An Asymptotically Uniformly Most Powerful Test for LSB Matching Detection

Rémi Cogranne *Member, IEEE,* and Florent Retraint

***Abstract*—This paper investigates the detection of information hidden in digital media by the Least Significant Bit (LSB) matching scheme. In a theoretical context of known medium parameters, two important results are presented. First, based on the likelihood ratio test, we present a test that asymptotically maximizes the detection power whatever the embedding rate might be. Second, the statistical properties of this test are analytically calculated; it is particularly, shown that the decision threshold which warrants a given probability of false-alarm is independent of inspected medium parameters. This provides an asymptotic upper-bound for the detection power of any test that aims at detecting data hidden with the LSB matching method. In practice, when detecting LSB matching, the unknown medium parameters have to be estimated. Based on a local model of digital media, a generalized likelihood ratio test is presented by replacing the unknown parameters by their estimation. Numerical results on large databases highlight the relevance of the proposed methodology and comparison with state-of-the-art detectors shows that the proposed tests perform well.**

***Index Terms*—Hypothesis testing theory, Information hiding, Optimal detection, Nuisance parameters, Information forensics.**

I. Introduction and Contributions.

Steganography and steganalysis form a cat-and-mouse game. On the one hand, steganography aims at hiding the very presence of a secret message by hiding it within an innocuous cover medium. On the other hand, the goal of steganalysis (in the widest sense) is to obtain information about the potential steganographic system from an unknown medium. Usually, steganalysis focuses on exposing the existence of a hidden message in an inspected medium.

The "prisoners problem" [1], illustrates a typical scenario of steganography and steganalysis. Alice and Bob, two prisoners, communicate by imperceptibly embedding a secret binary message $\boldsymbol{M}$ into a cover-object $\boldsymbol{C}$ to obtain an innocuous looking stego-object $\boldsymbol{S}$. Then, Alice sends the stego-object $\boldsymbol{S}$ to Bob through a public channel. Wendy, the warden, examines all their communications in order to detect whether the inspected object $\mathbf{Z}$, contains a secret message $\boldsymbol{M}$ or not.

Rémi Cogranne and Florent Retraint are with the ICD - LM2S, Université de Technologie de Troyes (UTT), UMR STMR - CNRS.

Research partially funded by Troyes University of Technology (UTT) strategic program COLUMBO. 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).

Correspondance should be addressed to remi.cogranne@utt.fr or to florent.retraint@utt.fr.

A. State of the Art

Many steganographic tools are nowadays easily available on the Internet, making steganography within the reach of anyone for legitimate or malicious usage. It is thus crucial for security forces to be able to reliably detect steganographic content among a (possibly very large) set of media files. In this operational context, the detection of rather simple but most commonly found stegosystem is more important than the detection of very complex but rarely encountered stegosystem. The vast majority of downloadable steganographic tools insert the secret information in the LSB plane. For instance, as of December 2011, WetStone Technologies Inc. has 836 data hiding software among which 582 (70%) use one of the two LSB embedding functions [2]: LSB replacement and LSB matching, also known as ± 1 embedding (see [3]–[5] and the references therein). While the detection of LSB replacement is nowadays possible with a high degree of accuracy, the steganalysis of LSB matching remains much harder. When the LSB matching scheme is used, instead of LSB replacement, the detection power of state-of-the-art detectors is significantly lower, see [6], [7]. Therefore the detection of steganographic algorithms based on LSB matching embedding remains a live research topic.

It can be noted that many methods have been proposed to improve LSB embedding schemes. On the one hand, it has been proposed to improved embedding efficiency by using coding theory. Roughly speaking, the idea is to gather several samples and, using coding theory, to embed more than one bit of hidden data for each modification of cover medium samples [8], [9]. On the other hand, focusing on image steganography, it has been proposed to choose the pixels in textured areas on the assumption that those areas are difficult to model and, hence, hidden bits should be more difficult to detect [10], [11]. Similarly, the recently proposed HUGO algorithm [12] selects pixels location by minimizing a distortion function. However, those steganographic methods rely on LSB embedding and the

detection of simple LSB matching is a first step to addressing the detection of improved algorithms.

B. Contributions of the Paper

The recently proposed steganalyzers dedicated to LSB matching can be roughly divided into two categories [6]. On the one hand, most of the latest detectors are based on supervised machine learning methods and use targeted [13], [14] or universal features set [15], [16]. As in all applications of machine learning, a difficult problem is to choose an appropriate feature set. Moreover, the problem of measuring classification error probabilities remains open in the framework of statistical learning [17]. On the other hand, the authors of [18] observed that LSB matching acts as a low-pass filter on the medium Histogram Characteristic Function (HCF). This pioneering work led to an entire family of histogram-based detectors [7], [19]. While histogram based detectors have been shown to be very efficient, they have been designed with a limited exploitation of cover medium model and hypothesis testing. Hence, their statistical properties are evaluated through simulation but remain analytically unknown.

In practice, when inspecting digital images, the proposed steganalyzer must usually be immediately applicable. In addition, it might not always be possible to have access to sample image from the same camera. In particular, to train a machine learning based detector without facing the well-known cover source mismatch [20] problem, one needs sample from the same cover source which might not always be available. For these reasons, the present paper focuses on on analytical approach based on hypothesis testing theory together with a statistical model of inspected medium. The previous LSB matching steganalyzers are certainly very interesting and efficient, but they do not permit the calculation of detection errors probability. In fact, provided that the classifier is trained on an appropriate database, machine learning approaches have a higher robustness with respect to heterogeneity of inspected due to the use of a high-dimensional transformed feature space. In addition, machine learning based detectors can perform better than analytical approaches when the cover source is known, see [21]. However, the main problem address in this paper is to provide detection algorithms with an analytical expression for the false-alarm and missed-detection probabilities, for instance to warrant a false-alarm rate. This is only possible using a statistical model of inspected medium together with an analytical study of the statistical hypothesis test properties. Besides, this approach also permits the establishment of upper bounds on the detection performance one can expect from any detector and allows us to understand the influence of some medium parameters on such bounds.

The first step in the direction of hypothesis testing has been made in [22]–[25] for LSB replacement to design a statistical test with known statistical properties. In the present paper, this statistical approach is extended to the case of detecting LSB matching. It should be highlighted that for this extension is not immediate because considering a different embedding scheme implies to solve a different hypothesis testing problem. Moreover, in the case of LSB matching detection, even when all the signal or image parameters are known, the optimal solution, namely the Likelihood Ratio Test (LRT), is unknown. Hence, it is necessary, first, to design the LRT and, second, to establish its statistical properties in order to calculate its detection performance. Therefore, the contributions of this paper are the following:

1) The Most Powerful (MP) test is defined in the theoretical case when the cover medium parameters are known, namely the expectation and noise variance of each sample.
2) Under mild assumption, an Asymptotically Uniformly Most Powerful (AUMP) test is proposed. This test maximizes the detection power whatever the hidden information might be.
3) The statistical properties of proposed AUMP test are analytically established as the number of samples grows to infinity. This provides an upper-bound on the detection power for any test that aims at detecting LSB matching. This also shows that the decision threshold does not depend on inspected medium parameter, but only on the prescribed false-alarm probability.
4) Eventually, when the inspected medium parameters are unknown, two efficient implementations of the AUMP are proposed, based on two different local estimations of expectation and variance of each sample.

Compared to the prior works on the statistical detection of LSB replacement using hypothesis testing theory [23]–[25], the present paper investigates the detection of LSB matching scheme. Though this might seems to be a small difference, this changes the whole hypothesis testing problem. Particularly, the test proposed in the present paper for LSB matching detection essentially rely on the accurate estimate of pixels' variance which is much more difficult than the estimation of pixels' expectation on which rely the detection of LSB replacement.

