done empirically. Moreover, the problem of measuring classification error probabilities remains open in the framework of statistical learning [41].

In certain operational context, for example a steganalysis tool for the law enforcement agencies, a good detection performance might not suffice. To avoid false alarm, the detector should be provided with an analytically predictable error probability in order to guarantee the respect of a prescribed false-alarm probability. In fact, among the four previously described categories of steganalyzers, only detectors based on decision theory can be statistically studied.

However, the application of hypothesis testing theory is not straightforward because of some fundamental difficulties. Firstly, the cover medium is quantized which prevents a direct application of classical hypothesis tests. Secondly, a digital medium exhibits a complex and structured content which acts as nuisance parameters as it has no interest for hidden information detection. Thirdly, no assumption on the size of hidden data (or more precisely on the relative payload) is available to the steganalyst, the tested hypothesis are thus composite.

In the present work the embedding scheme is assumed to belong to the commonly used family of LSB replacement scheme. Actually, as of December 2011, WetStone Technologies Inc. has 836 data hiding software among which 582 (70%) uses LSB replacement [22]. In addition, detection of mostly encountered algorithms is more important than the detection on seldom found ones. Thus, requirement of efficient and robust detection methods for the LSB replacement steganographic scheme is still a live research topic.

1.2. Contributions of this Paper

The first step in the application of hypothesis testing theory for steganalysis has been done in [13] in 2004 using a simplistic model of independent and identically distributed (i.i.d) samples. This methodology was latter proposed in [8, 9] in 2011 to design an efficient test using a complex model of cover medium. During the same year, a theoretical approach was also used in [10, 50] to design locally most powerful test (around a given hidden message length) which is difficult to apply in practice.

The fundamental originalities of the proposed article are that the content of cover medium as well as the impact of quantization are considered. In fact, it is necessary to take into account these two phenomena to apply hypothesis testing theory and to precisely establish the performance of proposed statistical tests.

To highlight the contributions of the presented methodology, let us first denote that the detection performance of steganalyzers is usually measured using a fixed hidden data length with a receiver operating characteristic (ROC) curve [15]. However, it is known that in practice, detection results do not only depend on relative payload or embedding rate. For instance, it has been shown that results depend on inspected medium content [5] and hidden data length [38]; the phenomena referred to as "camera mismatch" was also observed during BOSS contest [2]. Likewise, the detection performance of proposed detectors is not compared with an optimal bound or with the most powerful test.

In fact, the relation between cover medium properties and detection performance remains unclear for most of steganalyzers and optimal detection performance has only been established under the dubious condition of neglected quantization.

On the opposite, this paper proposes a novel methodology to detect information hidden in the LSB of a digital medium using hypothesis testing theory. The main contribution is threefold:

1. Throughout this paper, the quantization of pixels is thoroughly studied in order to measure its impact on hidden information detection. It is especially shown that data quantization and hidden information in the LSB plane heavily impact on the test performance.
2. In the ideal context when medium content is known, the statistical performance of the Likelihood Ratio Test (LRT) is then analytically established. This result provides an

optimal upper-bound on the power function one can expect from any detector. Moreover, it is shown that detection performance depends on an "Insertion-to-Noise Ratio" (INR) which allows us to understand how some of cover medium properties impact the performance of the LRT.

3. Finally, when the structured content of inspected medium is unknown —that is the expectation and the variance of each sample— this nuisance parameter is explicitly taken into account using a linear parametric model. Based on this model of cover content, a sub-optimal Generalised Likelihood Ratio Test (GLRT) is proposed and its statistical properties are analytically given to guarantee, in practice, a prescribed false-alarm constraint.

The relevance of theoretical findings are emphasized through numerical experimentations on simulated data and on large databases of natural images.

1.3. Organization of the Paper

The paper is organized as follows. Section 2 formally states the problem of steganalysis paying a careful attention to further difficulties. Then, Section 3 details the design of the LRT and the calculation of its performances in the ideal case when the cover medium parameters are assumed to be known. The more realistic case non-i.i.d samples is studied in Section 4. Section 5 investigates the practical case when no information about cover medium is available. First, the linear parametric model used to estimated unknown parameters of inspected medium is presented. Then, the design of the GLRT is detailed together with the calculation of its statistical properties. Numerical results and comparisons with prior art steganography detectors are presented in Section 6. Finally, Section 7 concludes the paper.

2. Problem Statement and Difficulties

Let the vector $\boldsymbol{C} = \{c_n\}_{n=1}^N$ represents a digital cover medium of N samples. Each sample is usually quantized with b bits, hence $\boldsymbol{C} \in \mathcal{Z}^N$ with $\mathcal{Z} = \{0, 1, \ldots, 2^b - 1\}$. The value of a cover sample c_n is given by:

$$c_n = Q_\Delta(y_n), \tag{1}$$

where $y_n \in \mathbb{R}$ denotes the recorded sample value and $Q_\Delta(y_n)$ is the operation of uniform quantization with step Δ defined, for all $k \in \mathcal{Z}, k \neq 0, k \neq 2^q - 1$, by:

$$Q_\Delta(x) = k \Leftrightarrow x \in \Big[\Delta\,(k - 1/2)\,;\Delta\,(k + 1/2)\Big[. \tag{2}$$

For clarity, effects of quantizer saturation, which arise for $k = 0$ and $k = 2^b - 1$, are neglected in this paper; note that it can be taken into account at the cost of complicated calculations [45]. The recorded sample value y_n can be written as [19, 24]

$$y_n = \theta_n + \xi_n, \tag{3}$$

where θ_n is the mathematical expectation of y_n and ξ_n is the realization of a zero-mean random variable representing all the noises corrupting the signal during acquisition. For definition, it is assumed in this paper that the mean vector $\boldsymbol{\theta} = \{\theta_n\}_{n=1}^N$ belongs to a compact set Θ.
Let probability mass function (pmf) of the quantized sample c_n be denoted:

$$P_{\theta_n} = \{p_{\theta_n}[0], \cdots, p_{\theta_n}[2^b - 1]\}. \tag{4}$$

To model statistically the modification due to insertion of secret message $\boldsymbol{M}$, let the payload $0 < R \leq 1$ be defined as the number of hidden bits per cover medium sample[1]. After insertion of the hidden message $\boldsymbol{M}$, a sample s_n from the stego-medium $\boldsymbol{S} = \{s_n\}_{n=1}^N$ is characterized by the pmf denoted

$$Q_{\theta_n}^R = \{q_{\theta_n}^R[0], \cdots, q_{\theta_n}^R[2^b - 1]\}, \tag{5}$$

which, of course, depends on the embedding scheme.
The LSB replacement method consists in inserting message bits $\boldsymbol{M}$ by substituting samples' LSB. This embedding scheme can be modeled statistically thanks to the two following assumptions commonly used in steganalysis [13, 21]:

A-1 Because the message is previously compressed and/or cyphered, each hidden bits of message $\boldsymbol{M}$ (0 or 1) is drawn from a binomial distribution $\mathcal{B}(1, 1/2)$.

A-2 The insertion locations in the cover-object are chosen pseudo-randomly using a secret key, hence, each cover pixel c_n are used with the same probability (referred as "*mutually independent embedding*" in [18]).

This situation is captured by introducing a random variable T_n which represents the impact of the bit hidden in the n-th sample [13]:

$$\mathbb{P}[T_n{=}\varnothing] = (1{-}R),$$
$$\mathbb{P}[T_n{=}0] = \mathbb{P}[T_n{=}1] = \tfrac{R}{2},$$

which is interpreted as follows: the n-th sample c_n is not used when $T_n{=}\varnothing$ which occurs with a probability $1 - R$ and is used to hide a bit $T_n = \{0; 1\}$ with the same probability $R/2$. Hence, a short calculation [13] shows that $Q_{\theta_n}^R$, the pmf of the stego-medium sample s_n, is given for all $k \in \mathcal{Z}$ by:

$$\begin{aligned} q_{\theta_n}^R[k] &= (1{-}R)\,p_{\theta_n}[k] + \frac{R}{2}(p_{\theta_n}[k] + p_{\theta_n}[\bar{k}]) \\ &= \left(1{-}\frac{R}{2}\right)p_{\theta_n}[k] + \frac{R}{2}p_{\theta_n}[\bar{k}], \end{aligned} \tag{6}$$

where $\bar{k}$ indicates the integer k whose LSB is flipped [4, 20], i.e., $\bar{k} = k + (-1)^k = k + 1 - 2\,\mathrm{lsb}(k)$.

[1]For clarity, the relative payload or embedding rate R is not distinguished from the actual change-rate in the present paper. However, those two notions are different for steganographic scheme which does not embed one bit per change, using error correcting codes for instance [36].

When inspecting a digital medium $\mathbf{Z}$ in order to detect hidden information, the problem one wich to solve is to decide between the two following hypotheses:

$$\begin{cases}\mathcal{H}_0 = \{z_n \sim P_{\theta_n}, \forall n \in \{0,\dots,N\}\} \\ \mathcal{H}_1 = \{z_n \sim Q^R_{\theta_n}, \forall n \in \{0,\dots,N\}, \forall R \geq 0\}\end{cases} \tag{7}$$

The goal is to find a test $\delta : \mathcal{Z}^N \to \{\mathcal{H}_0; \mathcal{H}_1\}$ such that hypothesis $\mathcal{H}_i$ is accepted if $\delta(\mathbf{Z}) = \mathcal{H}_i$ (see [33] for details about statistical hypothesis testing). Let

$$\mathcal{K}_{\alpha_0} = \left\{\delta : \sup_{\boldsymbol{\theta}\in\Theta} \mathbb{P}_{\mathcal{H}_0}\left[\delta(\mathbf{Z}) = \mathcal{H}_1\right] \leq \alpha\right\} \tag{8}$$

be the class of all tests whose false alarm probability is upper-bounded by α_0; here $\mathbb{P}_{\mathcal{H}_0}[\cdot]$ stands for conditional probability under the null hypothesis $\mathcal{H}_0$. The power function $\beta_{\delta,R}$ of a test δ is the probability of hidden bits detection defined by:

$$\beta_{\delta,R} = \mathbb{P}_{\mathcal{H}_1,R}\left[\delta(\mathbf{Z}) = \mathcal{H}_1\right]$$

with $\mathbb{P}_{\mathcal{H}_1,R}[\cdot]$ the conditional probability under alternative hypothesis $\mathcal{H}_1$: a secret message was hidden with relative payload R. Obviously, it is aimed at finding a test in the class $\mathcal{K}_{\alpha_0}$ (to meet a prescribed false-alarm probability constraint α_0) which maximizes the power function $\beta_{\delta,R}$, if possible, uniformly with respect to the relative payload R.

The hypothesis testing problem as formulated in (7) highlights three major difficulties of the hidden information detection problem. First, when data are quantized most of the usual results from decision theory are no longer valid. Second, because the relative payload R is unknown the hypothesis $\mathcal{H}_{1,R}$ is composite. Last, the mean vector $\boldsymbol{\theta}$, representing the structured content of inspected digital medium, acts as a nuisance parameter for which an accurate estimation is an open problem of signal and image processing.

The problem of dealing with quantized observations and composite hypotheses are addressed in Section 3-4 while the problem of dealing with the nuisance parameter $\boldsymbol{\theta}$ is addressed in Section 5.

3. Steganalysis as a Composite Statistical Test with Quantized Observation

Let us suppose that the relative payload R as well as the pmf P_{θ_n} and $Q^R_{\theta_n}$, see (4) - (5), are known by the steganalyst. In this case the tested hypotheses (7) are simple and from the relation (6) the Likelihood Ratio (LR) is given, for the observation z_n, by:

$$\Lambda_R(z_n) = \frac{q^R_{\theta_n}[z_n]}{p_{\theta_n}[z_n]} = (1-R) + R\ \underbrace{\frac{p_{\theta_n}[z_n] + p_{\theta_n}[\overline{z}_n]}{2\,p_{\theta_n}[z_n]}}_{\Lambda_1(z_n)}. \tag{9}$$

It follows from the Neyman-Pearson Lemma [33, theorem 3.2.1] that the most powerful test δ^{np} over the class $\mathcal{K}_{\alpha_0}$ is the LRT defined by the following decision function:

$$\delta^{np}_R = \begin{cases}\mathcal{H}_0 \text{ if } \ln\Lambda_R(\mathbf{Z}) = \sum_{n=1}^{N} \ln\Lambda_R(z_n) < \tau_{\alpha_0} \\ \mathcal{H}_1 \text{ if } \ln\Lambda_R(\mathbf{Z}) = \sum_{n=1}^{N} \ln\Lambda_R(z_n) \geq \tau_{\alpha_0},\end{cases} \tag{10}$$

where the decision threshold is the solution of the equation

$$\mathbb{P}_{\mathcal{H}_0}\left[\Lambda_R(\mathbf{Z}) \geq \tau_{\alpha_0}\right] = \alpha_0,$$

such that $\delta^{np}_R \in \mathcal{K}_{\alpha_0}$.

The Equation (10) clearly shows that the test δ^{np}_R only depends on the observations $\mathbf{Z}$ through the quantity Λ_1, which corresponds to the LR ns the case of a payload $R = 1$. It is thus proposed to study this LR Λ_1 in order to get the statistical properties of the test δ^{np}_R whatever the relative payload R might be.

3.1. Expression of the LR for $R = 1$

For most of the digital media, the ξ_n's, representing noise values see (3), are well approximated as realization of independent Gaussian random variables Ξ_n satisfying $\Xi_n \sim \mathcal{N}(0, \sigma_n^2)$. This model of noise is quite general and can potentially be applied for a wide range of digital media. Focusing on digital images, which is the most widely used type of media in both steganography and steganalysis, the noise variance σ_n^2 varies from pixel to pixel due to the signal-dependent noise discussed in [19, 24]. It follows from (1) and (3) that $p_{\theta_n}[k]$ is defined, for all $k \in \mathcal{Z}, k \neq 0, k \neq 2^q - 1$, by:

$$\begin{aligned} p_{\theta_n}[k] &= \frac{1}{\sigma_n}\int_{\Delta(k-1/2)}^{\Delta(k+1/2)} \varphi\left(\frac{x-\theta_n}{\sigma_n}\right)dx \\ &= \Phi\left(\frac{\Delta(k+\frac{1}{2})-\theta}{\sigma_n}\right) - \Phi\left(\frac{\Delta(k-\frac{1}{2})-\theta}{\sigma_n}\right), \end{aligned} \tag{11}$$

where $\varphi(\cdot)$ and $\Phi(\cdot)$ are respectively the standard Gaussian probability density function (pdf) and cumulative distribution function (cdf) defined by:

$$\varphi(x) = \frac{1}{\sqrt{2\pi}}\exp\left(-\frac{x^2}{2}\right) \text{ and } \Phi(x) = \int_{-\infty}^{u}\varphi(u)du. \tag{12}$$

As already explained for the Equation (2), effects of quantizer saturation are omitted from relation (12) for clarity.

Using the well-known Taylor series expansion of the function φ [47, p.931] around the value Δk, the midpoint of quantization step, see (2), a short calculation shows that:

$$p_{\theta_n}[k] = \frac{\Delta}{\sigma_n}\varphi\left(\frac{\Delta k-\theta_n}{\sigma_n}\right)(1+\varepsilon_{\theta_n}[k]), \tag{13}$$

where the analytic expression of the corrective term $\varepsilon_{\theta_n}[k]$ is:

$$\varepsilon_{\theta_n}[k] = \sum_{i=1}^{\infty}(-1)^i\frac{2}{2^{2i}(2i+1)!}\frac{\Delta^{2i}}{\sigma_n^{2i}}H_{2i}\left(\frac{\Delta k-\theta}{\sigma}\right). \tag{14}$$

with H_i the Hermite polynomial of order i [47, p.1350].