C. Organization of the Paper

The paper is organized as follows. The problem of LSB matching steganalysis is cast within the framework of hypothesis testing in Section II. Following the Neyman-Pearson approach, Section III first presents the MP Likelihood Ratio Test (LRT). Next, the AUMP criterion of optimality is presented and discussed. Finally, an AUMP test is presented when all the medium parameters (statistical expectation and variance of samples) are known. The statistical performance of this AUMP test is analytically calculated in Section IV. Section V addresses the problem of LSB matching detection when the parameters of each sample are unknown and have to be estimated. Using a linear parametric model of inspected medium a Generalized LRT (GLRT) is presented in Section V. To show the relevance of the proposed approach, numerical results on two large databases of natural images are shown in Section VI. Section VII concludes the paper.

II. Hidden Information Detection Problem Statement.

A. Statistical model of media

This paper mainly focuses on natural images, *i.e.* recorded with some imaging device, but the extension of the presented results to any kind of digital media is immediate. Hence, the column vector $\boldsymbol{C} = (c_1, \dots, c_N)^T$ represents in this paper a cover medium of $N = N_x \times N_y$ samples. The samples are usually represented as unsigned integers encoded with B bits, hence each c_n belongs to the set $\mathcal{Z} = \{0; \dots; 2^B - 1\}$. Each cover sample c_n results from the quantization:

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

where $y_n \in \mathbb{R}^+$ denotes the raw pixel intensity recorded by the camera photosensor (or the sample value in the case of other media) and Q_Δ represents the uniform quantization with a step Δ defined as:

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

Seeking simplicity, it is chosen in the present paper not to distinguish the quantized value Δk from the quantization index k. Observing that $Q_\Delta(x) = Q_1(x/\Delta)$ it is considered in the whole paper that samples are scaled by Δ^{-1} prior to being quantized with a unit step. Similarly, it is assumed for clarity that the saturation effect is absent, *i.e.* the probability that y_n exceeds quantizer boundaries is negligible.

The recorded pixel value can be decomposed as [25], [26]:

$$y_n = \mu_n + \xi_n, \tag{2}$$

where μ_n is a deterministic parameter corresponding to the mathematical expectation of y_n. On the contrary, ξ_n is a random variable representing all the noise corrupting the cover image during acquisition. For most of the digital media, ξ_n is accurately modeled as a realization of a zero-mean Gaussian random variable $\Xi_n \sim \mathcal{N}(0, \sigma_n^2)$ with variance σ_n^2. It is important to note that the raw pixels are statistically independent [26], [27] and that the variance σ_n^2 varies from pixel to pixel, mainly due to the photo-counting shot noise. As described in [26], this model is an accurate approximation of noisy raw images produced by digital imaging devices.

It thus follows, from Equations (1) and (2), that c_n follows a distribution denoted P_{θ_n} and entirely characterized by the parameters $\theta_n = (\mu_n \sigma_n)^T$ with $\mathbf{A}^T$ the transpose of $\mathbf{A}$. For the sake of precision let θ_n belong to a space $\Theta_n \subset \mathbb{R}^2$ and define $\boldsymbol{\theta} = (\theta_1, \dots, \theta_N)$, $\boldsymbol{\theta} \in \Theta = \Theta_1 \times \dots \times \Theta_N$ representing the whole image parameter.

The distribution P_{θ_n} is defined by its probability mass function (pmf) $P_{\theta_n} = (p_{\theta_n}[0], \dots, p_{\theta_n}[2^B - 1])$ where for all $k \in \mathcal{Z}$:

$$\begin{aligned} p_{\theta_n}[k] &= \Phi\left(\frac{k + 1/2 - \mu_n}{\sigma_n}\right) - \Phi\left(\frac{k - 1/2 - \mu_n}{\sigma_n}\right), \\ &= \frac{1}{\sigma_n} \int_{k-1/2}^{k+1/2} \phi\left(\frac{u - \mu_n}{\sigma_n}\right) du. \end{aligned} \tag{3}$$

In this paper, ϕ denotes the standard Gaussian probability distribution function (pdf) $\phi(u) = (2\pi)^{-1/2} \exp(u^2/2)$ and Φ represents the standard Gaussian cumulative distribution function (cdf) defined by $\Phi(x) = \int_{-\infty}^{x} \phi(u) du$.

In virtue of the mean value theorem, the probability $p_{\theta_n}[k]$ defined in Equation (3) can be written as:

$$p_{\theta_n}[k] = \frac{1}{\sigma_n} \phi\left(\frac{k - \mu_n}{\sigma_n}\right) + \epsilon, \tag{4}$$

where ϵ is a (small) corrective term. More precisely, the well known Taylor expansion of the function φ [28, p.931] shows that

$$\epsilon = 0 + o\left(\sigma_n^{-2}\right) \tag{5}$$

where $y = o(x)$ means that y/x tends to 0 as x tends to 0, see details in [23], [29]. As it is considered in the paper that a unit step quantizer is used, the noise variance σ_n^2 actually represents the ratio ς^2/Δ^2, where ς_n^2 represents the variance of n-th sample before it is scaled by Δ^{-1}. This paper focuses on the case $\Delta \ll \varsigma_n$ in which the problem of hidden information detection is the hardest. In practice this assumption is especially relevant for uncompressed digital media because raw sound files usually result from a quantization using $B = 16$ bits and digital raw images are usually coded with $B = 12, 14$ or even 16 bits.

To model statistically stego-image pixels from (3) - (4), the two following assumptions are usually adopted [22], [30] :

1) Because the message is previously compressed and/or cyphered, each hidden bit of message $\boldsymbol{M} = (m_1, \dots, m_\ell)^T$ is drawn from a binomial distribution $\mathcal{B}(1, 1/2)$, *i.e.* $\forall m \in \{1, \dots, \ell\}$, m_l is either 0 or 1 with the same probability.
2) The insertion locations in the cover-object are chosen pseudo-randomly using a secret key, hence, each cover pixel c_n is used with the same probability.

Let the embedding rate $R \in (0, 1]$, $R = \ell/N$ be the number of hidden bits per cover pixel and let $\boldsymbol{S} = \{s_1, \dots, s_N\}$ be the values of stego-image pixels, *i.e.* after insertion of hidden information. The previous assumptions allow us to capture the impact of LSB matching data hiding by denoting [7], [13], [18] for all $n \in \{0, \dots, N\}$:

$$\begin{cases} \mathbb{P}[s_n = c_n] = (1 - R/2)\,, \\ \mathbb{P}[s_n = c_n + 1] = \mathbb{P}[s_n = c_n - 1] = R/4, \end{cases} \tag{6}$$

Hence, it follows from (6) that for all $n \in \{1, \dots, N\}$, the pmf of the stego-pixel s_n after embedding at rate R with LSB matching is given by $Q_{\theta_n}^R = \left(q_{\theta_n}^R[0], \dots, q_{\theta_n}^R[2^b - 1]\right)$ with for all $k \in \mathcal{Z}$:

$$q_{\theta_n}^R[k] = \frac{R}{4}\left(p_{\theta_n}[k-1] + p_{\theta_n}[k+1]\right) + \left(1 - \frac{R}{2}\right) p_{\theta_n}[k]. \tag{7}$$

B. Hypothesis Testing Problem Statement

When analyzing an unknown medium $\mathbf{Z} = (z_1, \dots, z_N)^T$ the goal of LSB matching steganalysis is to decide between the two following hypotheses:

$$\begin{aligned} \mathcal{H}_0 &= \left\{ z_n \sim P_{\theta_n}, \forall n \in \{1, \dots, N\}, \forall \boldsymbol{\theta} \in \Theta \right\} \\ \mathcal{H}_1 &= \left\{ z_n \sim Q_{\theta_n}^R, \forall n \in \{1, \dots, N\}, \forall \boldsymbol{\theta} \in \Theta, \forall R \in (0, 1] \right\}. \end{aligned} \tag{8}$$

The goal is to find a test $\delta : \mathcal{Z}^N \mapsto \{\mathcal{H}_0, \mathcal{H}_1\}$, such that hypothesis $\mathcal{H}_i$ is accepted if $\delta(\mathbf{Z}) = \mathcal{H}_i$ (see [31] for details about statistical hypothesis testing). As explained in the introduction, in an operational forensics context the most important challenge is first, to warrant a prescribed (very low) false-alarm probability. Hence, let the class $\mathcal{K}_\alpha$ of tests whose false-alarm probability is upper-bounded by α_0 be defined as:

$$\mathcal{K}_\alpha = \left\{ \delta : \sup_{\boldsymbol{\theta}\in\Theta} \mathbb{P}_0[\delta(\mathbf{Z}) = \mathcal{H}_1] \leq \alpha_0 \right\}, \tag{9}$$

where $\mathbb{P}_i(\cdot)$ stands for the probability under hypotheses $\mathcal{H}_i$, $i = \{0; 1\}$. Then, it is obviously desirable, to maximize the detection power defined by:

$$\beta_\delta = \mathbb{P}_1[\delta(\mathbf{Z}) = \mathcal{H}_1].$$

The problem of steganalysis as stated in Equation (8) highlights fundamental difficulties, from a hypothesis testing point of view, which remain open for the LSB matching detection. The first difficulty is due to the fact that, even when image content $\boldsymbol{\theta}$ and embedding rate R are known, the optimal solution, namely the Likelihood Ratio Test (LRT), is unknown. Hence, it is necessary i) to design the LRT and ii) to establish its statistical properties in order to calculate its detection performance. The second difficulty occurs in practice because the embedding rate R is unknown. Consequently, the hypothesis $\mathcal{H}_1$ becomes composite and the ultimate goal is to find a Uniformly Most Powerful (UMP) test, *i.e.* that maximizes the detection power whatever R might be. It is straightforward here to verify that the hypotheses do not admit a monotonic likelihood ratio, therefore the existence of a UMP test is compromised [31, Theorem 3.4.1]. The third difficulty is due to the fact that the parameter $\boldsymbol{\theta}$ is unknown. In fact, image content $\boldsymbol{\theta}$ acts a nuisance parameter, which prevents hidden information detection because it has no interest for the considered detection problem (8) while it appears in pixel statistical models (3)-(7). It has specifically been shown that inaccurate estimation of $\boldsymbol{\theta}$ may cause detection error [32], [38]. Moreover, it is crucial to propose a detection algorithm which takes a decision as independently as possible of image content [6]. Hence, it is necessary to design a statistical test which eliminates $\boldsymbol{\theta}$ by explicitly taking into account this nuisance parameter.

The main goals of this paper are, first, to provide a statistical test with an analytical expression for the detection error probabilities, and to prove that this test is optimal for any embedding rate $R \in [0; 1]$. Then, to propose a practical implementation when no information on analyzed medium is available; this problem of dealing with nuisance parameters $\theta_1, \ldots, \theta_N$ is addressed using a linear parametric of samples in Section V.

III. Most Powerful Likelihood Ratio Test for LSB Matching

Let us start with the simplest case, when the embedding rate R and the parameter $\boldsymbol{\theta}$ are known. In this case, the hypothesis testing problem (8) is reduced to a test between two simple hypotheses.

In virtue of the Neyman-Pearson lemma, see [31, Theorem 3.2.1], the most powerful (MP) test over the class $\mathcal{K}_{\alpha_0}$ (9) is the LRT given by the following decision rule:

$$\delta_R(\mathbf{Z}) = \begin{cases} \mathcal{H}_0 & \text{if} \quad \Lambda_R(\mathbf{Z}) \leq \tau_{\alpha_0} \\ \mathcal{H}_1 & \text{if} \quad \Lambda_R(\mathbf{Z}) > \tau_{\alpha_0}, \end{cases} \tag{10}$$

where τ_{α_0} is the solution of $\mathbb{P}_0[\delta(\mathbf{Z}) > \tau_{\alpha_0}] = \alpha_0$, to ensure that $\delta_R \in \mathcal{K}_{\alpha_0}$, and the likelihood ratio (LR) $\Lambda_R(\mathbf{Z})$ is given, from the statistical independence between samples, by:

$$\Lambda_R(\mathbf{Z}) = \sum_{n=1}^{N} \Lambda_R(z_n) = \sum_{n=1}^{N} \log \left(\frac{q^R_{\theta_n}[z_n]}{p_{\theta_n}[z_n]} \right). \tag{11}$$

It is important to note that the LRT can be used for any detection problem provided that the statistical distribution of observations under each hypothesis $\mathcal{H}_0$ and $\mathcal{H}_1$ is known. However, the previous work for detection of LSB replacement [23]–[25] can hardly be used to derive a test for LSB matching detection because the definition of alternative hypothesis $\mathcal{H}_1$ changes. Therefore the whole decision problem which it is aimed to solve differs from LSB replacement and LSB matching.

Using the definition of sample distribution under alternative hypothesis $\mathcal{H}_1$ (7), the LR can be written:

$$\begin{aligned} \Lambda_R(\mathbf{Z}) &= \sum_{n=1}^{N} \log \left(\frac{R}{4} \frac{p_{\theta_n}[z_n-1] + p_{\theta_n}[z_n+1]}{p_{\theta_n}[z_n]} + \left(1 - \frac{R}{2}\right) \right) \\ &= \sum_{n=1}^{N} \log \left(1 + \frac{R}{2} \left(\frac{p_{\theta_n}[z_n-1] + p_{\theta_n}[z_n+1]}{2p_{\theta_n}[z_n]} - 1 \right) \right). \end{aligned} \tag{12}$$

It can be noted that $\Lambda_R(z_n)$ depends on sample values z_n through the quantity:

$$\frac{1}{2} \frac{p_{\theta_n}[z_n - 1] + p_{\theta_n}[z_n + 1]}{p_{\theta_n}[z_n]},$$

which should be analyzed in order to provide an explicit expression of the LR $\Lambda_R(z_n)$.

The exact expression for the LR $\Lambda_R(z_n)$ is complicated due to the corrective terms ϵ defined in (4). However, as established in Equation (5), the calculation shows that these corrective terms are negligible when $\Delta \ll \sigma_n$ which is the case considered in this paper. Therefore, from Equation (4), a short algebra detailed in Appendix A permits the writing of:

$$\begin{aligned} \frac{p_{\theta_n}[z_n-1]}{p_{\theta_n}[z_n]} &= \exp\left(-\frac{1}{2\sigma_n^2}\right) \exp\left(\frac{z_n-\mu_n}{\sigma_n^2}\right) + o\left(\sigma_n^{-2}\right), \\ \frac{p_{\theta_n}[z_n+1]}{p_{\theta_n}[z_n]} &= \exp\left(-\frac{1}{2\sigma_n^2}\right) \exp\left(\frac{\mu_n-z_n}{\sigma_n^2}\right) + o\left(\sigma_n^{-2}\right). \end{aligned} \tag{13}$$

By using the results from Equation 13, one can write:

$$\begin{aligned} &\frac{1}{2} \frac{p_{\theta_n}[z_n-1] + p_{\theta_n}[z_n+1]}{p_{\theta_n}[z_n]} = \\ &\qquad \frac{1}{2} \exp\left(-\frac{1}{2\sigma_n^2}\right) \left[\exp\left(\frac{\mu_n-z_n}{\sigma_n^2}\right) + \exp\left(\frac{z_n-\mu_n}{\sigma_n^2}\right) \right]. \end{aligned} \tag{14}$$

It is obvious from Equation (14) that

$$\frac{1}{2} \frac{p_{\theta_n}[z_n-1] + p_{\theta_n}[z_n+1]}{p_{\theta_n}[z_n]} - 1 \to 0,$$

as Δ/ς_n tends to 0. Hence a Taylor series expansion of the function $\log(1+x)$, detailed in Appendix A, permits the writing of:

$$\Lambda_R(z_n) = \frac{R}{4\sigma_n^4}\left((z_n-\mu_n)^2-\sigma_n^2+\frac{1}{4}\right) - \frac{R^2}{32\sigma_n^4} + o\left(\sigma_n^{-4}\right). \tag{15}$$

This expression (15) is used to design the proposed AUMP test in the next Section IV.