Let $k^{(0)} = \min\{k; \overline{k}\} = \frac{1}{2}(\overline{k} + k - 1)$ represents the integer k whose LSB is set to 0. The term $p_{\theta_n}[k] + p_{\theta_n}[\overline{k}]$ represents the

probability that z_n belongs to the interval $[\Delta(k^{(0)} - 1/2); \Delta(k^{(0)} + 3/2)[$ and can thus be expressed as the following integral:

$$p_{\theta_n}[k] + p_{\theta_n}[\bar{k}] = \frac{1}{\sigma_n} \int_{\Delta(k^{(0)}-1/2)}^{\Delta(k^{(0)}+3/2)} \varphi\left(\frac{x-\theta_n}{\sigma_n}\right) dx.$$

Similarly to the Equation (13), a short calculation using the Taylor series expansion of the function φ around the value $\Delta(k^{(0)} + 1/2)$, permits the writing of:

$$p_{\theta_n}[k]+p_{\theta_n}[\bar{k}] = \frac{2\Delta}{\sigma_n}\varphi\Big(\frac{\Delta(k^{(0)}+\frac{1}{2})-\theta_n}{\sigma_n}\Big)(1+\varepsilon^{(0)}_{\theta_n}[k]), \tag{15}$$

where the corrective term $\varepsilon^{(0)}_{\theta_n}[k]$ is given as:

$$\varepsilon^{(0)}_{\theta_n}[k] = \sum_{i=1}^{\infty}(-1)^i \frac{2}{2^{2i}(2i+1)!}\frac{\Delta^{2i}}{\sigma_n^{2i}} H_{2i}\Big(\frac{\Delta(k^{(0)}+\frac{1}{2})-\theta}{\sigma}\Big). \tag{16}$$

Using the expression (13) and (15), it is straightforward to write the logarithm of LR $\Lambda_1(z_n)$ (9) as follows:

$$\begin{aligned}\ln(\Lambda_1(z_n)) &= \frac{1}{2\sigma_n^2}\Big((\Delta z_n-\theta_n)^2-(\Delta(z_n^{(0)}+\tfrac{1}{2})-\theta_n)^2\Big) \\ &\quad + \ln(1+\varepsilon_{\theta_n}(z_n)) - \ln(1+\varepsilon^{(0)}_{\theta_n}(z_n^{(0)})).\end{aligned} \tag{17}$$

where $z_n^{(0)} = \min\{z_n; \bar{z}_n\} = \frac{1}{2}(\bar{z}_n + z_n - 1)$, as previously defined. Due to corrective terms $\varepsilon_{\theta_n}[k]$ and $\varepsilon^{(0)}_{\theta_n}[k]$, the exact expression of the LR $\ln(\Lambda_1(z_n))$ is difficult to use in practice. However, by using (14) and (16) a Taylor series expansion shows that $\ln(1+\varepsilon_{\theta_n}(z_n)) - \ln(1+\varepsilon^{(0)}_{\theta_n}(z_n^{(0)})) = o(\Delta^2/\sigma_n^2)$. Therefore, in the present paper, it is proposed to neglect these corrective terms in the calculation of the LR $\ln(\Lambda_1(z_n))$. This simplification is especially accurate in practice because for most digital RAW media it holds that $\Delta \ll \sigma_n$.
By using the definition $z_n^{(0)} = \frac{1}{2}(\bar{z}_n + z_n - 1)$ a direct calculation gives:

$$(\Delta(z_n^{(0)}+\tfrac{1}{2})-\theta_n)^2 = (\Delta z_n-\theta_n)^2 + \frac{\Delta^2}{4} + \Delta(z_n-\bar{z}_n)(\Delta z_n-\theta_n).$$

Using this result, the LR $\ln(\Lambda_1(z_n))$ can be approximated by:

$$\ln(\Lambda_1(z_n)) = \frac{\Delta(z_n-\bar{z}_n)(\Delta z_n-\theta_n)}{2\sigma_n^2} - \frac{\Delta^2}{8\sigma_n^2} + o\Big(\frac{\Delta^4}{\sigma_n^4}\Big), \tag{18}$$

where the notation $y = o(x)$ means that y/x tends to 0 as x tends to 0.

3.2. Moments of the LR Λ_1

Even though the expression (18) of $\ln(\Lambda_1(z_n))$ is rather simple, it is not straightforward to establish the probability of each type of detection error of the test δ_R (10). To this end, an asymptotic approach is used by assuming that the number of samples N grows to infinity; this assumption is relevant in practice because the number of samples is very large in —almost— every digital media.
To study the asymptotic distribution of the LR $\ln(\Lambda_1(z_n))$, under both hypotheses $\mathcal{H}_0$ and $\mathcal{H}_1$, it is proposed to apply the well-known Lindeberg's central limit theorem (CLT) [33, theorem 11.2.5] from which it follows that:

$$\frac{\sum_{n=1}^{N}\ln(\Lambda_1(z_n)) - \mathbb{E}_i[\ln(\Lambda_1(z_n))]}{\sqrt{\sum_{n=1}^{N}\mathbb{V}ar_i[\ln(\Lambda_1(z_n))]}} \rightsquigarrow \mathcal{N}(0,1), \tag{19}$$

where for $i = \{0; 1\}$, the notation $\mathbb{E}_i[\cdot]$ and $\mathbb{V}ar_i[\cdot]$ respectively denotes the mathematical expectation and the variance under the hypothesis $\mathcal{H}_i$ and $\rightsquigarrow$ represents the convergence in distribution as N tends to infinity.
It should be noted that the application of Lindeberg's CLT (19) requires that the Lindeberg's condition is satisfied [33, Eq. (11.11)]. In the present case this condition is easy to verify by using the Lyapounov's condition [33, Eq. (11.12)] which implies the Lindeberg's condition.
It follows from the CLT (19) that to establish the error probabilities of the LR test δ_R, it is necessary to calculate the two first moments of $\Lambda_1(z_n)$, under both hypotheses $\mathcal{H}_0$ and $\mathcal{H}_1$.
under the hypothesis $\mathcal{H}_0$, the expectation of the approximated LR $\ln(\Lambda_1(z_n))$ (18) is given by:

$$\mu_0 \overset{\text{def.}}{=} \mathbb{E}_{\mathcal{H}_0}[\ln(\Lambda_1(z_n))] = -\frac{\Delta^2}{8\sigma_n^2} + \frac{\Delta m_0}{2\sigma_n^2}, \tag{20}$$

where the quantity m_0, which represents the impact of quantization, is given by:

$$\begin{aligned} m_0 = m_0(\theta_n) &= \mathbb{E}_{\mathcal{H}_0}[(k-\theta_n)(k-\bar{k})] \\ &= \sum_{k\in\mathcal{Z}} \mathbb{P}_{\mathcal{H}_0}[z_n{=}k](k-\theta_n)(k-\bar{k}). \end{aligned} \tag{21}$$

An explicit expression of m_0 is given in the Appendix B.
Likewise, under the hypothesis $\mathcal{H}_1$, assumption A-1 permits us to calculate the expectation of approximated LR $\ln(\Lambda_1(z_n))$:

$$\mu_1 \overset{\text{def.}}{=} \mathbb{E}_{\mathcal{H}_1}[\ln(\Lambda_1(z_n))] = \frac{\Delta^2}{8\sigma_n^2}. \tag{22}$$

A graphical representation of the term μ_i, $i \in \{0; 1\}$ as a function of θ_n is provided in the Figure 1.

Likewise, the variance of the LR $\ln(\Lambda_1(z_n))$, denoted σ_0^1 and σ_1^2 respectively under hypotheses $\mathcal{H}_0$ and $\mathcal{H}_1$, are given by:

$$\sigma_0^2 = \frac{\Delta^2}{4\sigma_n^4}\Big(\mathbb{E}_{\mathcal{H}_0}[(\Delta z_n-\theta_n)^2]-m_0^2\Big), \tag{23}$$

$$\sigma_1^2 = \frac{\Delta^2}{4\sigma_n^4}\left(\mathbb{E}_{\mathcal{H}_0}\left[(\Delta z_n-\theta_n)^2\right] + \frac{\Delta^2}{4}\right). \tag{24}$$

The calculation of the moments (20) - (24) are detailed in the Appendix B.

3.3. Detection Performance in the Case $R \in [0; 1]$

It follows from the Neyman-Pearson lemma that the LRT δ_1^{np}, based on $\ln(\Lambda_1(\mathbf{Z}))$, is the most powerful test designed for $R = 1$ provided that the decision threshold is correctly chosen. In practice, the assumption that relative payload R is known does not hold; hence, the hypothesis $\mathcal{H}_1$ becomes composite

and the ultimate goal is to find a Uniformly Most Powerful (UMP) test, that is a test that maximizes the power function whatever R might be. Here, it is straightforward to verify that the hypotheses do not admit a monotonic likelihood ratio; therefore the existence of a UMP test is compromised [33, theorem 3.4.1].

The problem of finding an optimal test for $R \in [0;1]$ is deeply studied in [16, 10, 50]. In [16] it is shown that the test δ_1 (10), based on the LR $\ln(\Lambda_1(\mathbf{Z}))$ (18) is Asymptotically UMP (AUMP) using the dubious assumption that the quantization step Δ tends to zero, and thus becomes negligible. Taking into account the impact of quantization, a Locally AUMP (LAUMP) test, *i.e.* a most powerful around a given payload $R^\star$, is proposed in [10, 50].

Because the design of a UMP or a AUMP test for LSB replacement steganalysis seems out of reach, in realistic conditions, it is proposed in the present paper to use the test δ_1^{np} designed for $R = 1$. The main reason behind this choice is that whatever the real payload $R \in [0;1]$ might be, each pixel is used or not for hiding a secret bit and hence, actual payload is either 0 or 1 for each pixel.
From Equation (9), the law of total expectation and results (20) - (22) permits us to establish the expectation μ_R of the LR $\ln(\Lambda_1(z_n))$:

$$\mu_R = (1-R)\mu_0 + R\mu_1 = \frac{\Delta^2}{8\sigma_n^2}(2R-1) + \frac{(1-R)m_0}{2\sigma_n^2}. \quad (25)$$

Similarly, the variance σ_R^2 of the LR for any $R \in [0;1]$ can be calculated from the law of total variance:

$$\sigma_R^2 = (1-R)(\sigma_0^2+\mu_0^2) + R(\sigma_1^2+\mu_1^2) - ((1-R)\mu_0 + R\mu_1)^2\,, \quad (26)$$

where the moments μ_0, μ_1 σ_0^2 and σ_1^2 are respectively given in Equations (20) - (24).

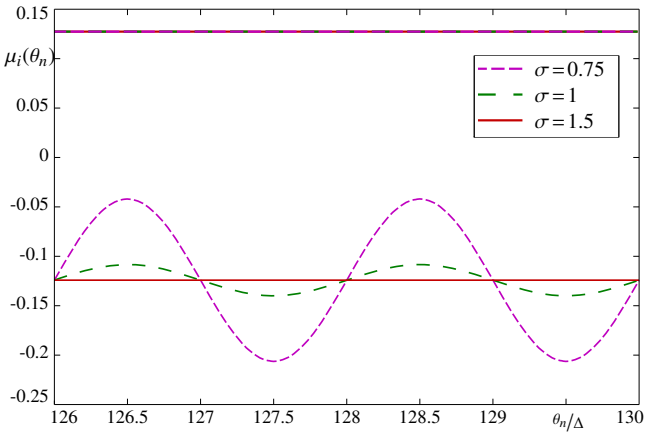


Figure 1: Impact of quantization on the expectation of the LR $\Lambda(z_n)$ as a function of samples expectation θ_n, for different values of $\sigma_n = \{0.75; 1; 1.5\}$ and $\Delta = 1$. These results show that under the hypothesis $\mathcal{H}_1$, the expectation μ_1 does not depend on θ_n while under $\mathcal{H}_0$ the impact of quantization becomes rather negligible only when $\sigma_n \gtrsim 1.5\Delta$.

For clarity, let us define for $i = \{0;1\}$:

$$\widetilde{\mu}_i = \frac{1}{N}\sum_{n=1}^{N}\mathbb{E}_i\left[\ln(\Lambda_1(z_n))\right]\,,\ \widetilde{\sigma}_i^2 = \frac{1}{N}\sum_{n=1}^{N}\mathbb{V}ar_i\left[\ln(\Lambda_1(z_n))\right]. \quad (27)$$

which respectively represent the "mean expectation" and the "mean variance" of the LR $\ln(\Lambda_1(\mathbf{Z}))$. Obviously, when samples are i.i.d, it immediately follows has $\widetilde{\mu}_i = \mu_i$ and $\widetilde{\sigma}_i^2 = \sigma_i^2$. It follows from Lindeberg's CLT (19), that for any relative payload $R \in]0;1]$, the term $\frac{1}{\sqrt{N}}\sum_{n=1}^{N}\ln(\Lambda_1(z_n))$ follows, under both hypotheses, the asymptotic distribution given by:

$$\begin{cases} \dfrac{1}{\sqrt{N}}\displaystyle\sum_{n=1}^{N}\ln(\Lambda_1(z_n)) \rightsquigarrow \mathcal{N}(\widetilde{\mu}_0\sqrt{N}\,;\widetilde{\sigma}_0^2) \quad \text{under} \quad \mathcal{H}_0 \\ \dfrac{1}{\sqrt{N}}\displaystyle\sum_{n=1}^{N}\ln(\Lambda_1(z_n)) \rightsquigarrow \mathcal{N}(\widetilde{\mu}_R\sqrt{N}\,;\widetilde{\sigma}_R^2) \quad \text{under} \quad \mathcal{H}_1, \end{cases} \quad (28)$$

where the terms $\widetilde{\mu}_i$ and $\widetilde{\sigma}_i^2$ are defined in (27). Following the Neyman-Pearson approach, once the false-alarm probability α_0 is defined, it is necessary, first, to calculate the decision threshold τ_{α_0} that guarantees this false-alarm probability so that $\delta \in \mathcal{K}_{\alpha_0}$, and second, to maximize the power function of the test δ. The following Theorem 1 and 2 respectively provides an analytic expression for the decision threshold τ_{α_0} and for the power function β_{δ_1}.

Theorem 1. *For any $\alpha_0 \in]0;1[$, the threshold value given by:*

$$\tau_{\alpha_0} = \left(\widetilde{\sigma}_0\sqrt{N}\right)\Phi^{-1}(1-\alpha_0) + (\widetilde{\mu}_0 N)\,, \quad (29)$$

where $\Phi^{-1}(\cdot)$ is the standard Gaussian inverse cumulative distribution function (cdf), guarantees that asymptotically, as N tends to ∞, the test δ_1 (10) satisfies $\alpha_{\delta_1} = \alpha_0$.

Proof. Using the result (28) it asymptotically holds that for any $\tau_{\alpha_0} \in \mathbb{R}$:

$$\alpha_{\delta_1} = \mathbb{P}_{\mathcal{H}_0}\left[\ln(\Lambda_R(\mathbf{Z})) \geq \tau_{\alpha_0}\right] = 1 - \Phi\left(\frac{\tau_{\alpha_0} - \widetilde{\mu}_0 N}{\widetilde{\sigma}_0\sqrt{N}}\right).$$

Hence, since Φ is an increasing function, for any $\alpha_0 \geq \alpha_{\delta_1}$ one has:

$$\Phi^{-1}(1-\alpha_0) \leq \Phi^{-1}(1-\alpha_{\delta_1}) = \frac{\tau_{\alpha_0} - \widetilde{\mu}_0 N}{\widetilde{\sigma}_0\sqrt{N}}$$
$$\Leftrightarrow \quad \tau_{\alpha_0} \leq (\widetilde{\sigma}_0\sqrt{N})\Phi^{-1}(1-\alpha_0) + (\widetilde{\mu}_0 N)\,.$$

□

Theorem 2. *For any $R \in]0;1]$ and for any $\alpha_0 \in]0;1[$, assuming that the parameters $\boldsymbol{\theta} = \{\theta_n\}_{n=1}^N$ and $\boldsymbol{\sigma} = \{\sigma_n\}_{N=1}^N$ are known, then the power function β_{δ_1} associated with the test δ_1 (10) is asymptotically given, as N tends to ∞, by:*

$$\beta_{\delta_1} = 1 - \Phi\left(\frac{\widetilde{\sigma}_0\Phi^{-1}(1-\alpha_0) + (\widetilde{\mu}_0 - \widetilde{\mu}_1)R\sqrt{N}}{\widetilde{\sigma}_R}\right) \quad (30)$$

It can be noted that the Theorems 1 and 2 are of crucial interest; the first allows the establishing of the decision threshold which asymptotically allows us to guarantee that the test δ_1 satisfies a given prescribed false-alarm probability; the decision threshold τ_{α_0} (29) does not depend on the relative payload and, thus, holds for any $R \in [0;1]$. Theorem 2 is also very useful as it provides the test δ_1, optimal for $R = 1$, with an analytic expression of its power function for any $R \in [0;1]$.

The Figure 2 provides a graphical representation of the power function β_{δ_1} (30) for a particular case of i.i.d. samples (with constant expectation θ_n and constant variance σ_n^2 for all n).

Remark 1. *The proposed approach is closely related to the one adopted in [13]: in both cases the Neyman-Pearson Lemma is used to obtain a simple expression of the most powerful LRT. However, it is supposed in [13] that the samples are* i.i.d*, i.e. for all $n \in \{0,\dots,N\}$, $\theta_n = \theta$ and $\sigma_n^2 = \sigma^2$. Under this assumption it is shown in [13] that the LRT can be written as follows:*

$$D_{KL}(P_{\mathbf{Z}}, Q_\theta^R) - D_{KL}(P_{\mathbf{Z}}, P_\theta) \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\lessgtr}} \tau,$$

where $P_{\mathbf{Z}} = \left\{p_{\mathbf{Z}}[0],\dots,p_{\mathbf{Z}}[2^b-1]\right\}$ denotes the empirical distribution of analyzed samples and $D_{KL}(P,Q)$ is the Kullback-Leibler divergence between distributions P and Q.
By using Equation (9), a short calculation shows that when samples are i.i.d, the LR $\ln(\Lambda_1(\mathbf{Z}))$ can be written:

$$\ln(\Lambda_R(\mathbf{Z})) = -N\left(D_{KL}(P_{\mathbf{Z}}, Q_{\theta_n}^R) - D_{KL}(P_{\mathbf{Z}}, P_{\theta_n})\right).$$

However, the fundamental strength of present paper is that samples are not considered i.i.d. and expectation vector $\boldsymbol{\theta} = \{\theta_n\}_{n=1}^N$ is explicitly taken into account as nuisance parameter. This eventually allows us to design a test with a much higher power function by considering properties of each sample.