IV. From the LRT to the Proposed AUMP Test

A. The AUMP criterion of optimality

It is very difficult to use the LR $\Lambda_R(z_n)$, as given in Equation (15), because it depends on the embedding rate R, which is unknown. Therefore, it is necessary to transform the quantity $\Lambda_R(z_n)$ slightly to remove this dependence with respect to R, while keeping the optimality of the LR test. In the framework of hypothesis testing theory, this corresponds to finding an UMP test. Formally, a test $\delta^\star$ is UMP in the class $\mathcal{K}_{\alpha_0}$ if for any other test $\delta \in \mathcal{K}_{\alpha_0}$ it holds that $\forall R \in (0;1]\,, \forall \theta \in \Theta\,, \beta_\delta - \beta_{\delta^\star} \leq 0$.
In other words, in the presence of a nuisance parameter $\boldsymbol{\theta}$ and an unspecified distribution parameter R, a test is UMP if, whatever θ and R might be, it warrants a false-alarm probability α_0 while it simultaneously maximizes the detection power. Unfortunately, as described in Section II-B the existence of a UMP test is compromised [31, Theorem 3.4.1] for testing hypotheses $\mathcal{H}_0$ and $\mathcal{H}_1$ (8). The alternative solution proposed in this paper is to design a test that asymptotically coincides with a UMP test. This corresponds to an AUMP test whose definition [31, Definition 13.3.2] is hereby recalled.

Definition 1. *For testing the hypotheses $\mathcal{H}_0$ and $\mathcal{H}_1$ (8), a test $\delta^\star$ is AUMP in the class $\mathcal{K}_{\alpha_0}^{\infty}$ given by:*

$$\mathcal{K}_{\alpha_0}^{\infty} = \left\{\delta : \limsup_{N\to\infty} \sup_{\boldsymbol{\theta}\in\Theta} \mathbb{P}_0[\delta(\mathbf{Z}) = \mathcal{H}_1] \leq \alpha_0\right\}.$$

if $\delta^\star \in \mathcal{K}_{\alpha_0}^{\infty}$ and for any other test $\delta \in \mathcal{K}_{\alpha_0}^{\infty}$ it holds that $\forall R \in (0;1]\,, \forall \theta \in \Theta\,, \limsup_{N\to\infty} \beta_\delta - \beta_{\delta^\star} \leq 0$.

B. Definition and Properties of the Proposed AUMP Test

From the expression (15), it is obvious that when R and $\boldsymbol{\theta}$ are known, the LR Λ_R only depends on the observation through the term:

$$\frac{(z_n-\mu_n)^2}{\sigma_n^4}.$$

Hence, it is proposed to base the proposed test on the following quantity:

$$\Lambda_{\text{aump}}(z_n) = \frac{(z_n-\mu_n)^2 - 1/12}{\sigma_n^4} - \frac{1}{\sigma_n^2}. \tag{16}$$

The choice to replace LR $\Lambda_R(z_n)$ in the proposed test the by the quantity $\Lambda_{\text{aump}}(z_n)$ is motivated by the following arguments. First, it can be noted that $\Lambda_{\text{aump}}(z_n)$ differs from the LR $\Lambda_R(z_n)$ only by an additive constant and a multiplicative constant, which do not change the performance of the ensuing test, as formalized in Theorem 2. Second, by using the fact that that $y_n \sim \mathcal{N}(\mu_n, \sigma_n^2)$ and $z_n = Q_1(y_n)$, it is well known, see [33] for details, that $\mathbb{E}\left[(z_n-\mu_n)^2\right] = \sigma_n^2 + 1/12$. Hence, the expectation of $\Lambda_{\text{aump}}(z_n)$ is zero under hypothesis $\mathcal{H}_0$. Last but not least, the dependance with R has been removed from Equation (16); this quantity can thus be calculated when R is unknown, provided that $\theta_n = (\mu_n, \sigma_n)^T$ is known.
Let the quantity $\bar{\sigma}^4$, which roughly speaking represents the "mean squared variance" of samples, be defined as:

$$\bar{\sigma}^{-4} \stackrel{\text{def.}}{=} N^{-1}\sum_{n=1}^{N}\sigma_n^{-4}. \tag{17}$$

The test proposed in this paper for detecting LSB matching is defined by:

$$\delta_{\text{aump}} = \begin{cases}\mathcal{H}_0 & \text{if} \quad \Lambda_{\text{aump}}(\mathbf{Z}) \leq \tau_{\alpha_0} \\ \mathcal{H}_1 & \text{if} \quad \Lambda_{\text{aump}}(\mathbf{Z}) > \tau_{\alpha_0},\end{cases} \tag{18}$$

$$\text{where} \quad \Lambda_{\text{aump}}(\mathbf{Z}) = \frac{\bar{\sigma}^2}{\sqrt{2N}}\sum_{n=1}^{N}\Lambda_{\text{aump}}(z_n). \tag{19}$$

As previously discussed, the main challenge is to provide the proposed test δ_{aump} with analytical expression for the false-alarm and missed detection probabilities. To this end, the asymptotic approach, which consists of assuming that the number N of samples grows to infinity, is used in the present paper. On a practical point of view, the approach is particularly relevant for the problem of steganalysis as, usually, digital media are made of a very large number of samples.
In this framework, the asymptotic distribution of $\Lambda_{\text{aump}}(\mathbf{Z})$, under both hypotheses $\mathcal{H}_0$ and $\mathcal{H}_1$, can be established from the well known Lindeberg's central limit theorem (CLT) [31, Theorem 11.2.5] which states that:

$$\frac{\sum_{n=1}^{N}\Lambda_{\text{aump}}(z_n) - \mathbb{E}_i\left[\Lambda_{\text{aump}}(z_n)\right]}{\sqrt{\sum_{n=1}^{N}\mathbb{V}ar_i\left[\Lambda_{\text{aump}}(z_n)\right]}} \rightsquigarrow \mathcal{N}(0,1), \tag{20}$$

where for $i = \{0;1\}$, the notations $\mathbb{E}_i[\cdot]$ and $\mathbb{V}ar_i[\cdot]$ respectively denote the mathematical expectation and the variance under $\mathcal{H}_i$ and $\rightsquigarrow$ represents the convergence in distribution as N tends to infinity.
It should be noted that the application of Lindeberg's CLT (20) requires that the well known Lindeberg's condition [31, Eq. (11.11)] is satisfied. In the present case it is easy to verify the Lyapounov's condition [31, Eq. (11.12)] which implies Lindeberg's condition.

It is shown in the Appendix A-B that under hypothesis $\mathcal{H}_0$ one has:

$$\mathbb{E}_0\left[\Lambda_{\text{aump}}(z_n)\right] = 0 + o(\sigma_n^{-4})$$
$$\text{and } \mathbb{V}ar_0\left[\Lambda_{\text{aump}}(z_n)\right] = \frac{2}{\sigma_n^4} + o(\sigma_n^{-8}).$$

Hence, as Δ/ς_n tends to 0, it immediately follows from Equations (17), (19) and from Lindeberg CLT that under $\mathcal{H}_0$:

$$\frac{\sum_{n=1}^{N}\Lambda_{\text{aump}}(z_n)}{\sqrt{2\sum_{n=1}^{N}\sigma_n^{-4}}} = \Lambda_{\text{aump}}(\mathbf{Z}) \rightsquigarrow \mathcal{N}(0,1). \tag{21}$$

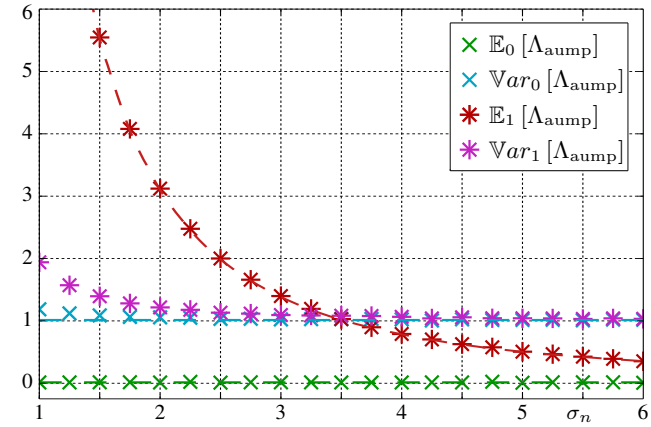


Fig. 1: Comparison between empirical moments of Λ_{aump} and their theoretical expression as Δ/ς_n tends to 0 (dashed lines).

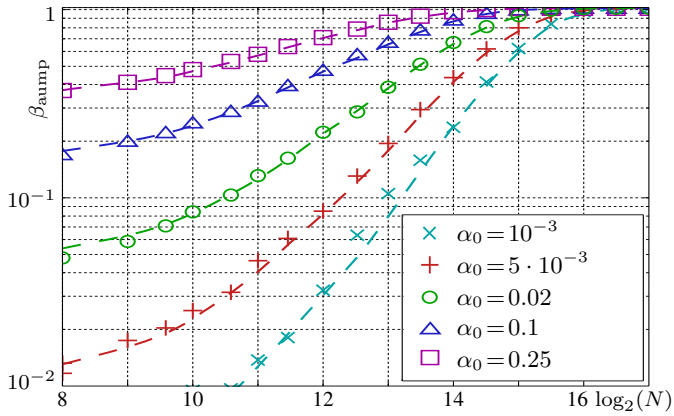


Fig. 2: Comparison between empirical and theoretical (dashed line) detection power of δ_{aump} as a function of sample number N and for few false-alarm probabilities α_0.

Similarly, under hypothesis $\mathcal{H}_1$, it is shown in the Appendix A-B that the moments of $\Lambda_{\text{aump}}(z_n)$ are given by:

$$\mathbb{E}_1[\Lambda_{\text{aump}}(z_n)] = \frac{R}{2\sigma_n^2} + o(\sigma_n^{-4})$$
$$\text{and } \mathbb{V}ar_1[\Lambda_{\text{aump}}(z_n)] = \frac{2}{\sigma_n^4} + o(\sigma_n^{-4}).$$

From the Lindeberg's CLT, the distribution of $\Lambda_{\text{aump}}(z_n)$ is asymptotically given under $\mathcal{H}_1$, as Δ/ς_n tends to 0, by:

$$\Lambda_{\text{aump}}(\mathbf{Z}) \rightsquigarrow \mathcal{N}\left(\sqrt{N}\frac{R}{\bar{\sigma}^2\sqrt{8}}, 1\right). \tag{22}$$

The Figure 1 illustrates the sharpness of the results (21) - (22) through a comparison between empirical moments of $\Lambda_{\text{aump}}(\mathbf{Z})$, under both hypotheses $\mathcal{H}_0$ and $\mathcal{H}_1$, and their theoretical expressions (dashed lines). The empirical moments were calculated from a Monte-Carlo simulation with 2000 samples and 10^5 realizations. It can specifically be noted from Figure 1 that the variance $\mathbb{V}ar_1[\Lambda_{\text{aump}}]$ might be impacted by the term $o(\sigma_n^{-4})$ when σ_n is rather small, which corresponds to the case of a sample with a few level of noise.

Finally, the asymptotic distribution of $\Lambda_{\text{aump}}(\mathbf{Z})$ given in Equation (21) - (22) allows us to establish analytically the parameters of the proposed test δ_{aump} in the following Theorem 1. Those parameters depend on the quantity

$$\varrho \overset{\text{def.}}{=} \frac{R}{\bar{\sigma}^2\sqrt{8}} \tag{23}$$

which is interpreted as an "Insertion-to-noise Ratio" and serves, in this paper, to define the upper-bound for the detection power of any test that aims at detecting LSB matching.

Theorem 1. *For any given probability of false alarm $\alpha_0 \in (0,1)$, assuming that the parameter $\boldsymbol{\theta}$ is known, the decision threshold $\widetilde{\tau}_{\alpha_0}$ given by:*

$$\tau_{\alpha_0} = \Phi^{-1}(1-\alpha_0) \tag{24}$$

where $\Phi^{-1}(\cdot)$ is the Gaussian inverse cumulative distribution, asymptotically warrants that the test δ_{aump} (18) is in $\mathcal{K}_{\alpha_0}$. For any $\alpha_0 \in (0,1)$, assuming that the parameter $\boldsymbol{\theta}$ is known, the power function $\beta_{\text{aump}}(\varrho)$ associated with the test δ_{aump} (18) is asymptotically given, as $N \to \infty$, by:

$$\beta_{\text{aump}}(\varrho) = 1 - \Phi\left(\Phi^{-1}(1-\alpha_0) - \sqrt{N}\varrho\right). \tag{25}$$

Proof: The proof of Theorem 1 is given in Appendix A-B ■

The Theorem 1 highlights two main interests of the proposed test δ_{aump} (18). First, the decision threshold given by (24) does not depend on parameter θ, but only on prescribed false-alarm probability α_0. Hence for any inspected medium, it is straightforward to respect a false-alarm probability constraint. Second, the power function given in Equation (25) provides a simple expression of proposed test detection power, as Δ/ς tends to 0.
In addition, it can be noted that the detection power $\beta_{\text{aump}}(\varrho)$ of the proposed test complies with the square root law of steganographic capacity [34] as a short algebra immediately permits us to write:

$$\lim_{\sqrt{N}/L \to 0} \beta_{\text{aump}}(\varrho) = 1 \quad \text{and} \quad \lim_{\sqrt{N}/L \to \infty} \beta_{\text{aump}}(\varrho) = \alpha_0. \tag{26}$$

Lastly, the following Theorem 2 establishes the optimality of the proposed statistical test.

Theorem 2. *For any given probability of false alarm $\alpha_0 \in (0,1)$, assuming that $\boldsymbol{\theta}$ is known and that $\Delta/\varsigma_n \to 0$ then it holds that δ_{aump} is AUMP is the class $\mathcal{K}_{\alpha_0}^{\infty}$ provided that the decision threshold is chosen as in Equation (24).*

Proof: The proof of Theorem 2 is given in Appendix A ■

The Theorem 2 formally states that Equation 25 provides an upper bound for the detection power of any steganalyzer. It should be noted that it has been assumed in Sections III and IV that $\boldsymbol{\theta}$ is known, hence the Definition 1 of AUMP criterion must be understood without the supremum over Θ. The problem of dealing with the nuisance parameter $\boldsymbol{\theta}$ is addressed in the next Section V.

V. Practical Design of AUMP test: Dealing with Nuisance Parameters.

In practice, the application of the test δ_{aump} (18) is compromised because neither the expectation μ_n nor the variance σ_n^2 of samples is known. In such a situation, a usual solution consists in replacing the unknown values by their Maximum Likelihood Estimation (MLE), denoted $\widehat{\mu}_n$ and $\widehat{\sigma}_n^2$, respectively, to design a Generalized Likelihood Ratio Test (GLRT).

However, accurate estimation of the parameters μ_n and σ_n is a difficult problem but necessary to obtain a high detection performance. In the following Sections V-A and V-B two different solutions are presented. The underlying idea is that most of digital media acquired with a recording device can be represented as signals whose properties vary smoothly from sample to sample. Hence, those redundancies that naturally exist between neighbouring samples can be used to estimate locally unknown parameters.

A. Linear Parametric Model of Medium.

In this paper it is first proposed to use a linear parametric model of inspected medium $\mathbf{Z}$; to this end, $\mathbf{Z}$ is considered as a set of K non-overlapping blocks of L samples, with $N \approx KL$. Similarly to the scalar case (1) - (2), let us define, for all $k \in \{1, \ldots, K\}$, the k-th block $\mathbf{z}_k = (\mathbf{z}_{k,1}, \ldots, \mathbf{z}_{k,L})^T$ as:

$$\mathbf{z}_k = Q_\Delta(\mathbf{y}_k)\,,\ \mathbf{y}_k = \boldsymbol{\mu}_k + \boldsymbol{\xi}_k \sim \mathcal{N}(\boldsymbol{\mu}_k, \sigma_k^2 \mathbf{I}_L), \tag{27}$$

where the operation of uniform quantization Q_Δ is applied on each sample individually, σ_k^2 is the samples variance assumed constant on each block and $\mathbf{I}_L$ is the identity matrix of size $L \times L$.