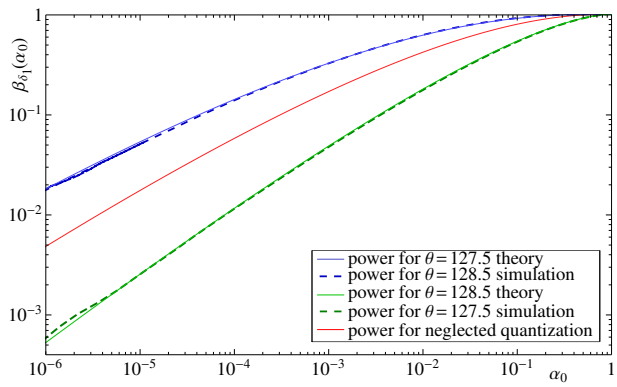


Figure 2: Impact of quantization on the power function of the MP test δ_1 shown through a ROC curve, $\beta\delta_1$ as a function of α_{δ_1}. Results were obtained using $R = 1$, $N = 1000$ pixels with parameters $\theta = \{127.5; 128.5\}$, $\sigma_n = 0.75$ and $\Delta = 1$; for Monte-Carlo simulations 10^8 repetitions were used.

4. Simplification for the General Case of Non-Stationary Samples

The results presented in Sections 3.2 - 3.3 explicitly take into account the impact of data quantization and analytically establish the statistical properties of the most powerful test δ_1. The impact of quantization on the expectation of the LR $\ln(\Lambda_1(z_n))$ and on the power function of the test δ_1 is respectively provided in the Figure 1 and in the Figure 2.
Even though, the impact of quantization on the performance of the test δ_1 can easily be calculated numerically using Equation (20) - (27) two major difficulties remain in practice. First, providing a simple analytic expression for the expectation $\widetilde{\mu}_i$ and for the variance $\widetilde{\sigma}_i$ (27) of the LR $\ln(\Lambda_1(\mathbf{Z}))$ is obviously difficult. Second, the decision threshold τ_{α_0} depends on the quantities $\widetilde{\mu}_0$ and $\widetilde{\sigma}_0$ which both depend on parameters $\boldsymbol{\theta} = \{\theta_n\}_{n=1}^N$ and $\boldsymbol{\sigma} = \{\sigma_n\}_{n=1}^N$. In practice, this is a major drawback as it is thus necessary to calculate a specific decision threshold τ_{α_0} for each inspected medium.
In the present section, it is proposed to overcome these difficulties by studying the behavior of the term $m_0(\theta_n)$, for a large set of samples which all have different parameters θ_n and σ_n. Unfortunately, this is hardly possible in general and an assumption on these parameters is required. To this end, let us define $\zeta_n \in [-\Delta;\Delta]$, $\zeta_n = \theta_n - Q_{2\Delta}(\theta_n)$, a quantity on which only the moments of $\ln(\Lambda_1(z_n))$ depends.
Without any extra information on a medium $\mathbf{Z}$ the following assumption is adopted.

A-3 Let us assume that in the analyzed medium $\mathbf{Z}$, the values ζ_n asymptotically occurs with the same frequency. In other words, denoting N_{x_0,x_1}, $x_0 < x_1$, $\{n \,/\, \zeta_n \in [x_0, x_1]\}$, that is the number of samples which verify $\zeta_n \in [x_0; x_1]$, as N tends to infinity it is assumed that :

$$\forall x_0, x_1 \in [-\Delta;\Delta]^2, x_0 < x_1, \lim_{N\to\infty} N_{x_0,x_1} = \frac{x_1 - x_0}{2\Delta} \quad (31)$$

It is obviously difficult to formally justify the assumption A-3. This *a priori* model for ζ_n roughly speaking corresponds to the assumption that the quantization noise is uniform, *i.e.* $\theta_n - Q_{2\Delta}(\theta_n)$ occurs like a uniformly distributed random variable.
Using the assumption A-3, the corrective term m_0 tends to become negligible as the number of pixel N grows to infinity. In fact, the Equation (21) shows that $m_0(\zeta_n) = -m_0(\zeta_n + \Delta)$; hence, using assumption A-3, the sum of all terms $m_0(\zeta_n)$ tends to 0, see the Appendix C for details.
The following Proposition 1 formalizes this result.

Proposition 1. *Under assumption A-3, the mean expectation $\widetilde{\mu}_i$ and the mean variance $\widetilde{\sigma}_i^2$ (27) of LR $\ln(\Lambda_1(z_n))$ are asymptotically, as N tends to infinity, given by:*

$$\widetilde{\mu}_0 = \frac{1}{N}\sum_{n=1}^N -\frac{\Delta^2}{8\sigma_n^2}, \qquad \widetilde{\mu}_1 = \frac{1}{N}\sum_{n=1}^N \frac{\Delta^2}{8\sigma_n^2}, \quad (32)$$

$$\widetilde{\sigma}_0^2 = \frac{1}{N}\sum_{n=1}^N \frac{\Delta^2}{4\sigma_n^2}\left(1 + \frac{\Delta^2}{12\sigma_n^2}\right), \qquad \widetilde{\sigma}_1^2 = \frac{1}{N}\sum_{n=1}^N \frac{\Delta^2}{4\sigma_n^2}\left(1 + \frac{\Delta^2}{3\sigma_n^2}\right). \quad (33)$$

From Equations (32) and (33) and from the laws of total expectation and total variance, see (25) and (26), it follows that:

$$\begin{aligned} \widetilde{\mu}_R &= \frac{1}{N}\sum_{n=1}^{N}\frac{\Delta^2(2R-1)}{8\sigma_n^2}, \\ \widetilde{\sigma}_R^2 &= \frac{1}{N}\sum_{n=1}^{N}\frac{\Delta^2}{4\sigma_n^2}\left(1+\frac{\Delta^2}{4\sigma_n^2}(2R-R^2)+\frac{\Delta^2}{12\sigma_n^2}\right). \end{aligned} \tag{34}$$

Proof. Proof of Proposition 1 is given in the Appendix C. □

For clarity and simplicity, it is proposed in the present paper to normalize the LR $\ln(\Lambda_1(z_n))$, using expressions (32) and (33). To this end, let the quantities $\overline{\sigma}$ and $\ln(\widetilde{\Lambda}(\mathbf{Z}))$ be defined as:

$$\frac{1}{\bar{\sigma}^2} \overset{\text{def.}}{=} \frac{1}{N}\sum_{n=1}^{N}\left[\sigma_n^2\left(1+\frac{\Delta^2}{12\sigma_n^2}\right)\right]^{-1}, \tag{35}$$

$$\begin{aligned} \ln(\widetilde{\Lambda}(\mathbf{Z})) &\overset{\text{def.}}{=} \frac{\Delta\bar{\sigma}}{\sqrt{N}}\sum_{n=1}^{N}\frac{(z_n-\bar{z}_n)(\Delta z_n-\theta_n)}{\sigma_n^2(1+\Delta^2/12\sigma_n^2)} \\ &= \frac{2\bar{\sigma}}{\sqrt{N}}\sum_{n=1}^{N}\frac{[\ln(\Lambda_1(\mathbf{Z}))-\widetilde{\mu}_0]}{(1+\Delta^2/12\sigma_n^2)}. \end{aligned} \tag{36}$$

From these expressions, it immediately follows from Proposition 1 and Lindeberg's CLT (19) that under the null hypothesis $\mathcal{H}_0$ one has:

$$\ln(\widetilde{\Lambda}(\mathbf{Z})) \rightsquigarrow \mathcal{N}(0,1). \tag{37}$$

Similarly, under the hypothesis $\mathcal{H}_1$ that $\mathbf{Z}$ contains information hidden with a payload $R \in]0;1]$, one has:

$$\ln(\widetilde{\Lambda}(\mathbf{Z})) = \frac{\bar{\sigma}}{\sqrt{N}}\sum_{n=1}^{N}\ln(\widetilde{\Lambda}(z_n)) \rightsquigarrow \mathcal{N}(\varrho, 1+\gamma_R), \tag{38}$$

$$\text{with } \gamma_R = \frac{\Delta^2}{4}(2R-R^2)\frac{\sum_{n=1}^{N}\left[\sigma_n^2\left(1+\Delta^2/12\sigma_n^2\right)\right]^{-2}}{\sum_{n=1}^{N}\left[\sigma_n^2\left(1+\Delta^2/12\sigma_n^2\right)\right]^{-1}},$$

and the "Insertion-to-Noise Ratio" (INR) ϱ is defined as:

$$\varrho = \sqrt{N}\frac{R\Delta}{2\bar{\sigma}}. \tag{39}$$

The results (37) and (38) are demonstrated in the Appendix C.2.

The crucial importance of this INR ϱ for power function is highlighted in Theorems 4 and 6 and throughout numerical results of the Section 6.

The results (37) and (38) are illustrated in the Figure 3 which represents the two first moments of the "simplified" LR $\ln(\widetilde{\Lambda}(\mathbf{Z}))$ as a function of relative payload $R \in [0;1]$; note that for a better readability, the displayed variance is actually $\mathbb{V}ar\left[\ln(\widetilde{\Lambda}(\mathbf{Z}))\right]-1 = \gamma_R$.

For definition, let the test $\widetilde{\delta}$ associated with the LR $\ln(\widetilde{\Lambda}(z_n))$ be defined as:

$$\widetilde{\delta} = \begin{cases} \mathcal{H}_0 & \text{if } \ln(\widetilde{\Lambda}(\mathbf{Z})) = \dfrac{\bar{\sigma}}{\Delta\sqrt{N}}\displaystyle\sum_{n=1}^{N}\ln(\widetilde{\Lambda}(z_n)) < \widetilde{\tau}_{\alpha_0}, \\ \mathcal{H}_1 & \text{if } \ln(\widetilde{\Lambda}(\mathbf{Z})) = \dfrac{\bar{\sigma}}{\Delta\sqrt{N}}\displaystyle\sum_{n=1}^{N}\ln(\widetilde{\Lambda}(z_n)) \geq \widetilde{\tau}_{\alpha_0}. \end{cases} \tag{40}$$

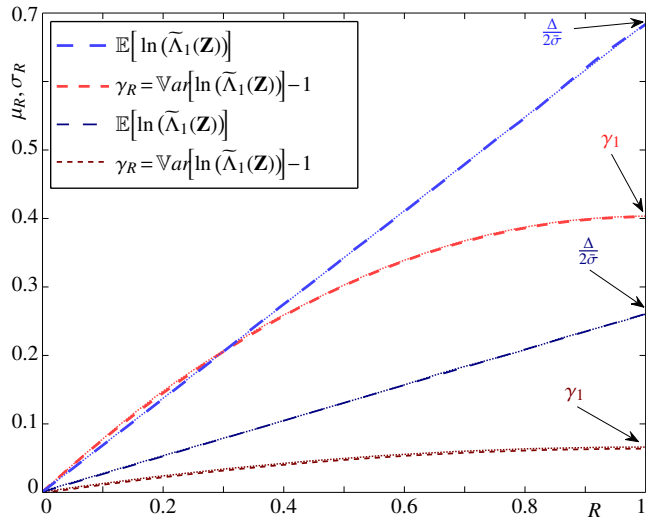


Figure 3: Expectation and variance of LR $\ln(\widetilde{\Lambda}(z_n))$ (36) as a function of the payload R. The light lines, on the top, correspond to $\Delta = 0.65 > \sigma_n = 0.475$; the dark lines, on the bottom, correspond to $\Delta = 0.65$ and $\sigma_n = 1.25$. The thin dotted lines are the theoretical moments from (38) while the thick dashed lines result from Monte-Carlo simulations satisfying assumption A-3.

Theorem 3. *For any $\alpha_0 \in]0;1[$, the threshold value given by:*

$$\widetilde{\tau}_{\alpha_0} = \Phi^{-1}(1-\alpha_0), \tag{41}$$

asymptotically guarantees that $\widetilde{\delta}$ (40) satisfies $\alpha_0(\widetilde{\delta}_1) = \alpha_0$.

Theorem 4. *For any $R \in]0;1]$ and for any $\alpha_0 \in]0;1[$, assuming that the parameters $\boldsymbol{\theta} = \{\theta_n\}_{n=1}^N$ and $\boldsymbol{\sigma} = \{\sigma_n\}_{N=1}^N$ are known, then the power function $\beta_{\widetilde{\delta}}$ associated with the test $\widetilde{\delta}$ (40) is asymptotically given, as N tends to ∞, by:*

$$\beta_{\widetilde{\delta}} = 1-\Phi\left(\frac{\Phi^{-1}(1-\alpha_0)-\varrho}{\sqrt{1+\gamma_R}}\right) \tag{42}$$

Proof. The demonstrations of Theorems 3 and 4 are detailed in the Appendix C. □

The main interests of the test $\widetilde{\delta}$ (40) are twofold. First, the decision threshold given by (41) does not depend on any medium parameters but only on the prescribed false-alarm probability α_0 ; hence for any analyzed medium, it is straightforward to guarantee a prescribed false-alarm probability. Second, the power function given in Equation (42) provides a simple expression and an accurate approximation of power function of the most powerful test. The power function as given in (42) can thus be used as an optimal bound for any steganalyzer which aims at detecting LSB replacement.

Finally, it can be noted that when the quantization step is small compared to the noise standard deviation, *i.e.* $\Delta \ll \sigma$ see especially [9, 8, 16] in which the impact of quantization is neglected, the Equation (42) of the power function simplifies to $\beta_{\widetilde{\delta}} = 1-\Phi\left(\Phi^{-1}(1-\alpha_0)+\varrho\right)$.

Remark 2. *As discussed in the beginning of Section 3.1, the noise variance varies from sample to sample. This property of noise non-stationarity, or heteroscedasticity, especially studied for digital images in [19, 24], helps the steganalyzers because, as shown in the Appendix A, one can note that:*

$$\bar{\sigma}^2 \leq \frac{1}{N}\sum_{n=1}^{N}\sigma_n^2\left(1+\frac{\Delta^2}{12\sigma_n^2}\right), \tag{43}$$

$$\Rightarrow \varrho = \sqrt{N}\frac{R\Delta}{2\bar{\sigma}} \geq \sqrt{N}\frac{R\Delta}{2}\left(\frac{1}{N}\sum_{n=1}^{N}\sigma_n^2\left(1+\frac{\Delta^2}{12\sigma_n^2}\right)\right)^{-1/2}$$

In other words, the Equation (43) shows that for a given mean variance of pixels (or mean noise level), the INR (39) ϱ is minimal when all the samples have the same variance. It is obvious that the power function as given in Equation (42) is an increasing function of ϱ . Therefore, for any medium for which the noise heteroscedastic property holds the power function of LRT $\widetilde{\delta}$ (40) is higher than for a medium with the same mean variance whose samples all have the same variance.
It should be noted that this result only holds true under assumptions A-1 and A-2. For a steganographic scheme which embeds hidden bits only in selected samples, this result not necessarily holds.

5. Dealing with Nuisance Parameters θ and σ in Practice

In a practical situation, the steganalyst usually has no information on the analyzed medium. From a statistical point of view, the problem is then to use quantized observations to test two composite hypotheses in presence of an unknown nuisance parameter $\boldsymbol{\theta}$. Obviously, the hypothesis testing theory does not provide a general methodology for finding an optimal test for such problems.
It is necessary to estimate the parameter θ_n for each pixel. However, an estimation of each parameter θ_n is impossible and hence, the "theoretical" decision problem (7) can not be solved.