The literature proposes a wide range of mathematical models to approximate locally vectors $\boldsymbol{\mu}_k = (\mu_{k,1}, \ldots, \mu_{k,L})^T$ of expectations. In the present paper, the following linear parametric model [23], [32] is used:

$$\boldsymbol{\mu}_k = \mathbf{H}\mathbf{x}_k, \tag{28}$$

where $\mathbf{H}$ is a known full rank matrix of size $L \times p$, with $p < L$, and $\mathbf{x}_k \in \mathbb{R}^p$ is the nuisance parameter describing the expectation of signal $\mathbf{z}_k$.

The hypothesis testing theory is relatively well developed for models such as (28). In fact, such a model permits the rejection of nuisance parameters $\boldsymbol{\mu}_k$ by using the theory of invariance. Note that the theory of invariance is used here because it is assumed that Δ/ς_n tends to 0, this theory, however, formally holds for non-quantized observations [31, Chap. 6].

From model (27) - (28), a short algebra shows that the maximum likelihood estimator (MLE) $\widehat{\boldsymbol{\theta}}_k = (\widehat{\theta}_{k,1}, \ldots, \widehat{\theta}_{k,L})^T$ of $\boldsymbol{\theta}_k$ is given by:

$$\widehat{\boldsymbol{\theta}}_k = \mathbf{H}(\mathbf{H}^T\mathbf{H})^{-1}\mathbf{H}^T\mathbf{z}_k \tag{29}$$

Theory of invariance thus permits us to reject nuisance parameters, and from (14), to write the proposed GLR calculated on k-th block as:

$$\Lambda_{\text{glr}}(\mathbf{z}_k) = \sum_{l=1}^{L}\left[\frac{(z_{k,l} - \widehat{\theta}_{k,l})^2}{\sigma_k^4}\right] - (L-p)\frac{1/12 + \sigma_k^2}{\widehat{\sigma}_k^4}.$$

With these definitions, the proposed GLRT is given as:

$$\delta_{\text{glr}}(\mathbf{Z}) = \begin{cases} \mathcal{H}_0 & \text{if} \quad \Lambda_{\text{glr}}(\mathbf{Z}) \ \leq \ \tau_{\alpha_0} \\ \mathcal{H}_1 & \text{if} \quad \Lambda_{\text{glr}}(\mathbf{Z}) \ > \ \tau_{\alpha_0}, \end{cases} \tag{30}$$

$$\text{with } \Lambda_{\text{glr}}(\mathbf{Z}) = \frac{\bar{\sigma}^2}{\sqrt{2K(L-p)}} \sum_{k=1}^{K} \Lambda_{\text{glr}}(\mathbf{z}_k). \tag{31}$$

The following Theorem 3 establishes the power of the proposed practical test based on a linear parametric model of inspected medium.

Theorem 3. *For any given probability of false alarm $\alpha_0 \in (0,1)$, assuming that the model of inspected medium $\mathbf{Z}$ described in Equations (27) and (28) holds, the decision threshold $\widetilde{\tau}_{\alpha_0}$ given by:*

$$\widehat{\tau}_{\alpha_0} = \Phi^{-1}(1-\alpha_0) \tag{32}$$

asymptotically warrants that the test δ_{glr} (30) is in $\mathcal{K}_{\alpha_0}$. Under the same conditions, for any $\alpha_0 \in (0,1)$, the power function $\beta_{\text{glr}}(\varrho)$ associated with the test δ_{glr} (30) is asymptotically given, as $K \to \infty$, by:

$$\beta_{\text{glr}}(\varrho) = 1 - \Phi\left(\Phi^{-1}(1-\alpha_0) - \sqrt{K(L-p)}\varrho\right). \tag{33}$$

Proof: The proof of Theorem 3 is given in Appendix B. ∎

As discussed in [38], the estimation of samples expectation, even locally, is a very difficult problem. In particular, digital images exhibit a complex structured content which is difficult to model accurately. Consequently, in the present paper the use an adaptive model of the inspected medium is proposed. This choice is lead by the fact that the rather simple model proposed in [24], [32], [38] could have been improve to estimate more accurately the variance. The idea of the adaptive model used in this paper is to adapt the p vector of matrix $\mathbf{H}$ to the local content of each block $\mathbf{z}_k$, see [39], [40] and the references therein. For the numerical simulation presented in this paper, a two-dimensional Discrete Cosine Transform (2D-DCT) was used [41]. The components matrix of $\mathbf{H}$ were chosen by selecting the p most important absolute value of 2D-DCT coefficients.

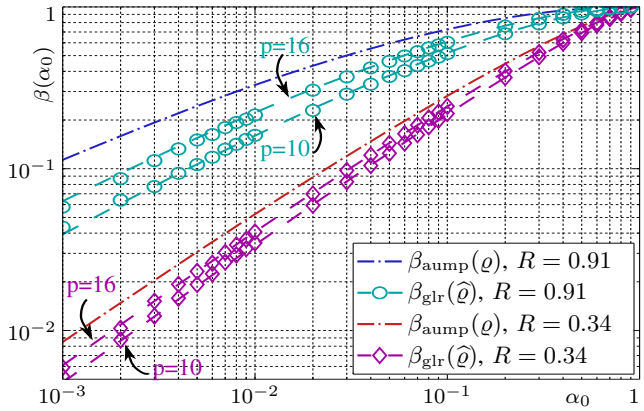
In practice when the parameters σ_k^2 are unknown they can be replaced by their ML estimation:

$$\widehat{\sigma}_k^2 = \frac{\left\|\mathbf{z}_k - \widehat{\boldsymbol{\theta}}_k\right\|_2^2}{L-p} - \frac{1}{12}.$$

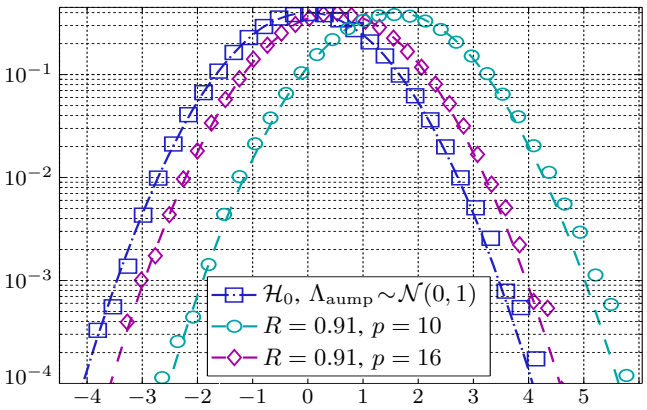
It should be noted that a major problem remains open: the statistical inference between cover image and hidden information have not been considered Hence, the impact of hidden information on estimators $\widehat{\boldsymbol{\theta}}_k$ and $\widehat{\sigma}_k$ should be studied and taken into account to establish the statistical performance of proposed GLRT.

B. Autoregressive Model of Medium.

Another possible approach to dealing with the nuisance parameter $\boldsymbol{\theta}$ is by using a local autoregressive (AR) model of inspected medium. Such models have been used in image



(a) Power of proposed test $\beta_{\text{glr}}(\varrho)$ as a function of false-alarm probability α_0 for different embedding rates R and different parametric models.



(b) Comparison between empirical (□ , ○, and ◊) and theoretical (dashed lines) distributions of Λ_{glr} under both hypotheses $\mathcal{H}_0$ and $\mathcal{H}_1$.

Fig. 3: Comparisons of empirical and theoretical (dashed lines) properties of proposed test δ_{glr} on simulated data.

processing [36] and specifically for LSB replacement detection through the well-known Weighted Stego-image steganalysis (WS), initially proposed in [30]. The authors of [30] propose estimating $\mu_{m,n}$ by filtering the inspected image so that $\widehat{\mu}_{m,n}$ corresponds to the mean of the four surrounding pixels. The WS method has been studied thoroughly in [37]; the authors specifically enhanced the estimation of pixel expectations by testing different local filters.