5.1. Decision Problem for Unknown Parameters $\boldsymbol{\theta}$ and $\boldsymbol{\sigma}$

To overcome the previously discussed difficulty of dealing with nuisance parameter, the main idea is to group the samples into small sets. This allows us to exploit the redundancies that naturally exist between neighboring samples to estimate locally their expectation.
Hence, it is proposed to divide the medium $\mathbf{Z}$ into a set of K statistically independent (non-overlapping) "blocks" of $L > 0$ consecutive samples denoted, for $k = 1,\dots,K$, by $\mathbf{z}_k=(z_{k,1},\dots,z_{k,L})^T$, where $\mathbf{A}^T$ is the transpose of matrix $\mathbf{A}$. Of course, L is chosen rather small to ensure a simple local estimation and $K = \lfloor N/L \rfloor$ (rounded down) to includes -almost- all samples of $\mathbf{Z}$ during its inspection.
As explained in Section 2, samples are assumed to be statistically independent. Hence, the vector of quantized observations $\mathbf{z}_k$ can be written, thanks to (1) and (3), as:

$$\mathbf{z}_k = Q_\Delta(\boldsymbol{\theta}_k + \boldsymbol{\xi}_k),$$

where the quantizer $Q_\Delta(\cdot)$, defined in (2), is applied to each component individually, the mean vector $\boldsymbol{\theta}_k$ is defined by $\boldsymbol{\theta}_k = (\theta_{k,1},\dots,\theta_{k,L})^T$ and the stochastic term $\boldsymbol{\xi}_k$ is the realization of independent Gaussian vector $\Xi_k \sim \mathcal{N}(0,\Sigma_k)$, with $\Sigma_k = \mathrm{diag}(\sigma_{k,1}^2,\dots,\sigma_{k,L}^2)$.
It thus follows from (4) and (5) that the joint distribution of each vector of samples $\mathbf{z}_k$ is given by the distribution product, see [3],

$$\begin{cases} P_{\boldsymbol{\theta}_k} = P_{\theta_{k,1}} \times \cdots \times P_{\theta_{k,L}} & \text{under } \mathcal{H}_0 \\ Q^R_{\boldsymbol{\theta}_k} = Q^R_{\theta_{k,1}} \times \cdots \times Q^R_{\theta_{k,L}} & \text{under } \mathcal{H}_1. \end{cases} \tag{44}$$

Using the joint distribution of the vector of samples from (44), the alternative hidden information decision problem becomes:

$$\begin{cases} \mathcal{H}_0=\{\mathbf{z}_k\sim\mathcal{P}_{\boldsymbol{\theta}_k}, \forall k=1\dots,K\}, \\ \mathcal{H}_1=\{\mathbf{z}_k\sim Q^R_{\boldsymbol{\theta}_k}, \forall k=1\dots,K, \forall R\geq 0\}. \end{cases} \tag{45}$$

Problem (45) is strictly equivalent to problem (7) when $\boldsymbol{\theta}$ is known. When $\boldsymbol{\theta}$ is unknown, exploiting the redundancies between the pixels of the same block is necessary to limit the number of unknown parameters with respect to the number of samples.

5.2. Cover Content Estimation and Ensuing Detection Performance

The issue is then to model accurately the local redundancies that exist between neighboring samples to allow an efficient estimation of $\boldsymbol{\theta}_k$. While some accurate and efficient models of the content of natural images have already been proposed for steganalysis, see [9, 8], this problem lies outside the scope of the present paper which aims at applying statistical decision theory for steganalysis. Hence, among the wide range of possible local model, see [1, 23], in this paper the mean vector $\boldsymbol{\theta}_k$ is defined by the following linear parametric model [30, 31] for which theory of hypothesis testing is rather well developed:

$$\boldsymbol{\theta}_k = \mathbf{H}\,\mathbf{a}_k, \tag{46}$$

where $\mathbf{H}$ is a matrix of size $L\times p$ and $\mathbf{a} \in \mathbb{R}^p$. It is assumed that $\mathbf{H}$ is a full rank column matrix, that is $\mathrm{rank}(\mathbf{H}) = p < L$. For definition, it is assumed in the rest of this paper that $\boldsymbol{\theta} \in \Theta = \omega^K$ where ω is the $\mathbb{R}^p$ subspace of $\mathbb{R}^L$ defined by $\omega = \mathrm{im}(\mathbf{H})$.
The choice of the matrix $\mathbf{H}$ is fundamental for such a parametric model. The problem of designing a good parametric model for local signal approximation is out of the scope of this paper, some discussion can be found in [1, 23, 35]. In this paper, it is assumed that as long as block size remains rather small, they can efficiently, be modeled by algebraic polynomial, see details in Section 6.1; similarly, due to the small block size, the noise variance is assumed constant over each block: $\Sigma_k = \sigma^2\mathbf{I}_L$, with $\mathbf{I}_L$ the identity matrix of size L.
It follows from the parametric model (46) that the maximum likelihood estimators of parameters $\boldsymbol{\theta}_k$ and $\boldsymbol{\sigma}_k$ are given by:

$$\widehat{\boldsymbol{\theta}}_k = \mathbf{P}_H\,\mathbf{z}_k \text{ with } \mathbf{P}_H = \mathbf{H}\left(\mathbf{H}^T\mathbf{H}\right)^{-1}\mathbf{H}^T, \tag{47}$$

$$\widehat{\sigma}_k^2 = \frac{\Delta^2}{L-p}\left|\mathbf{P}_H^\perp\,\mathbf{z}_k\right|_2^2 \text{ with } \mathbf{P}_H^\perp = \mathbf{I}_L - \mathbf{P}_H. \tag{48}$$

The parameter $\boldsymbol{\theta}_k$ acts here as nuisance parameter. In fact, as shown in Equations (18) and (36) the θ_n's explicitly occur in the decision function of the LR test even though have no interest for hidden information detection. The theoretical aspect of dealing with nuisance parameters for testing statistical hypothesis is discussed in [33, chap.6]. An efficient and well-known approach consists of using the statistical theory of invariance. Application of optimal invariant tests for image processing has already been studied in [17, 40].

Let us note that the decision problem described in (45) remains "almost" invariant under the group of translation $G : \{g(\mathbf{z}_k) = \mathbf{z}_k + \mathbf{H}\mathbf{a}_k\}$ [10]; the word "almost" is here due to the quantization without which the invariance would be exact. Hence, it is proposed to use this invariance property to design a test close to the generalized LR test (GLRT) by using the "simplified" LR $\ln\left(\widetilde{\Lambda}(\mathbf{Z})\right)$ replacing the θ_n by the estimate $\widehat{\boldsymbol{\theta}}_k = (\widehat{\theta}_{k,1}, \ldots, \widehat{\theta}_{k,L})^T$ (47) and the noise variance $\sigma_n^2 + {}^{\Delta^2}/_{12}$ by its estimation $\widehat{\sigma}_k^2$ (48). The proposed test $\widehat{\delta}$ is thus given by:

$$\widehat{\delta} = \begin{cases} \mathcal{H}_0 & \text{if } \ln\left(\widehat{\Lambda}(\mathbf{Z})\right) = \dfrac{\widehat{\bar{\sigma}}}{\sqrt{K}} \displaystyle\sum_{k=1}^{K} \ln\left(\widehat{\Lambda}(\mathbf{z}_k)\right) < \widehat{\tau}_{\alpha_0}, \\ \mathcal{H}_1 & \text{if } \ln\left(\widehat{\Lambda}(\mathbf{Z})\right) = \dfrac{\widehat{\bar{\sigma}}}{\sqrt{K}} \displaystyle\sum_{k=1}^{K} \ln\left(\widehat{\Lambda}(\mathbf{z}_k)\right) \geq \widehat{\tau}_{\alpha_0}, \end{cases} \tag{49}$$

where the decision threshold $\widehat{\tau}_{\alpha_0}$ is the solution of $\sup_{\boldsymbol{\theta}\in\Theta} \mathbb{P}_{\mathcal{H}_0}\left[\widehat{\Lambda}(\mathbf{Z}) \geq \widehat{\tau}_{\alpha_0}\right] = \alpha_0$ to ensure that $\widehat{\delta} \in \mathcal{K}_\alpha$. By substituting in the LR $\ln\left(\widetilde{\Lambda}(\mathbf{Z})\right)$ (36) the expectation and the variance of samples by their estimations, the GLR $\ln\left(\widehat{\Lambda}(\mathbf{z}_k)\right)$ is defined by:

$$\ln\left(\widehat{\Lambda}(\mathbf{z}_k)\right) = \frac{1}{2\widehat{\sigma}_k^2\sqrt{L-p}} \sum_{l=1}^{L} (z_{k,l} - \bar{z}_{k,l})(\Delta z_{k,l} - \widehat{\theta}_{k,l}), \tag{50}$$

where $\widehat{\theta}_{k,l}$ and $\widehat{\sigma}_k^2$ are respectively estimation of parameter $\boldsymbol{\theta}_k$ and σ_k^2 given by Equations (47) - (48) and the term $\widehat{\bar{\sigma}}$ is defined as:

$$\frac{1}{\widehat{\bar{\sigma}}^2} = \frac{1}{K} \sum_{k=1}^{K} \frac{1}{\widehat{\sigma}_k^2}. \tag{51}$$

Once again, it is proposed to study the probability of each error of the test $\widehat{\delta}$ (49) by applying Lindeberg's CLT (19) in order to establish the asymptotic distribution of $\ln\left(\widehat{\Lambda}(\mathbf{Z})\right)$. To draw a meaningful comparison with the "simplified" LR $\ln\left(\widetilde{\Lambda}(\mathbf{Z})\right)$ (36), let us define $\widehat{\varrho}$ as:

$$\widehat{\varrho} = \sqrt{K(L-p)}\frac{R\Delta}{2\widehat{\bar{\sigma}}}. \tag{52}$$

Assuming that $\boldsymbol{\theta} \in \Theta$, a short algebra that is detailed in the Appendix D, immediately permits us to establish that under the null hypothesis $\mathcal{H}_0$ one has:

$$\frac{\widehat{\bar{\sigma}}}{\sqrt{K}} \sum_{n=1}^{N} \ln\left(\widehat{\Lambda}(\mathbf{z}_k)\right) = \widehat{\Lambda}(\mathbf{Z}) \rightsquigarrow \mathcal{N}(0\,;\,1) \tag{53}$$

Under the alternative hypothesis $\mathcal{H}_1$, the main difference with the calculations from Section 4 is that data hidding biases the estimated noise variance $\widehat{\sigma}_k^2$; in fact, a straightforward calculation permits us to verify that when $\mathbf{Z}$ contains information hidden with payload $R \in]0;1]$, then the mathematical expectation of estimator $\widehat{\sigma}_k^2$ is:

$$\mathbb{E}\left[\widehat{\sigma}_k^2\right] = \sigma_k^2 + \frac{\Delta^2}{12} + \frac{R\Delta^2}{2} = \sigma_k^2\left(1 + \frac{\Delta^2}{12\sigma_k^2} + \frac{R\Delta^2}{2\sigma_k^2}\right). \tag{54}$$

Taking into account the bias of noise variance estimator (54), it is shown in the Appendix D, that under the alternative hypothesis $\mathcal{H}_1$ the GLR $\widehat{\Lambda}(\mathbf{Z})$ satisfies:

$$\frac{\widehat{\bar{\sigma}}}{\sqrt{K}} \sum_{k=1}^{k} \ln\left(\widehat{\Lambda}(\mathbf{z}_k)\right) = \widehat{\Lambda}(\mathbf{Z}) \rightsquigarrow \mathcal{N}\left(\widehat{\varrho}\,;\,1 - \widehat{\gamma}_R\right), \tag{55}$$

where:

$$\widehat{\gamma}_R = \sum_{k=1}^{K} \frac{R^2\Delta^2}{4} \frac{\sum_{k=1}^{K}\left[\sigma_k^2\left(1 + {}^{\Delta^2}/_{12\sigma_k^2} + {}^{R\Delta^2}/_{2\sigma_k^2}\right)\right]^{-2}}{\sum_{k=1}^{K}\left[\sigma_k^2\left(1 + {}^{\Delta^2}/_{12\sigma_k^2} + {}^{R\Delta^2}/_{2\sigma_k^2}\right)\right]^{-1}}. \tag{56}$$

The asymptotic distributions (53) and (55) of the GLR $\widehat{\Lambda}(\mathbf{Z})$ permit us to calculate analytically the decision threshold that guarantees a false-alarm probability as well as the power function of the test $\widehat{\delta}$.

Theorem 5. *For any $\alpha_0 \in]0;1[$ and for any $\boldsymbol{\theta} \in \Theta$, the threshold value given by*

$$\tau_{\alpha_0} = \Phi^{-1}(1 - \alpha_0), \tag{57}$$

guarantees that asymptotically, as N tends to ∞, the test $\widehat{\delta}$ (49) satisfies $\alpha_{\delta_1} = \alpha_0$.

Theorem 6. *For any $R \in]0;1]$, for any $\alpha_0 \in]0;1[$ and for any $\boldsymbol{\theta} \in \Theta$, the power function $\beta_{\widehat{\delta}}$ associated with the test $\widehat{\delta}$ (49) is asymptotically, as N tends to ∞, given by:*

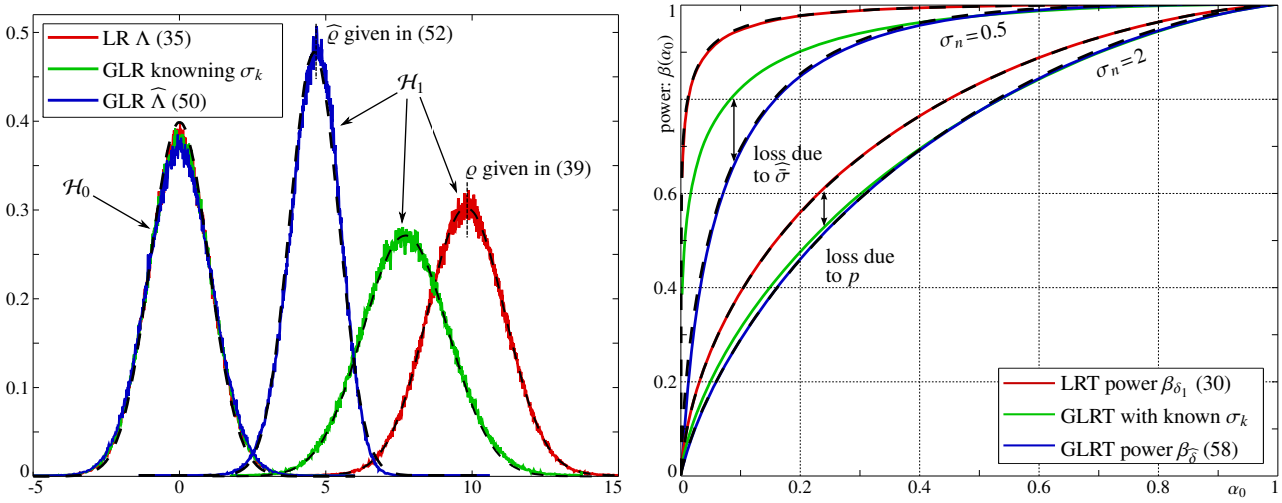
$$\beta_{\widehat{\delta}} = 1 - \Phi\left(\frac{\Phi^{-1}(1-\alpha_0) - \widehat{\varrho}}{\sqrt{1 + \widehat{\gamma}_R}}\right). \tag{58}$$

Proof. The proof of Theorems 5 and 6 are given in the Appendix D. □

The comparison between the power function of the LRT β_{δ_1} (30) and the power function of the proposed GLR test $\beta_{\widehat{\delta}}$ (58), shows that the loss of power of the latter is due to two phenomena. As illustrated in the Figure 4b, the main loss of optimality is due to the use of the parametric model (46) which reduces the number of "free parameter" from $N \approx KL$ to $K(L-p)$.

On the one hand, when p is small the loss of power due to the estimation of sample expectation is small as well. Unfortunately, the assumption that multimedia signals can be represented exactly by a sparse linear parametric model hardly holds true in practice. On the other hand, using a less sparse model with a larger p insure a rather accurate representation of multimedia signals. However, this implies a greater loss of power due the loss of more "free parameters".

This point highlights a general problem of all steganalysis



(a) Empirical distributions of likelihood ratio $\ln(\Lambda_1)$, $\ln(\widetilde{\Lambda})$ and $\ln(\widehat{\Lambda})$ under the hypothesis $\mathcal{H}_0$ and $\mathcal{H}_1$.

(b) ROC Curves: power functions β and $\widehat{\beta}$ of the tests δ and $\widehat{\delta}$.

Figure 4: Comparison of proposed tests theoretical (- -) and empirical (—) results obtained from simulated data with relative payload $R = 1$.

methods which use an estimation or a "calibration" process to estimate cover content: a compromise has to be found between a sparse representation (to keep p small) and a good approximation (to avoid error in the estimation of the expectation $\widehat{\boldsymbol{\theta}}_k$). Note that to emphasize the two different factors of loss of power, the GLRT was performed without the noise estimation (so that the only loss of power is due to content estimation). The results obtained with this theoretical GLR is shown in light green line in Figures 4a and 4b

In addition it can be noted that the relative payload R impacts the power function of the proposed GLRT in two different manners. On the one hand, Equation (55) shows that the variance of the GLR tends to decrease as the embedding increases. This phenomenon has a positive effect on the detection performance because a lower variance of the GLR under the hypothesis $\mathcal{H}_1$ increases the power function. On the other hand, the definition of $\widehat{\varrho}$ (52) shows that the mathematical expectation of the GLR does not linearly depend on R. In fact, the estimated mean variance of pixels increases with the payload R. Therefore, the expectation of the GLR increases fewer when the parameters σ_k^2 have to be estimated which causes a loss of power compared to the LRT.