Following the WS filtering method, in this paper it is proposed to estimate the parameters $\mu_{m,n}$ and $\sigma^2_{m,n}$, for digital images, as follows [37]:

$$\begin{aligned}\widehat{\mu}_{m,n} = {}& {}^1\!/_2(z_{m,n-1}+z_{m,n+1}+z_{m-1,n}+z_{m+1,n}) \\ & - {}^1\!/_4(z_{m-1,n-1}+z_{m-1,n+1}+z_{m+1,n-1}+z_{m+1,n+1}).\end{aligned} \tag{34}$$

and:

$$\begin{aligned}\widehat{\sigma}^2_{m,n} = {}& {}^1\!/_3\left[(z_{m,n-1}-\widehat{\mu}_{m,n})^2+(z_{m,n+1}-\widehat{\mu}_{m,n})^2\right. \\ & \left.+(z_{m-1,n}-\widehat{\mu}_{m,n})^2+(z_{m+1,n}-\widehat{\mu}_{m,n})^2\right].\end{aligned} \tag{35}$$

With the estimations $\widehat{\mu}_{m,n}$ and $\widehat{\sigma}^2_{m,n}$ defined in Equations (34) - (35), the proposed test based on AR model is given by:

$$\delta_{\text{ar}}(\mathbf{Z}) = \begin{cases} \mathcal{H}_0 & \text{if} \quad \Lambda_{\text{ar}}(\mathbf{Z}) \leq \tau_{\alpha_0} \\ \mathcal{H}_1 & \text{if} \quad \Lambda_{\text{ar}}(\mathbf{Z}) > \tau_{\alpha_0}, \end{cases} \tag{36}$$

$$\Lambda_{\text{ar}}(\mathbf{Z}) = \frac{\widehat{\bar{\sigma}}^2}{\sqrt{2MN}} \sum_{m=1}^{M}\sum_{n=1}^{N} \frac{(z_{m,n}-\widehat{\mu}_{m,n})^2-{}^1\!/_{12}-\widehat{\sigma}^2_{m,n}}{\widehat{\sigma}^4_{m,n}},$$

and $\widehat{\bar{\sigma}}^4 = K^{-1}\sum_{k=1}^{K}\widehat{\sigma}_k^{-4}$, represents the estimated "mean squared variance".

Though the numerical results presented in the next Section VI show that the test δ_{ar} has a very good detection power, its parameters (especially decision threshold and detection power) can not be established statistically. Indeed, estimations $\widehat{\mu}_{m,n}$ and $\widehat{\sigma}^2_{m,n}$, given in Equations (34) and (35) do not correspond to a rigorous statistical estimation but rather to a simple ad-hoc procedure. Therefore, the statistical properties of these estimations are unknown, which prevents us establishing the distribution of Λ_{ar}.

VI. Numerical Simulations

One of the main motivations for this paper is to show that the hypothesis testing theory can be applied in practice to design a statistical test with known statistical properties for LSB matching steganalysis.

To verify that the proposed test δ_{glr} (30) performs as established in Theorem 3, a numerical simulation was performed on simulated data. The Monte-Carlo simulation was repeated $5{\cdot}10^4$ times by generating $K = 200$ blocks of $L = 32$ samples which follow the linear parametric model (27) - (28) with $\sigma_n = 3.78$ and $\Delta = 1$. Two different matrices $\mathbf{H}$, with $p = 10$ and $p = 16$ parameters, and two different embedding rates, $R = 0.91$ and $R = 0.34$, are used. The results are presented in Figure 3 in two different ways. First, Figure 3a offers a comparison between theoretical and empirical detection power as a function of prescribed false-alarm probability α_0 (ROC curves). Figure 3a highlights that the expected detection power fits almost perfectly the observed results. Similarly, Figure 3b

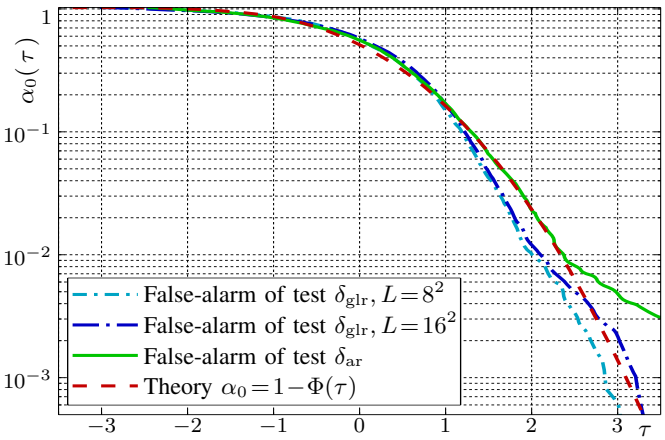


Fig. 4: Comparison between theoretically established false-alarm probability and empirically observed false-alarm probability as a function of decision threshold τ_{α_0}. Empirical Results are obtained using the 10 000 raw images from BOWS database (version 1.00).

presents the comparison between theoretical and empirical distribution of $\Lambda_{\rm glr}$ under hypotheses $\mathcal{H}_0$ and $\mathcal{H}_1$ for two different numbers of parameters and $R = 0.91$; those results also highlight the relevance of the proposed approach which permits accurately establishing of the distribution of $\Lambda_{\rm glr}$.

In addition, one of the main goal of the present paper is to propose a test which permits, in practice, the warranting of a false-alarm probability. To verify this contribution, a numerical simulation is performed on on the 10000 raw images from BOSS database [20]. Prior to our experimentation, those image are converted in 8bits grayscale image using the software *DCRAW* (with command dcraw -j -D). Then images are cropped to 512×512 pixels extracted from the red channel. The comparison between the theoretically establish false-alarm probability and the empirically obtained false-alarm probability of the proposed tests are presented in Figure 4. This particularly shows that the empirical false-alarm probability are very close to the theoretical result except for the test $\Lambda_{\rm ar}$ probability because it relies on estimations not rigorous but rather ad-hoc.

Another main motivation of the present paper is to design an efficient statistical test for LSB matching detection. To highlight the efficiency of proposed tests, a numerical comparison with state-of-the-art detectors on large image databases is required. The potential competitors for LSB matching detection are not as numerous as for LSB replacement. As briefly described in the introduction, the operational context selected in this paper makes difficult all prior-art detectors based on machine learning. In addition, a meaningful comparison with machine learning based detectors might be difficult due to the well-known cover-source mismatch problem [20]. Almost every other detector found in the literature is based on the image histogram. For the present comparison, two recent histogram-based detectors, namely the ALE (amplitude of local extrema [7]) and the 2D-HCF (adjacency Histogram Characteristic Function [19]) detector, were used due to their high detection performance. In addition, for a meaningfull comparison with prior-art, the test recently proposed in [38] was used in numerical experimentation; in fact the test proposed in [38] is rather similar to the one proposed in this paper as its a based on a simplistic GLRT which exploits an Autoregressive (AR) model for the inspected medium. Contrary to the approach exploited in the proposed paper, the statistical performance of the test proposed in [38] is not clearly established and, in addition, the moments used in the central limit theorem are fixed from empirical results.