These two phenomena are shown in Figures 4a and 4b. The Figure 4a presents a comparison between the distribution of the LR $\ln(\Lambda)$ and the distribution of the GLR $\ln(\widehat{\Lambda})$. Similarly, Figure 4b shows a comparison between LRT and GLRT power function as a function of false alarm $\beta(\alpha_0)$ (namely, the Receiver Operating Characteristic -ROC- curves). The results presented in the Figure 4b were obtained using 400 blocks of 32 samples which satisfy the polynomial model detailed in Section 6.1. The additive noise follows a zero-mean Gaussian distribution with $\sigma_k = \{0.5\Delta; 2\Delta\}$.

5.3. Comparison with the Weighted-Stego (WS) Image Analysis

In order to highlight the similarity between proposed LR tests and the WS detector [20, 29], let us rewrite the LR $\ln(\widetilde{\Lambda}(\mathbf{Z}))$ defined in Equation (36), as follows:

$$\underbrace{\frac{\bar{\sigma}}{\sqrt{KL}}}_{\text{normalization}} \sum_{k=1}^{K}\sum_{l=1}^{L} \underbrace{\frac{1}{\sigma_{k,l}^2}}_{\text{weights}} \underbrace{(z_{k,l} - \bar{z}_{k,l})}_{\pm 1} \underbrace{(\Delta z_{k,l} - \theta_{k,l})}_{\text{residuals}}. \tag{59}$$

Similarly the GLR $\ln(\widehat{\Lambda}(\mathbf{Z}))$ used in the test $\widehat{\delta}$, see Equation (50), can alternatively be written as follows:

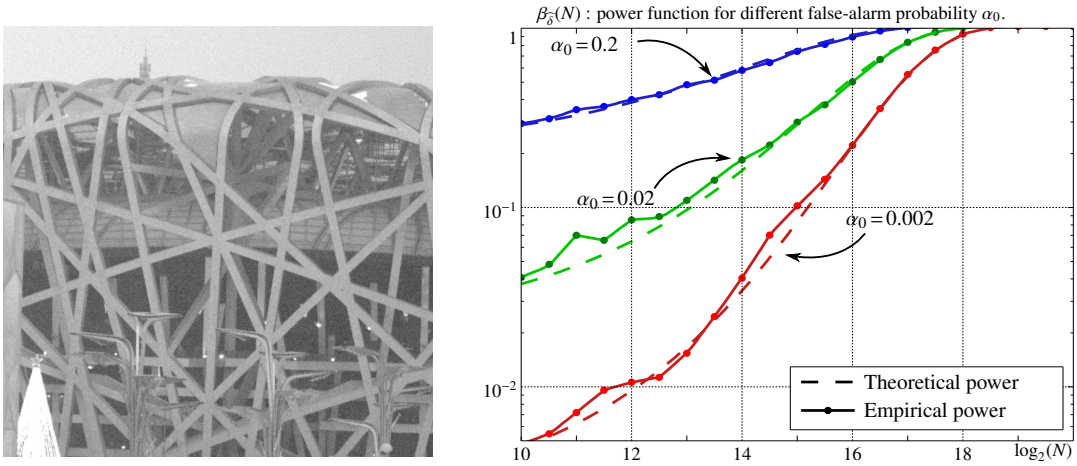
$$\underbrace{\frac{\widehat{\bar{\sigma}}}{\sqrt{K(L-p)}}}_{\text{normalization}} \sum_{k=1}^{K}\sum_{l=1}^{L} \underbrace{\frac{1}{\widehat{\sigma}_k^2}}_{\text{weights}} \underbrace{(z_{k,l} - \bar{z}_{k,l})}_{\pm 1} \underbrace{(\Delta z_{k,l} - \widehat{\theta}_{k,l})}_{\text{residuals}}. \tag{60}$$

These two previous Equations (59) and (60) are very similar to the Weighted Stego-image (WS) detector initially proposed in [20] as an estimator of the relative payload R and later deeply studied in [29]. The estimated payload provided by the WS can be written as follows :

$$\underbrace{w}_{\text{normalization}} \sum_{k=1}^{K}\sum_{l=1}^{L} \underbrace{\frac{1}{w_{k,l}}}_{\text{weights}} \underbrace{(z_{k,l} - \bar{z}_{k,l})}_{\pm 1} \underbrace{(z_{k,l} - \widehat{c}_{k,l})}_{\text{residuals}}. \tag{61}$$

where $\widehat{c}_{k,l}$ is an estimation of cover pixel value based on a local auto-regressive filtering process $\widehat{c}_{k,l} = \mathcal{F}(\mathbf{Z})_{k,l}$ and $w_{k,l} = (\widehat{\sigma}_{k,l}^2 + \alpha)$ is a weight so that the influence of each pixel depends on the variance neighboring pixels. In the case of the WS, the normalization parameter $w = \sum_{k,l} w_{k,l}$ allows us to guarantee that $w \sum_{k,l} {}^1/_{w_{k,l}} = 1$. Different values for α and different filters have been proposed and compared in [29].

In comparison with the WS detector, this paper proposes two major novelties. First, the test is derived from the statistical theory of hypothesis testing (see Section 3). Hence, the weights



(a) Photograph used for the numerical simulations

(b) Power function associated with the GLR test $\widehat{\delta}$ (49) as a function of number of samples N for three different false-alarm probabilities.

Figure 5: Graphical representation of proposed GLR test $\widehat{\delta}$ (49) power function; results obtained from a Monte-Carlo simulation using the natural image 5a and the 2D polynomial model (62) of order $p = 2$ with a block width of $L = 4$ pixels.

$w_{k,l}$ are theoretically established and not heuristically chosen. Besides, the proposed methodology allows us to calculate analytically the statistical properties of proposed tests and proposed estimators. The same methodology can potentially be applied to a wider range of embedding scheme (a first step has been done in the use of proposed statistical methodology for LSB matching detection in [6, 7, 11]).

Second, the estimates $\widehat{c}_{k,l}$ used in the WS (61) are replaced in decision function $\widehat{\Lambda}(\mathbf{Z})$ (50) by the estimates $\widehat{\theta}_{k,l}$, which physically describe the cover image content. It is thus expected that the proposed test has a higher detection performance than the WS and, more important, allows the decision to be taken independently of the expectation of samples considered as a nuisance parameter.

6. Steganalysis Results and Comparisons

6.1. Theoretical Results on Simulated Data

Following the arguments given in [1, 10, 25, 42], it was chosen to represent the expectation of samples —*i.e.* the two dimensional structured image content— by modeling the expectation $\boldsymbol{\theta}$ with a piecewise two-dimensional (2D) polynomial of order p. This model is applied by extracting non-overlapping blocks of $L \times L$ pixels from the inspected image. By denoting the expectation of pixels from the k-th block $\boldsymbol{\theta}_k = \{\theta_{k;l,m}\}$, $l \in \{1, \ldots, L\}$, $m \in \{1, \ldots, L\}$, the 2D polynomial of order p can be written:

$$\theta_{k;l,m} = \sum_{u=0}^{p} \sum_{v=0}^{p} a_{k;l,m} l^u m^v .$$

By putting these blocks in vector of L^2 components denoted $\boldsymbol{\theta}_k$, this model lead to the following parametrization

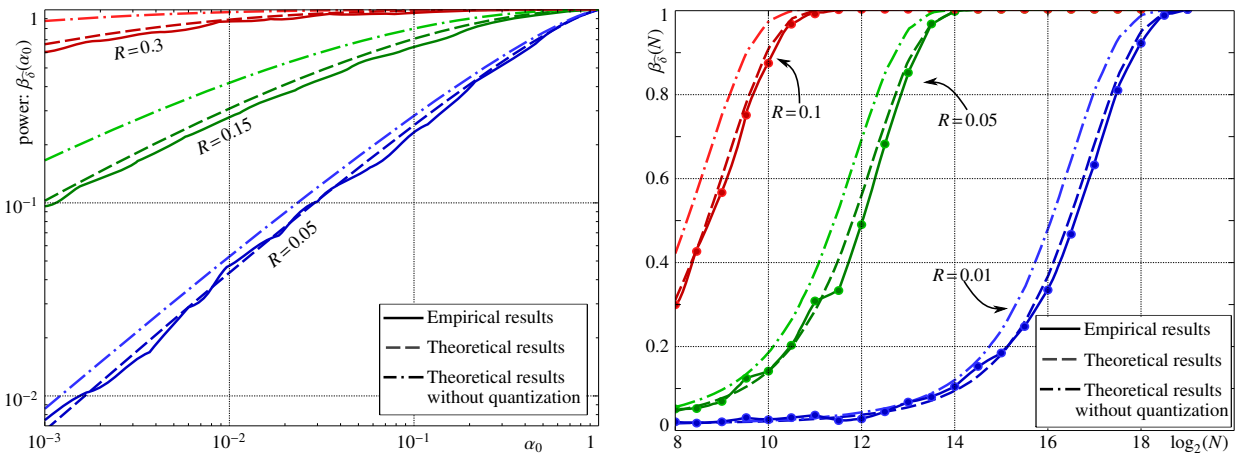
$$\begin{aligned} \boldsymbol{\theta}_k &= \mathbf{H}\mathbf{a}_k, \\ \mathbf{H} &= \left(\mathbf{1}, \mathbf{x}, \mathbf{y}, \mathbf{x}\cdot\mathbf{y}, \mathbf{x}^{\cdot 2}, \mathbf{y}^{\cdot 2}, \mathbf{x}^{\cdot 2}\cdot\mathbf{y}, \ldots, \mathbf{x}^{\cdot p}\cdot\mathbf{y}^{\cdot p}\right) \end{aligned} \tag{62}$$

where $\mathbf{x}\cdot\mathbf{y}$ and $\mathbf{x}^{\cdot n}$ respectively represents the array product and array exponent, made component by component, $\mathbf{1} \in \mathbb{R}^{L^2}$ is a column vector whose elements are ones, $\mathbf{x} \in \mathbb{R}^{L^2}$ and $\mathbf{y} \in \mathbb{R}^{L^2}$ are given by putting into column vectors the following matrices

$$\mathbf{X} = \begin{pmatrix} \frac{1}{L} & \frac{2}{L} & \cdots & \frac{L-1}{L} & 1 \\ \frac{1}{L} & \frac{2}{L} & \cdots & \frac{L-1}{L} & 1 \\ \frac{1}{L} & \frac{2}{L} & \cdots & \frac{L-1}{L} & 1 \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ \frac{1}{L} & \frac{2}{L} & \cdots & \frac{L-1}{L} & 1 \end{pmatrix} \text{ and } \mathbf{Y} = \begin{pmatrix} \frac{1}{L} & \frac{1}{L} & \cdots & \frac{1}{L} \\ \frac{2}{L} & \frac{2}{L} & \cdots & \frac{2}{L} \\ \vdots & \vdots & \vdots & \vdots \\ \frac{L-1}{L} & \frac{L-1}{L} & \cdots & \frac{L-1}{L} \\ 1 & 1 & \cdots & 1 \end{pmatrix}$$

The Figure 5b presents results obtained from a Monte-Carlo simulation with 10^5 realizations of proposed tests using the rather complex natural image shown in the Figure 5a. To model this image, an algebraic 2D-polynomial of order $p = 2$ was used with block width of $L = 4$ pixels. A zero-mean stationary Gaussian noise with $\sigma = 2.6\Delta$ was added to the original image before each simulation; this corresponds to a typical case when quantization step is rather small compared to noise variance. The Figure 5b shows the empirical power function, numerically obtained, as a function of the number of pixel and for some values of prescribed false-alarm probability. The results shown in the Figure 5b emphasizes one of the main advantage of the proposed test, the empirically obtained power function is very close the theoretical expected value given by (42) and (58).

Though this paper focuses on digital images, the proposed methodology can potentially be applied to detect information hidden in any kind of digital media as long as a linear parametric model can represents accurately the expectation of each sample —that is the cover medium content—. To enlarge the application of the proposed GLR test, the Figure 6 presents the results obtained from a Monte-Carlo simulation using an uncompressed WAV sound (a Doppler-record of in-utero baby heartbeat). Because the sound is a one-dimensional signal, a 1D-polynomial was used instead of the 2D-polynomial model (62) (see [9, 8, 50] for details on this model). Due to



(a) Comparison between theoretically established detection performances, as function of false-alarm probability, and empirical results obtained with the proposed GLR test $\widehat{\delta}$ (49).

(b) Comparison between theoretically established detection performances, as function of number of sample for $\alpha_0 = 1 \cdot 10^{-2}$, and empirical results obtained with the proposed GLR test $\widehat{\delta}$ (49).

Figure 6: Illustration of quantization impact on power function of the proposed GLR test $\widehat{\delta}$ (49); results obtained from a Monte Carlo simulation with "babyheart" wav sound and an additive zero-mean stationary Gaussian noise with $\sigma = 0.52$.

the rather simple content of such a sound, the size of blocks was set to $L = 32$ samples and a 1D-polynomial model of order $p = 6$ was used. In this experimentation a stationary Gaussian noise with $\sigma = 0.52\Delta$ was added to explore a case in which quantization impact is far from being negligible. In fact, Figures 5b and 6 together emphasize the accuracy of the established power function when quantization step is negligible (when $\sigma_n \gg \Delta$, Figure 5b) as well as when the quantization is important (when $\sigma_n \ll \Delta$, Figure 6). The Figure 6a shows the power function of the proposed GLRT as a function of false-alarm probability (namely as a ROC curves) for different payloads R. Similarly, the Figure 6b shows the power function of proposed GLRT as a function of samples number and for different payloads R. These results highlight that the power function of proposed GLR test is very close to the theoretically established power, given in the Theorem 4. The Figure 6 also shows that the loss of power due to quantization, precisely given by factor $\widehat{\gamma}_R$ in Equation (55), is rather important in the present case because $\sigma = 0.52\Delta$.

6.2. *Experimental Results on Image Databases and Comparison with State-of-the-art Steganalyzers*

To highlight the relevance of theoretical findings in practice, it was chosen to verify numerically that the proposed detection scheme allows the guaranteeing of a prescribed false-alarm probability. For a large scale verification of these results, it is proposed to use RAW images from BOSS contest database [2]. These images were converted in grayscale 16-bits color depth images using the software *DCRAW* (with command dcraw -j -v -D -4). Finally, non-overlapping images of 512×512 pixels were extracted from each (non-processed) color channel; this allows us to inspect images which all have the same size, and also allows us to increase the number of tested images. Note that it has been chosen to use RAW images (which are not processed at all after acquisition, see [39] for details) because the proposed Gaussian noise model (11) is especially accurate for such images; on the opposite the post-acquisition operations, such as demosaicing, white balancing, gamma correction and JPEG compression, can heavily change the distribution of pixels [46].

The Figure 7 shows a comparison between the empirical false-alarm probability of the proposed test as a function of decision threshold $\widehat{\tau}_{\alpha_0}$ and the theoretical false-alarm probability, calculated from Equation (53). These results were obtained using the 2D-polynomial model of pixels expectations (62) with order $p = 2$ and block width $L = 4$ and $L = 5$ pixels. However, it should be highlighted that some phenomena were omitted from proposed model (for instance quantizer saturation and hot / dead pixels). Therefore, Figure 7 presents two different results for each block width $L = 4$ and $L = 5$ pixels; one obtained by taking into account every pixels, and one by only taking into account the blocks for which the proposed model of both Gaussian noise (11) and 2D-polynomial model (62) holds. The selection of these blocks was made by adapting methodology proposed in [42] to identify blocks which can accurately be modeled by a 2D-polynomial model (62).
It can be noted from Figure 7 that the false-alarm probability of proposed GLRT $\widehat{\delta}$ (49) slightly differs from theoretical results for high detection threshold (typical corresponding to theoretical false-alarm probability of $\alpha_0 = 10^{-3}$). This phenomenon can be explained by the use of the CLT which does not permit us to get very accurate tail distribution of the GLR. Note also that some "outliers" pixels, typically dead and hot pixels, are excluded from this result because they do not follow the proposed Gaussian model.

For comparing the performance of proposed GLRT, there is a wide range of steganalyzers that potentially could be used.
It was chosen to use one of the leading competitors from *struc-*

tural detectors due to their known rather good performance. By using the Regular-Singular detector (RS) [21], the Sample Pair Analysis (SPA) [14] and the SPA Least Square Method (SPA-LSM) [34], it was empirically observed that the RS (with original mask, see [21]) and the SPA-LSM [34] obtained the best performance. Therefore these two steganalyzers were used for comparisons.

It was also tried to use detectors based on decision theory such as the LRT based on i.i.d pixels distributions [13], the χ^2 attack [48] or a recent improvement of this detector, namely the Generalised Category Attack (GCA) [32], and the AUMP test proposed in [8, 9, 16]. Only this last AUMP test exhibits a good detection performance during our experimentation. Hence, only the results of the AUMP test are presented in Figure 10.

Finally, as shown in Section 5.3, the expression of proposed GLR is very similar to Weighted-Stego steganalysis (WS) [20]. In addition the WS steganalysis is known to be one of the most efficient steganalyzers dedicated to LSB replacement. Therefore, the improved WS detector proposed in [29] is included in numerical comparisons.[2]

Note that it was chosen not to include *blind* steganalyzers in comparisons. In fact, the main goal of the present article is to design a test with analytically established properties, in order to guarantee a prescribed false-alarm probability, which seems currently out of reach of any supervised learning based steganalysis method.

It should also be noted that the use of the estimated variance of pixels in the proposed GLRT is difficult; in fact for most images a very small number of pixels have an estimated variance equals to zero, typically in overexposed areas. Hence, it is proposed to insure that each block has a minimal variance of $\widehat{\sigma}_k = 0.1$. The blocks for which estimated variance verify $\widehat{\sigma}_k < 0.1$ were normalized to set their variance to the acceptable minimum. This empirical rule is similar to the weighting coefficients proposed for WS steganalysis in [20, 29], see also the Equation (61), which have been shown to increase the empirical power function.

The Figure 8 shows a comparison of the power function of the chosen detectors as Receiver Operational Characteristics (ROC) curves. Those results are obtained from RAW images of the BOSS database with payload $R = 0.025$. For this image database, the proposed GLRT is used with a 2D-polynomial model of order $p = 2$ and two different block width of $L = 4$ and $L = 5$ pixels. Though a more accurate model of image content might be used instead of the 2D-polynomial (62), the results shown in the Figure 8 clearly shows that proposed GLRT performs much better than the state-of-the-art competitors. Note that Figure 8 also shows the theoretical power function of pro-

[2]The *Matlab* source code of RS, AUMP and WS steganalyzers can be downloaded from the website of the DDE (Digital Data Embedding) Laboratory: http://dde.binghamton.edu/download/

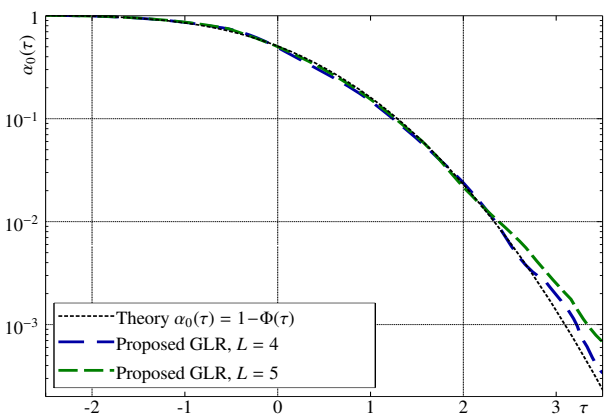


Figure 7: Comparison between theoretical and empirically obtained false-alarm probability α_0 as a function of decision threshold τ_{α_0}; results obtained with RAW images from BOSS database [2].

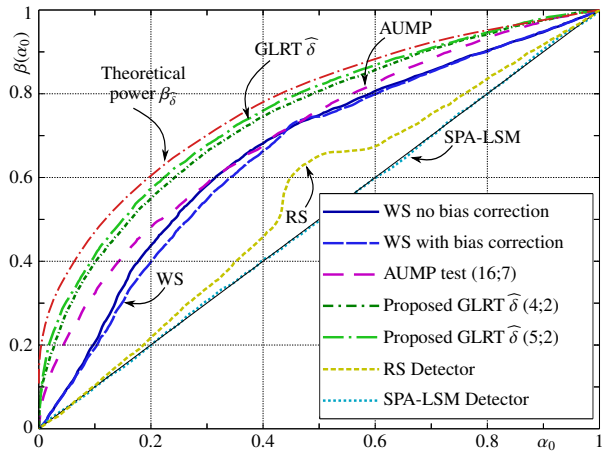


Figure 8: Comparison of the power function of chosen detectors through ROC curves $\beta(\alpha_0)$; results obtained with RAW images from BOSS database [2] for payload $R = 0.025$.

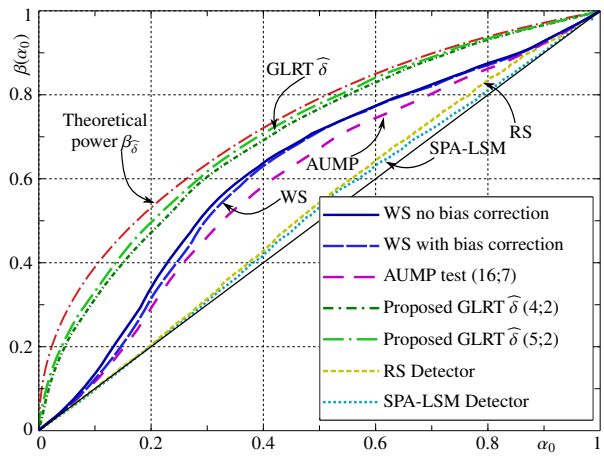
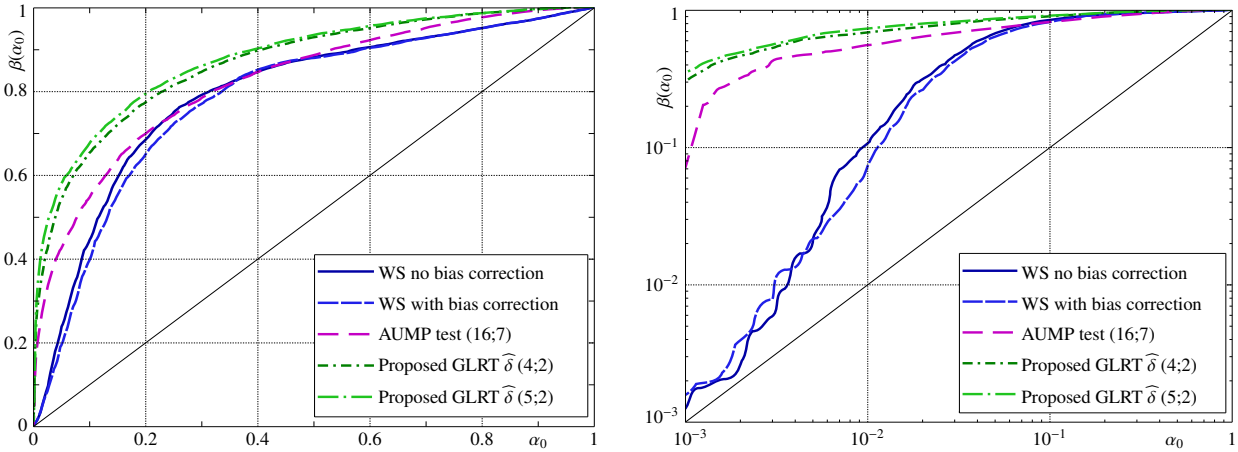


Figure 9: Comparison of the power function of chosen detectors through ROC curves $\beta(\alpha_0)$; results obtained for 8bits RAW images from BOSS database [2] for payload $R = 0.01$.



(a) Comparison of proposed state-of-the-art detectors and proposed GLRT power function through ROC curves for relative payload $R = 0.05$.

(b) Comparison of proposed state-of-the-art detectors and proposed GLRT power function through ROC curves in log-log scale for relative payload $R = 0.10$.

Figure 10: Comparison of the power function of chosen detectors through ROC curves $\beta(\alpha_0)$; results obtained with RAW images from BOSS database [2] for relative payload $R = 0.05$, Figure 10a, and $R = 0.10$, Figure 10b.

posed GLRT obtained from Equation (58) using blocks variance estimation (47) obtained with block width $L = 4$. It can be observed that the power function of the proposed GLRT is very close to the theoretically established power; the small loss of power can be explained by the block variance threshold and by the use of all pixels blocks while, as previously discussed, the Gaussian model might be not very accurate for all of them.

Let us recall that the use of RAW images from BOSS database permits us to obtain results for the case when quantization is rather negligible compared to the noise variance, $\sigma_n \gg \Delta$. Hence, to complete the numerical provided in Figures 10 and 8 numerical results on 8 bit images are provided in the Figure 9. Once again, in the Figure 9, the performance of the different detectors is compared through ROC curves and the same two implementations of the proposed GLR test, with $L = 4$ and $L = 5$, are used. Note that for the case of 8 bit images, a smaller relative payload of $R = 0.01$ because, even though the quantization has a larger impact, the detection is easier when the ratio Δ/σ increases. Finally, it can be noted from the Figure 9 that the proposed GLR test performs better than its competitors. More interestingly, it can also be noted that the AUMP test is outperformed by the WS detector. This is not surprising because the AUMP detector has been designed for the case when Δ/σ tends to 0 which not holds true for 8 bits images.

Figures 10a and 10b present a numerical comparison of the power function of the chosen detectors; those results are obtained using the same RAW images from BOSS contest database [2]. Again, these images are converted in grayscale 16-bits color depth images and all crop to size 512×512 pixels. Results shown in the Figure 10a are obtained with a relative payload $R = 0.05$; this allows us to show that the proposed GLRT still performs much better than its competitors for higher payloads R. Note that, due to their low detection performance and for a better readability, it has been chosen to remove the RS and SPA-LSM detectors from Figures 10a and 10b.

Similarly, the Figure 10b shows the power function of the same steganalyzers for relative payload $R = 0.10$. The use of a log-log scale allows us to show that for very small false-alarm probability, the WS (with our without bias correction) performs much worse that the other detectors. On the opposite, the AUMP test performs rather well for small false-alarm probability but still has a much lower power function than the proposed GLRT. This phenomenon can be explained by the fact that AUMP test is based on a rather simplistic 1D model of natural image content which is not very accurate for large segment size (while the author of [16] suggest a segment size of 16 pixels). In fact, even though the AUMP detector is relevant for 16 bits images, the error of modeling caused by such a naive model largely impacts this detector for a small set of images.

7. Conclusions

This paper is a first step made to apply hypothesis testing theory for the detection of hidden information. The problem of detecting hidden information in the LSB of quantized samples is formally stated and studied with the three following goals. First, taking carefully into account quantization impact, the most powerful LR test is designed in the ideal settings of known samples distributions. The statistical properties of this test are analytically established. This test serves as an upper bound for the power function one can expect from any detector and highlights the significant impact that the quantization of samples might have. Second, the content of inspected medium is explicitly considered as a nuisance parameter modeled by a piecewise linear parametric model. Finally, in a practical context of hidden data detection, it is very important to provide the proposed test with a guaranteed false-alarm probability. Hence, thanks to the precise study of quantization impact and to the linear parametric image model, the statistical properties of the proposed GLR test are asymptotically established. This allows the guaranteeing of a false-alarm probability and to show that

the loss of optimality, compare to the optimal LRT, is small.
Focusing on digital images, it is shown that the proposed test is close to the well-known Weighted Stego (WS) detector. Numerical results on a large image database show the relevance of the presented approach to guarantee a false-alarm probability and to detect hidden data with a higher power function than state-of-the-art steganalyzers.
A possible future work, which is out of the scope of this paper, is the exploitation of a more accurate image model. Natural images are usually preferred media for information hiding and the use of a specific model which takes into account properties of images is expected to increase the performance of the proposed test. Similarly, the proposed methodology, based on hypothesis theory, could be applied to detect other information hiding schemes by designing tests with known statistical properties.

Appendix A. Proof of Minimal INR for Homoscedastic Cover

For readability, it is proposed to sketch a proof of remark 2 first; the next appendices are devoted to the study of LR and GLR statistical study and demonstration of proposed theorems. In Remark 2 it is stated that the heteroscedastic properties helps the steganalyzer in the sense that for a given payload R, and for a given quantization step Δ, the INR ϱ (39) is minimal when all the samples have the same variance (43):

$$\bar{\sigma}^2 \leq \frac{1}{N}\sum_{n=1}^{N}\sigma_n^2\left(1+\frac{\Delta^2}{12\sigma_n^2}\right)$$
$$\Leftrightarrow \frac{1}{\bar{\sigma}^2} \leq N\left(\sum_{n=1}^{N}\sigma_n^2\left(1+\frac{\Delta^2}{12\sigma_n^2}\right)\right)^{-1}. \tag{A.1}$$

By using the definition of $\bar{\sigma}$ (35) the above equation becomes:

$$\frac{1}{\bar{\sigma}^2} \overset{\text{def.}}{=} \frac{1}{N}\sum_{n=1}^{N}\left[\sigma_n^2\left(1+\frac{\Delta^2}{12\sigma_n^2}\right)\right]^{-1}.$$

For readability, let us define:

$$s_n = \sigma_n^2\left(1+\frac{\Delta^2}{12\sigma_n^2}\right) \geq 0\,,$$

in order to rewrite Equation (A.1) as:

$$\frac{1}{N}\sum_{n=1}^{N}s_n^{-1} \leq N\left(\sum_{n=1}^{N}s_n\right)^{-1} \Leftrightarrow \left(\sum_{n=1}^{N}s_n^{-1}\right)\left(\sum_{n=1}^{N}s_n\right) \leq N^2.$$

Let us define $\mathbf{s} = (s_1, \ldots, s_n)$ and $f(\mathbf{s}) = \left(\sum_{n=1}^{N}s_n^{-2}\right)\left(\sum_{n=1}^{N}s_n^{2}\right)$; by solving $\frac{\partial f(\mathbf{s})}{\partial s_n} = 0$ one has:

$$\begin{cases} \sum_{j=2}^{N}s_j + \left(\sum_{j=2}^{N}s_j^{-1}\right)^{-1} = s_1, \\ \ldots \\ \sum_{j\neq n}s_j + \left(\sum_{j\neq n}s_j^{-1}\right)^{-1} = s_n, \\ \ldots \\ \sum_{j=1}^{N-1}s_j + \left(\sum_{j=1}^{N-1}s_j^{-1}\right)^{-1} = s_N. \end{cases}$$

Solving these equations lead to find that $f(\mathbf{s})$ admits a minimum of N^2 which is reached when $s_1 = s_2 = \ldots = s_n$, which ends the proof of the Remark 2.

Appendix B. Calculation of the Moments of $\ln(\Lambda_1(z_n))$

The main goal of this appendix is to provide a demonstration of Proposition 1 and Theorems 3 and 4. These proof are divided in three steps. First, the Appendix B provides a detailed calculation of the moments $\ln(\Lambda_1(z_n))$. Then, the Appendix C provides a demonstration of Proposition 1. Eventually, the demonstrations of Theorems 3 and 4 are detailed in the Appendix C.2.

Let us remind the expression (18) of the LR $\ln(\Lambda_1(z_n))$ (9):

$$\ln(\Lambda_1(z_n)) = \frac{\Delta(z_n-\bar{z}_n)(\Delta z_n-\theta_n)}{2\sigma_n^2} - \frac{\Delta^2}{8\sigma_n^2} + o_p\left(\frac{\Delta^2}{\sigma_n^4}\right).$$

Neglecting the term $o(\Delta^2/\sigma_n^4)$, it obviously suffices to calculate the moments of the term $(z_n-\bar{z}_n)(\Delta z_n-\theta_n)$ as $\Delta/2\sigma_n^2$ is a constant "scale factor".
under the hypothesis $\mathcal{H}_0$, one has $\mu_0 = -\frac{\Delta^2}{8\sigma_n^2} + \frac{\Delta m_0(\theta_n)}{2\sigma_n^2}$, where

$$\begin{aligned} m_0 &= m_0(\theta_n) = \mathbb{E}_{\mathcal{H}_0}\left[(\Delta z_n-\theta_n)(z_n-\bar{z}_n)\right] \\ &= \sum_{k\in\mathcal{Z}}\frac{\Delta(2k+1)-\theta_n}{\sigma_n}\int_{\Delta(2k+\frac{1}{2})}^{\Delta(2k+\frac{3}{2})}\phi\left(\frac{x-\theta_n}{\sigma_n}\right)dx \\ &\quad -\sum_{k\in\mathcal{Z}}\frac{2k\Delta-\theta_n}{\sigma_n}\int_{\Delta(2k-\frac{1}{2})}^{\Delta(2k+\frac{1}{2})}\phi\left(\frac{x-\theta_n}{\sigma_n}\right)dx. \end{aligned} \tag{B.1}$$

Similarly, denoting that $\forall z_n \in \mathcal{Z}$, $(z_n-\bar{z}_n)^2 = 1$, the variance σ_0^2 is given by:

$$\begin{aligned} \sigma_0^2 &\overset{\text{def.}}{=} \mathbb{E}_{\mathcal{H}_0}\left[\ln(\Lambda_1(z_n))^2\right] - \mu_0^2 \\ &= \frac{\Delta^2}{4\sigma_n^4}\mathbb{E}_{\mathcal{H}_0}\left[(\Delta z_n-\theta)^2 - \frac{\Delta}{2}(\Delta z_n-\theta)(z_n-\bar{z}_n) + \frac{\Delta^2}{16}\right] \\ &- \frac{\Delta^4}{8^2\sigma_n^4} - \frac{\Delta^2 m_0^2}{4\sigma_n^4} + \frac{\Delta^3 m_0}{8\sigma_n^4} \\ &= \frac{\Delta^2}{4\sigma_n^4}\left(\mathbb{E}_{\mathcal{H}_0}[(\Delta z_n-\theta_n)^2] - m_0^2\right) \\ &= \frac{\Delta^2}{4\sigma_n^4}\left(-m_0^2 + \sum_{k\in\mathcal{Z}}\frac{(k\Delta-\theta_n)^2}{\sigma_n}\int_{\Delta(k-\frac{1}{2})}^{\Delta(k+\frac{1}{2})}\phi\left(\frac{x-\theta_n}{\sigma_n}\right)dx\right). \end{aligned}$$

The expectation μ_1 can easily be calculated with assumption A-1, that hidden stego-bits $\{0; 1\}$ are uniformly distributed, which gives from (18):

$$\begin{aligned} &\mathbb{E}_{\mathcal{H}_1}[(\Delta z_n-\theta_n)(z_n-\bar{z}_n)] \\ &= \frac{1}{2}\mathbb{E}_{\mathcal{H}_1}[\Delta z_n-\theta_n|z_n-\bar{z}_n=1] - \frac{1}{2}\mathbb{E}_{\mathcal{H}_1}[\Delta z_n-\theta_n|z_n-\bar{z}_n=-1] \\ &= \frac{1}{2}\mathbb{E}_{\mathcal{H}_0}[\Delta z_n-\theta_n] + \frac{1}{4}\left(\mathbb{E}_{\mathcal{H}_0}[\Delta z_n-\theta_n+\Delta] - \mathbb{E}_{\mathcal{H}_0}[z_n-\theta_n-\Delta]\right) \\ &= \frac{\Delta}{2}. \end{aligned} \tag{B.2}$$

From which one gets the result (22) :

$$\mu_1 = -\frac{\Delta^2}{8\sigma_n^2} + \frac{\Delta^2}{4\sigma_n^2} = \frac{\Delta^2}{8\sigma_n^2}.$$

Eventually, the variance σ_1^2 can be calculated by denoting that $\forall z_n \in \mathcal{Z}$, $(z_n - \bar{z}_n)^2 = 1$ as follows:

$$\begin{aligned}\sigma_1^2 &\stackrel{\text{def.}}{=} \mathbb{E}_{\mathcal{H}_1}\left[\ln\left(\Lambda_1(z_n)\right)^2\right] - \mu_1^2 \\ &= \frac{\Delta^2}{4\sigma_n^4}\mathbb{E}_{\mathcal{H}_1}\left[(\Delta z_n - \theta)^2 - \frac{\Delta}{2}(\Delta z_n - \theta)(z_n - \bar{z}_n) + \frac{\Delta^2}{16}\right] - \frac{\Delta^4}{8^2\sigma_n^2},\end{aligned}$$

where

$$\begin{aligned}&\mathbb{E}_{\mathcal{H}_1}\left[(\Delta z_n - \theta_n)^2\right] = \frac{1}{2}\mathbb{E}_{\mathcal{H}_0}\left[(\Delta z_n - \theta_n)^2\right] \\ &+ \frac{1}{4}\left(\mathbb{E}_{\mathcal{H}_0}\left[(\Delta z_n - \theta_n - \Delta)^2\right] - \mathbb{E}_{\mathcal{H}_0}\left[(\Delta z_n - \theta_n + \Delta)^2\right]\right) \\ &= \mathbb{E}_{\mathcal{H}_0}\left[(\Delta z_n - \theta_n)^2\right] + \frac{\Delta^2}{2},\end{aligned}$$

which, together with (B.2), permits the writing of:

$$\sigma_1^2 = \frac{\Delta^2}{4\sigma_n^4}\left(\mathbb{E}_{\mathcal{H}_0}\left[(\Delta z_n - \theta_n)^2\right] + \frac{\Delta^2}{4}\right). \tag{B.3}$$

Appendix C. Demonstration of Theorems 3 and 4.

The proof of the Theorems 3 and 4 is divided in three steps. First, the Appendix C.1 proves the results from Proposition 1. Then the Appendix C.2 establishes the asymptotic distribution of LR $\ln\left(\widetilde{\Lambda}(\mathbf{Z})\right)$. Finally the demonstration of Theorems 3 and 4 are given in the Appendix C.3.

Appendix C.1. Moments of the LR $\ln\left(\widehat{\Lambda}(\mathbf{Z})\right)$ for non-i.i.d. Samples

Reminding that the quantizer saturation effects are neglected in this paper, it can be noted, from Equation (B.1), that $m_0(\theta_n) = -m_0(\theta_n + \Delta)$. Reminding that ζ_n is defined as follows $\zeta_n \in [-\Delta; \Delta]$, $\zeta_n = \theta_n - Q_{2\Delta}(\theta_n)$ and that N_{x_0,x_1}, $x_0 < x_1$, $\{n, \zeta_n \in [x_0, x_1]\}$, represents the number of samples which verify $\zeta_n \in [x_0; x_1]$. It follows from the parity properties of $m_0(\zeta_n)$ and Riemann theorem that:

$$\lim_{C\to\infty} h\sum_{c=1}^{C} m_0(-\Delta + ch)N_{(c-1)h,ch} = \int_{-\Delta}^{\Delta} m_0(\zeta_n)d\zeta_n = 0.$$

with $h = \frac{2\Delta}{C}$. Hence, when the observed samples are not i.i.d and assumption A-3 holds, the mean expectation of LR, see Equation (27) is given under $\mathcal{H}_0$ by:

$$\begin{aligned}\widetilde{\mu}_0 &= \lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N}\mathbb{E}_{\mathcal{H}_0}\left[\ln(\Lambda_1(z_n))\right], \\ &\lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N} -\frac{\Delta^2}{8\sigma_n^2} + m_0(\theta_n), \\ &-\sum_{n=1}^{N}\frac{\Delta^2}{8\sigma_n^2} + 2\Delta\int_{-\Delta}^{\Delta} m_0(\zeta_n)d\zeta_n = -\sum_{n=1}^{N}\frac{\Delta^2}{8\sigma_n^2}.\end{aligned} \tag{C.1}$$

In a similar fashion, it and Equation (23) that using assumption A-3:

$$\begin{aligned}\widetilde{\sigma}_0^2 &= \lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N}\mathbb{V}ar_{\mathcal{H}_0}\left[\ln(\Lambda_1(z_n))\right], \\ &\lim_{N\to\infty}\frac{1}{N}\frac{\Delta^2}{4\sigma_n^4}\left(\mathbb{E}_{\mathcal{H}_0}[(\Delta z_n - \theta_n)^2] - m_0^2\right).\end{aligned}$$

Taking into account assumption A-3 allows us to establish [44, 49]:

$$\lim_{N\to\infty}\frac{1}{N}\left(\mathbb{E}_{\mathcal{H}_0}[(\Delta z_n - \theta_n)^2]\right) = \sum_{n=1}^{N}\sigma_n^2\left(1 + \frac{\Delta^2}{12\bar{\sigma}^2}\right),$$

while on the other hand the term:

$$\lim_{N\to\infty}\frac{2\Delta}{N}\sum_{n=1}^{N} m_0(\zeta_n)^2 = \int_{-\Delta}^{\Delta} m_0(\zeta_n)^2 = o\left(\frac{\Delta^2}{\bar{\sigma}^2}\right).$$

Under the hypothesis $\mathcal{H}_1$, Equation (B.2) clearly shows that μ_1 does not depend on θ_n; it immediately follows from definition (35) of the "simplified" LR $\ln\left(\widetilde{\Lambda}_1(z_n)\right)$ that:

$$\widetilde{\mu}_1 = \sum_{n=1}^{N}\frac{\Delta^2}{8\sigma_n^2}. \tag{C.2}$$

Finally, the variance $\widetilde{\sigma}_1^2$ can be immediately deduced from Equation (23) and (B.3) that:

$$\begin{aligned}\widetilde{\sigma}_1^2 &= \lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N}\frac{\Delta^2}{4\sigma_n^4}\left(\mathbb{E}_{\mathcal{H}_0}\left[(\Delta z_n - \theta_n)^2\right] + \frac{\Delta^2}{4}\right) \\ &= \sum_{n=1}^{N}\frac{\Delta^2}{4\sigma_n^2}\left(1 + \frac{\Delta^2}{12\sigma_n^2}\right) + o\left(\frac{\Delta^4}{\bar{\sigma}^4}\right).\end{aligned} \tag{C.3}$$

Appendix C.2. Asymptotic Distribution of the LR $\ln\left(\Lambda_1(\mathbf{Z})\right)$.

From results of the Appendix C, it immediately follows from the law of total expectation that for any payload $R \in]0; 1]$ the expectation of $\ln\left(\Lambda_1(z_n)\right)$ is given by:

$$\widetilde{\mu}_R = (1 - R)\widetilde{\mu}_0 + R\widetilde{\mu}_1 = \frac{1}{N}\sum_{n=1}^{N}\frac{\Delta^2(2R - 1)}{8\sigma_n^2}. \tag{C.4}$$

Likewise, the law of total variance permits the writing of:

$$\begin{aligned}\widetilde{\sigma}_R^2 &= (1 - R)(\widetilde{\mu}_0^2 + \widetilde{\sigma}_0^2) + R(\widetilde{\mu}_1^2 + \widetilde{\sigma}_1^2) - \left((1 - R)\widetilde{\mu}_0 + R\widetilde{\mu}_1\right)^2 \\ &= \frac{1}{N}\sum_{n=1}^{N}\frac{\Delta^2}{4\sigma_n^2}\left(1 + \frac{\Delta^2}{4\sigma_n^2}(2R - R^2) + \frac{\Delta^2}{12\sigma_n^2}\right) + o\left(\frac{\Delta^4}{\bar{\sigma}^4}\right).\end{aligned} \tag{C.5}$$

Reminding that the "simplified" LR $\ln\left(\widetilde{\Lambda}(\mathbf{Z})\right)$ is defined as (36):

$$\begin{aligned}\ln\left(\widetilde{\Lambda}(\mathbf{Z})\right) &\stackrel{\text{def.}}{=} \frac{\Delta\bar{\sigma}}{\sqrt{N}}\sum_{n=1}^{N}\frac{(z_n - \bar{z}_n)(\Delta z_n - \theta_n)}{\sigma_n^2(1 + {}^{\Delta^2}/_{12\sigma_n^2})} \\ &= \frac{2\bar{\sigma}}{\sqrt{N}}\sum_{n=1}^{N}\frac{\left[\ln\left(\Lambda_1(\mathbf{Z})\right) - \widetilde{\mu}_0\right]}{(1 + {}^{\Delta^2}/_{12\sigma_n^2})}.\end{aligned}$$

It immediately follows from the previous results (C.1) - (C.5) that the moments of $\ln\left(\widetilde{\Lambda}(\mathbf{Z})\right)$ are given by:

$$\begin{aligned}\mathbb{E}_{\mathcal{H}_0}\left[\ln\left(\widetilde{\Lambda}(\mathbf{Z})\right)\right] &= 0 \\ \mathbb{V}ar_{\mathcal{H}_0}\left[\ln\left(\widetilde{\Lambda}(\mathbf{Z})\right)\right] &= \left[\sigma_n^2\left(1 + \tfrac{\Delta^2}{12\sigma_n^2}\right)\right]^{-1} \\ \mathbb{E}_{\mathcal{H}_R}\left[\ln\left(\widetilde{\Lambda}(\mathbf{Z})\right)\right] &= \tfrac{R\Delta}{2}\left[\sigma_n^2\left(1 + \tfrac{\Delta^2}{12\sigma_n^2}\right)\right]^{-1} \\ \mathbb{V}ar_{\mathcal{H}_R}\left[\ln\left(\widetilde{\Lambda}(\mathbf{Z})\right)\right] &= \left[\sigma_n^2\left(1 + \tfrac{\Delta^2}{12\sigma_n^2}\right)\right]^{-1} \\ &+ \left[\sigma_n^2\left(1 + \tfrac{\Delta^2}{12\sigma_n^2}\right)\right]^{-2}\tfrac{\Delta^2}{4}(2R - R^2).\end{aligned} \tag{C.6}$$

Finally, from the definition of $\bar{\sigma}$ (35):

$$\frac{1}{\bar{\sigma}^2} \stackrel{\text{def.}}{=} \frac{1}{N}\sum_{n=1}^{N}\left[\sigma_n^2\left(1+\frac{\Delta^2}{12\sigma_n^2}\right)\right]^{-1},$$

and Lindeberg's CLT (19) it holds that under assumption A-3, one has:

$$\begin{cases} \frac{\bar{\sigma}}{\sqrt{N}}\sum_{n=1}^{N}\ln\left(\widetilde{\Lambda}(z_n)\right) \rightsquigarrow \mathcal{N}(0\,;\,1) & \text{under} \quad \mathcal{H}_0 \\ \frac{\bar{\sigma}}{\sqrt{N}}\sum_{n=1}^{N}\ln\left(\widetilde{\Lambda}(z_n)\right) \rightsquigarrow \mathcal{N}(\sqrt{N}\frac{R\Delta}{2\bar{\sigma}}\,;\,1+\gamma_R) & \text{under} \quad \mathcal{H}_1, \end{cases} \tag{C.7}$$

where γ_R is given in (38) and from (39) $\sqrt{N}\frac{R\Delta}{2\bar{\sigma}} = \varrho$.

Appendix C.3. Demonstration of Theorems 3 and 4.

It follows from Equation (C.7), that for a given decision threshold τ the probability that under null hypothesis $\mathcal{H}_0$ the LR $\ln\left(\widetilde{\Lambda}(\mathbf{Z})\right)$ exceeds τ is given by:

$$\alpha_0(\tau) = 1 - \Phi(\tau),$$

using the Gaussian inverse cumulative distribution function $\Phi^{-1}(\cdot)$ it follows that the decision threshold τ_{α_0} which asymptotically, as N tends to ∞, that $\widetilde{\delta} \in \mathcal{K}_{\alpha_0}$ is given by:

$$\widetilde{\tau}_{\alpha_0} = \Phi^{-1}(1-\alpha_0).$$

This ends the demonstration of the Theorem 3.

Similarly, for a given decision threshold τ the probability that under the hypothesis $\mathcal{H}_R$ the LR $\ln\left(\widetilde{\Lambda}(\mathbf{Z})\right)$ exceeds τ is given by:

$$\beta(\tau) = 1 - \Phi\left(\frac{\tau-\varrho}{\sqrt{1+\gamma_R}}\right).$$

Replacing the decision threshold τ with the value $\widetilde{\tau}_{\alpha_0}$ one has

$$\beta_{\widetilde{\delta}} = 1 - \Phi\left(\frac{\Phi^{-1}(1-\alpha_0)-\varrho}{\sqrt{1+\gamma_R}}\right),$$

which ends the demonstration of the Theorem 4.

Appendix D. Demonstration of Theorem 5 and 6

The demonstration of Theorem 5 and 6 is divided in two steps. First, the Appendix D.1 to study the properties of ML estimations $\widehat{\boldsymbol{\theta}}_k$ and $\widehat{\sigma}_k^2$ and then establishes the asymptotic distribution of proposed GLR $\ln\left(\widehat{\Lambda}(\mathbf{Z})\right)$. Then, the demonstration of Theorems 5 and 6 are given in the Appendix D.2.

Appendix D.1. Asymptotic Distribution of GLR $\ln\left(\widehat{\Lambda}(\mathbf{Z})\right)$.

Let us first recall that the observations $\mathbf{z}_k$ are defined as $\mathbf{z}_k = Q_\Delta(\mathbf{y}_k)$ with $\mathbf{y}_k \sim \mathcal{N}(\mathbf{H}\mathbf{a}_k, \sigma_k^2\mathbf{I})$. It is well-known that if $\mathbf{y}_k \sim \mathcal{N}(\mathbf{H}\mathbf{a}_k, \sigma_k^2\mathbf{I})$ then the ML estimators of the expectation $\boldsymbol{\theta}_k = \mathbf{H}\mathbf{a}_k$ and variance σ_k^2 are:

$$\begin{aligned} \widehat{\boldsymbol{\theta}}_k &= \mathbf{P}_H\,\mathbf{y}_k \;\text{ with }\; \mathbf{P}_H = \mathbf{H}\left(\mathbf{H}^T\mathbf{H}\right)^{-1}\mathbf{H}^T, \\ \widehat{\sigma}_k^2 &= \frac{\Delta^2}{L-p}\left|\mathbf{P}_H^\perp\,\mathbf{y}_k\right|_2^2 \;\text{ with }\; \mathbf{P}_H^\perp = \mathbf{I}_L - \mathbf{P}_H. \end{aligned}$$

In addition, under the hypothesis $\mathcal{H}_0$ if $\mathbf{y}_k \sim \mathcal{N}(\mathbf{H}\mathbf{a}_k, \sigma_k^2\mathbf{I})$, then it holds true that:

$$\sum_{l=1}^{L} y_{k,l} - \widehat{\theta}_{k,l} \sim \mathcal{N}\left(0, \sigma_k^2\text{trace}(\mathbf{P}_H^\perp)\right) \;\text{ and }\; \frac{\|\mathbf{P}_H^\perp\,\mathbf{y}_k\|_2^2}{\sigma_k^2} \sim \chi^2_{L-p},$$

where $\text{trace}(\mathbf{P}_H^\perp) = L-p$ and χ^2_{L-p} represents the (central) chi-squared distribution with $L-p$ degree of freedom. Hence the ML estimators verify:

$$\widehat{\sigma}_k^2 = \frac{\Delta^2}{L-p}\left|\mathbf{P}_H^\perp\,\mathbf{y}_k\right|_2^2 \sim \Gamma\left(\frac{L-p}{2}, \frac{2\sigma_k^2}{L-p}\right),$$

where $\Gamma(k,\theta)$ represents the gamma distribution with shape parameter k and scale parameters θ.

However, the observations $\mathbf{z}_k = Q_\Delta(\mathbf{y}_k)$ are quantized in practice. In such a situation, the exact distributions of expectation $\widehat{\boldsymbol{\theta}}_k$ and variance $\widehat{\sigma}_k^2$ are difficult to establish. Nevertheless, it can be shown [44, 49] that the two first moments of those distributions are given, under assumption A-3, by:

$$\mathbb{E}_{\mathcal{H}_0}\left[\sum_{l=1}^{L} z_{k,l} - \widehat{\theta}_{k,l}\right] = 0; \quad \mathbb{V}ar_{\mathcal{H}_0}\left[\sum_{l=1}^{L} z_{k,l} - \widehat{\theta}_{k,l}\right] = \sigma_k^2 + \frac{\Delta^2}{12};$$

$$\mathbb{E}_{\mathcal{H}_0}\left[\widehat{\sigma}_k^2\right] = \sigma_k^2 + \frac{\Delta^2}{12}; \quad \mathbb{V}ar_{\mathcal{H}_0}\left[\widehat{\sigma}_k^2\right] = \frac{2}{L-p}\sigma_k^4 + \frac{\Delta^2}{12}.$$

Therefore it immediately follows from the Delta method [33, Theorem 11.2.14] that under the hypothesis $\mathcal{H}_0$:

$$\begin{aligned} \mathbb{E}_{\mathcal{H}_0}\left[\sum_{l=1}^{L}\frac{z_{k,l}-\widehat{\theta}_{k,l}}{\widehat{\sigma}_k}\right] &= 0; \\ \mathbb{V}ar_{\mathcal{H}_0}\left[\sum_{l=1}^{L}\frac{z_{k,l}-\widehat{\theta}_{k,l}}{\widehat{\sigma}_k}\right] &= \frac{L-p}{\sigma_k^2+\frac{\Delta^2}{12}}. \end{aligned}$$

Hence it finally follows from the previous calculations (C.1)-(C.3), from the definition of $\widehat{\bar{\sigma}}$ (51):

$$\frac{1}{\widehat{\bar{\sigma}}^2} = \frac{1}{K}\sum_{k=1}^{K}\frac{1}{\widehat{\sigma}_k^2}.$$

and from Slutsky's Theorem [33, Theorem 11.2.11] that under the hypothesis $\mathcal{H}_0$:

$$\ln\left(\widehat{\Lambda}(\mathbf{Z})\right) = \frac{\widehat{\bar{\sigma}}}{\sqrt{K}}\sum_{k=1}^{K}\ln\left(\widehat{\Lambda}(\mathbf{z}_k)\right) \sim \mathcal{N}(0;1). \tag{D.1}$$

On the opposite, under the hypothesis $\mathcal{H}_1$, the two first moments of estimated expectation $\widehat{\boldsymbol{\theta}}_k$ and variance $\widehat{\sigma}_k^2$ are given by:

$$\begin{aligned} \mathbb{E}_{\mathcal{H}_R}\left[\sum_{l=1}^{L} z_{k,l} - \widehat{\theta}_{k,l}\right] &= 0; \\ \mathbb{V}ar_{\mathcal{H}_0}\left[\sum_{l=1}^{L} z_{k,l} - \widehat{\theta}_{k,l}\right] &= \sigma_k^2 + \frac{\Delta^2}{12} + \frac{R\Delta^2}{2}; \\ \mathbb{E}_{\mathcal{H}_R}\left[\widehat{\sigma}_k^2\right] &= \sigma_k^2 + \frac{\Delta^2}{12} + \frac{R\Delta^2}{12}; \\ \mathbb{V}ar_{\mathcal{H}_0}\left[\widehat{\sigma}_k^2\right] &= \frac{2}{L-p}\sigma_k^4 + \frac{\Delta^2}{12} + \frac{R\Delta^2}{2}. \end{aligned}$$

Therefore it immediately follows from the Delta method [33, Theorem 11.2.14] that under the hypothesis $\mathcal{H}_1$:

$$\mathbb{E}_{\mathcal{H}_0}\left[\sum_{l=1}^{L}\frac{z_{k,l}-\widehat{\theta}_{k,l}}{\widehat{\sigma}_k}\right] = 0;$$
$$\mathbb{V}ar_{\mathcal{H}_0}\left[\sum_{l=1}^{L}\frac{z_{k,l}-\widehat{\theta}_{k,l}}{\widehat{\sigma}_k}\right] = \frac{L-p}{\sigma_k^2+\frac{\Delta^2}{12}+\frac{R\Delta^2}{2}}.$$

Hence it finally follows from the previous calculations (C.1)-(C.3), from the definition of $\widehat{\widetilde{\sigma}}$ (51) and from Slutsky's Theorem that under the hypothesis $\mathcal{H}_1$:

$$\ln\left(\widehat{\Lambda}(\mathbf{Z})\right) = \frac{\widehat{\widetilde{\sigma}}}{\sqrt{K}}\sum_{k=1}^{K}\ln\left(\widehat{\Lambda}(\mathbf{z}_k)\right) \sim \mathcal{N}(\widehat{\varrho}; 1-\widehat{\gamma}_R). \tag{D.2}$$

where $\widehat{\varrho}$ and $\widehat{\gamma}_R$ are respectively defined in Equations (52) and (56).

Appendix D.2. Demonstration of Theorems 5 and 6.

The demonstration of Theorems 5 and 6 immediately follows from the results (D.1) and (D.2). First, from the asymptotic distribution of $\ln\left(\widehat{\Lambda}(\mathbf{Z})\right)$, given in Equation (D.1) it immediately follows that for any prescribed false-alarm probability α_0, the decision threshold given by:

$$\tau_{\alpha_0} = \Phi^{-1}(1-\alpha_0), \tag{D.3}$$

asymptotically guarantees that $\mathbb{P}_{\mathcal{H}_0}\left[\ln\left(\widehat{\Lambda}(\mathbf{Z})\right) > \tau_{\alpha_0}\right] = \alpha_0$. The result (D.3) is straightforward using the proof of Theorem 1 and proves the Theorem 5.

Then, using the decision threshold given in Equation (D.3), it follows from the properties of Gaussian random variables that the power function of the GLRT $\widehat{\delta}(\mathbf{Z})$, defined in Equation (49), is given by:

$$\beta_{\widehat{\delta}} = 1-\Phi\left(\frac{\Phi^{-1}(1-\alpha_0)-\widehat{\varrho}}{\sqrt{1+\widehat{\gamma}_R}}\right), \tag{D.4}$$

which ends the proof of the Theorem 6.

References

[1] J. Astola, K. Egiazarian, V. Katkovnik, Local Approximation Techniques in Signal and Image Processing, volume PM157, SPIE Press, Monograph, 2006.

[2] P. Bas, T. Filler, T. Pevný, "Break our steganographic system"–The ins and outs of organizing boss, in: Information Hiding, volume 6958 of *Lecture Notes in Computer Science*, Springer Berlin Heidelberg, 2011, pp. 59–70.

[3] P. Billingsley, Probability and Measure, Wiley-Interscience, 3rd edition, 1995.

[4] R. Böhme, Advanced Statistical Steganalysis, Springer Publishing Company, 1st edition, 2010.

[5] G. Cancelli, G. Doërr, M. Barni, I.J. Cox, A comparative study of ±1 steganalyzers, in: Multimedia Signal Processing, IEEE 10th Workshop on, 2008, pp. 791–796.

[6] R. Cogranne, F. Retraint, Application of hypothesis testing theory for optimal detection of LSB matching data hiding, Signal Processing, Elsevier 93 (2013) 1724 – 1737.

[7] R. Cogranne, F. Retraint, An asymptotically uniformly most powerful test for LSB matching detection, Information Forensics and Security, IEEE Transactions on 8 (2013) 464–476.

[8] R. Cogranne, C. Zitzmann, L. Fillatre, I. Nikiforov, F. Retraint, P. Cornu, Reliable detection of hidden information based on a non-linear local model, in: Statistical Signal Processing Workshop (SSP), IEEE International Workshop on, 2011, pp. 493–496.

[9] R. Cogranne, C. Zitzmann, L. Fillatre, F. Retraint, I. Nikiforov, P. Cornu, A cover image model for reliable steganalysis, in: Information Hiding, volume 6958 of *Lecture Notes in Computer Science*, Springer Berlin Heidelberg, 2011, pp. 178–192.

[10] R. Cogranne, C. Zitzmann, L. Fillatre, F. Retraint, I. Nikiforov, P. Cornu, Statistical decision by using quantized observations, in: Information Theory Proceedings (ISIT), IEEE International Symposium on, 2011, pp. 1210–1214.

[11] R. Cogranne, C. Zitzmann, F. Retraint, I. Nikiforov, P. Cornu, L. Fillatre, Statistical detection of information hiding based on adjacent pixels difference, in: Signal Processing Conference (EUSIPCO), Proceedings of the 20th European, 2012, pp. 1737–1741.

[12] I. Cox, M. Miller, J. Bloom, J. Fridrich, T. Kalker, Digital Watermarking and Steganography, Morgan Kaufmann, 2nd edition, 2007.

[13] O. Dabeer, K. Sullivan, U. Madhow, S. Chandrasekaran, B. Manjunath, Detection of hiding in the least significant bit, Signal Processing, IEEE Transactions on 52 (2004) 3046–3058.

[14] S. Dumitrescu, X. Wu, Z. Wang, Detection of LSB steganography via sample pair analysis, Signal Processing, IEEE Transactions on 51 (2003) 1995–2007.

[15] T. Fawcett, An introduction to ROC analysis, Pattern Recognition Letters, Elsevier 27 (2006) 861 – 874.

[16] L. Fillatre, Adaptive steganalysis of least significant bit replacement in grayscale natural images, Signal Processing, IEEE Transactions on 60 (2012) 556–569.

[17] L. Fillatre, I. Nikiforov, F. Retraint, ε-optimal non-Bayesian anomaly detection for parametric tomography, Image Processing, IEEE Transactions on 17 (2008) 1985 –1999.

[18] T. Filler, A.D. Ker, J. Fridrich, The square root law of steganographic capacity for Markov covers, in: Proc. SPIE 7254, Media Forensics and Security, 2009, pp. 725408–11.

[19] A. Foi, M. Trimeche, V. Katkovnik, K. Egiazarian, Practical poissonian-gaussian noise modeling and fitting for single-image raw-data, Image Processing, IEEE Transactions on 17 (2008) 1737–1754.

[20] J. Fridrich, M. Goljan, On estimation of secret message length in LSB steganography in spatial domain, in: Proc. SPIE 5306, Security, Steganography, and Watermarking of Multimedia Contents VI, 2004, pp. 23–34.

[21] J. Fridrich, M. Goljan, R. Du, Detecting LSB steganography in color, and gray-scale images, MultiMedia, IEEE 8 (2001) 22–28.

[22] J. Fridrich, J. Kodovský, Steganalysis of LSB replacement using parity-aware features, in: Information Hiding, volume 7692 of *Lecture Notes in Computer Science*, Springer Berlin Heidelberg, 2013, pp. 31–45.

[23] R.C. Gonzalez, R.E. Woods, Digital Image Processing, Prentice Hall, 3rd edition, 2008.

[24] G. Healey, R. Kondepudy, Radiometric CCD camera calibration and noise estimation, Pattern Analysis and Machine Intelligence, IEEE Transactions on 16 (1994) 267–276.

[25] R. Kazinnik, S. Dekel, N. Dyn, Low bit-rate image coding using adaptive geometric piecewise polynomial approximation, Image Processing, IEEE Transactions on 16 (2007) 2225 –2233.

[26] A.D. Ker, A general framework for structural steganalysis of LSB replacement, in: Information Hiding, volume 3727 of *Lecture Notes in Computer Science*, Springer Berlin Heidelberg, 2005, pp. 296–311.

[27] A.D. Ker, Fourth-order structural steganalysis and analysis of cover assumptions, in: Proc. SPIE 6072, Security, Steganography, and Watermarking of Multimedia Contents VIII, 2006, pp. 607203–607203–14.

[28] A.D. Ker, Locating steganographic payload via ws residuals, in: Proc of the 10th workshop on Multimedia and security, MM&Sec '08, ACM, New York, NY, USA, 2008, pp. 27–32.

[29] A.D. Ker, R. Böhme, Revisiting weighted stego-image steganalysis, in: Proc. SPIE 6819, Security, Forensics, Steganography, and Watermarking of Multimedia Contents X, 2008, pp. 681905–681905–17.

[30] T.K. Kim, J. Kittler, Locally linear discriminant analysis for multimodally distributed classes for face recognition with a single model image, Pattern

Analysis and Machine Intelligence, IEEE Transactions on 27 (2005) 318–327.

[31] J.S. Lee, Digital image enhancement and noise filtering by use of local statistics, Pattern Analysis and Machine Intelligence, IEEE Transactions on 2 (1980) 165–168.

[32] K. Lee, A. Westfeld, S. Lee, Generalised category attack–Improving histogram-based attack on JPEG LSB embedding, in: Information Hiding, volume 4567 of *Lecture Notes in Computer Science*, Springer Berlin Heidelberg, 2007, pp. 378–391.

[33] E. Lehmann, J. Romano, Testing Statistical Hypotheses, Springer, 3rd edition, 2005.

[34] P. Lu, X. Luo, Q. Tang, L. Shen, An improved sample pairs method for detection of lsb embedding, in: Information Hiding, volume 3200 of *Lecture Notes in Computer Science*, Springer Berlin Heidelberg, 2005, pp. 116–127.

[35] S. Mallat, A wavelet tour of signal processing, Academic Press, 3rd edition, 2008.

[36] C. Munuera, Steganography and error-correcting codes, Signal Processing, Elsevier 87 (2007) 1528 – 1533.

[37] A. Nissar, A. Mir, Classification of steganalysis techniques: A study, Digital Signal Processing, Elsevier 20 (2010) 1758 – 1770.

[38] T. Pevný, J. Fridrich, Towards multi-class blind steganalyzer for JPEG images, in: Digital Watermarking, volume 3710 of *Lecture Notes in Computer Science*, Springer Berlin Heidelberg, 2005, pp. 39–53.

[39] R. Ramanath, W. Snyder, Y. Yoo, M. Drew, Color image processing pipeline, Signal Processing Magazine, IEEE 22 (2005) 34–43.

[40] L. Scharf, B. Friedlander, Matched subspace detectors, Signal Processing, IEEE Transactions on 42 (1994) 2146 –2157.

[41] C. Scott, R. Nowak, A neyman-pearson approach to statistical learning, Information Theory, IEEE Transactions on 51 (2005) 3806–3819.

[42] R. Shukla, P. Dragotti, M. Do, M. Vetterli, Rate-distortion optimized tree-structured compression algorithms for piecewise polynomial images, Image Processing, IEEE Transactions on 14 (2005) 343 –359.

[43] G. Simmons, The prisoners' problem and the subliminal channel, in: Advances in Cryptology, Springer US, 1984, pp. 51–67.

[44] A. Sripad, D. Snyder, A necessary and sufficient condition for quantization errors to be uniform and white, Signal Processing, IEEE Transactions on 25 (1977) 442 – 448.

[45] T. Thai, F. Retraint, R. Cogranne, Steganalysis of LSB replacement in clipped images based on the heteroscedastic noise model *(submitted)*.

[46] T. Thai, F. Retraint, R. Cogranne, Statistical model of natural images, in: Image Processing (ICIP), 19th IEEE International Conference on, 2012, pp. 2525–2528.

[47] E.W. Weisstein, CRC concise encyclopedia of mathematics, Chapman & Hall/CRC, 2003.

[48] A. Westfeld, A. Pfitzmann, Attacks on steganographic systems, in: Information Hiding, volume 1768 of *Lecture Notes in Computer Science*, Springer Berlin Heidelberg, 2000, pp. 61–76.

[49] B. Widrow, I. Kollár, Quantization Noise: Roundoff Error in Digital Computation, Signal Processing, Control, and Communications, Cambridge University Press, Cambridge, UK, 2008.

[50] C. Zitzmann, R. Cogranne, F. Retraint, I. Nikiforov, L. Fillatre, P. Cornu, Statistical decision methods in hidden information detection, in: Information Hiding, volume 6958 of *Lecture Notes in Computer Science*, Springer Berlin Heidelberg, 2011, pp. 163–177.