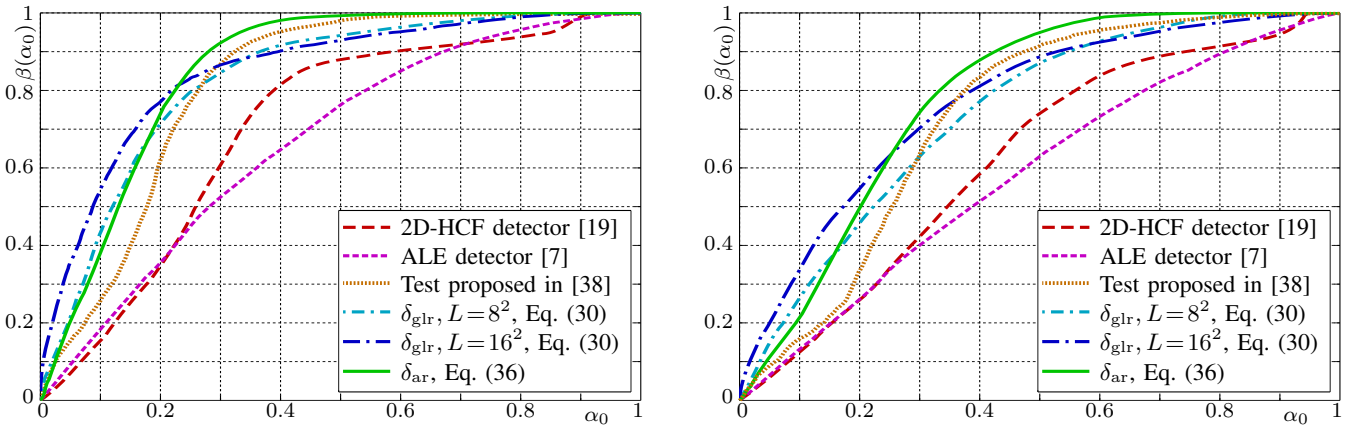
Two different parametrizations of proposed GLR test $\Lambda_{\rm glr}$ (31) are presented in Figures 5 and 6; on the one hand, the 2D-DCT is applied on blocks of size $L = 8 \times 8$ pixels and the $p = 8$ most relevant coefficients are selected while, on the other hand, the 2D-DCT is applied on blocks of size $L = 16 \times 16$ and $p = 16$ coefficients are kept.

Finally, it should be noted that the direct use of the estimated variance $\widehat{\sigma}_n^2$ may lead to numerical instability due to the terms $\widehat{\sigma}^{-2}$. For instance, on areas which are over or under-exposed, the estimated variance might be zero which obviously causes a computational problem. To tackle this problem, in the present paper the addition of a (small) constant $w = 0.3$ to the estimated variance is proposed. This technique is similar to the weighting of variance estimation proposed in the WS algorithm [30], [37], [38].

Figure 5 shows the results obtained with the 9 074 images from the Break Our Steganographic System (BOSS) contest [20]. It should be noted that the version 0.92 of the BOSS database is used here because about one third of images in version 1.00 contain artifacts at image boundaries (due to improperly implemented lens distortion correction). These artifacts might skew the steganalysis and, hence, the version 0.92 of the database is preferred. The embedding rate is $R = 1$ in Figure 5a and $R = 0.5$ in Figure 5b. Both figures show that the proposed tests achieve a better detection power for any prescribed false-alarm probability. In addition, it should be highlighted that the proposed test $\delta_{\rm ar}$ has a globally higher detection power than the proposed tests $\delta_{\rm glr}$ based on a 2D-DCT image model. However, for a very low false-alarm rate α_0, the proposed GLR test $\delta_{\rm glr}$ performs better than the test $\delta_{\rm ar}$. Finally, the ALE and the 2D-HCF detector has very poor detection power for low false-alarm probabilities, typically $\alpha_0 \in (0, 0.2]$. However, the 2D-HCF detector achieves a rather good detection power for much higher false-alarm probability, typically $\alpha_0 \in [0.3, 0.5]$. The explanation of this phenomenon is out the scope of present paper. Nevertheless, it should be noted that a test which can only detect hidden information accurately with such a high false-alarm probability is hardly usable in a practical forensics application, due to the large number of inspected media.

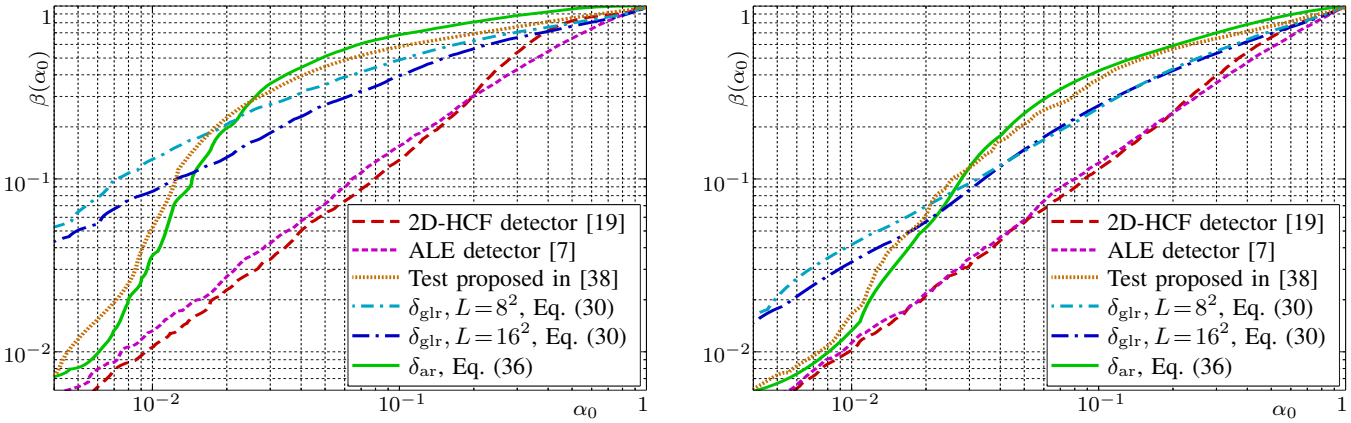
Similarly, the results presented in Figure 6 offer another numerical comparison of detectors performance. For a meaningful comparison, it is proposed to use another image database, from the second edition of Break Our Watermarking System (BOWS) contest[1]. This database is made up of 10 000 grayscale images, all of size 512×512 pixels. The embedding rate was $R = 0.5$ in Figure 6a and $R = 0.25$ in Figure 6b. In order to emphasize the fact that proposed test has a much higher detection power than the competitors for low false-alarm probabilities, the results are presented in Figures 6a and 6b using a logarithmic scale. On the one hand, Figure 6 emphasizes that the proposed GLR test $\delta_{\rm glr}$ performs better than the test $\delta_{\rm ar}$ for low false-alarm rate α_0. On the other hand, the detection power of 2D-HCF and ALE detectors is almost equal to the false-alarm probability; those tests do not perform much better than a random guess for low false-alarm rate α_0. On the contrary, the test proposed in [38] exhibits rather good performance; it perform almost as well as the AUMP test proposed in this paper based on a Autoregressive (AR) model for inspected medium. For low false-alarm probability, the AUMP test using a 2D-DCT adaptative model performs much better that the tests [38] and $\delta_{\rm ar}$ (36) based on AR model. Finally, it should be noted that the images from the two used databases are not raw (unprocessed) images. These database are chosen because they most likely represents the inspected images in practice. However, the post-acquisition processes used to rendered a full color and high quality image certainly introduces a statistical correlation and might changes slightly

[1]BOWS database is available on Internet website: http://bows2.ec-lille.fr/



(a) ROC curves for $R = 1$. (b) ROC curves for $R = 0.5$.

Fig. 5: Numerical comparisons of detectors performance using BOSS database [20].



(a) ROC curves for $R = 0.5$. (b) ROC curves for $R = 0.25$.

Fig. 6: Numerical comparisons of detectors performance using BOWS database.

the pixels' Gaussian distribution, see [42]. Therefore the proposed AUMP test might be sub-optimal for such image because the pixels might not follow the independent Gaussian distribution which describes null hypothesis $\mathcal{H}_0$. However, figures 5 and 6 shows that its performs better that its competitors for such "rendered" images.

VII. Conclusion and Future Works.

The paper presents cast the detection of data hidden with the LSB matching scheme within the framework of hypothesis testing theory. The main contribution is threefold. First, when the cover medium parameters are known, the most-powerful LRT is established. Based on the LRT, an AUMP test, which asymptotically maximizes the detection power whatever the hidden data embedding rate might be, is presented. Second, the detection power of the proposed AUMP test is analytically calculated. This particularly allows us to define an upper bound for the detection power of any detector. Lastly, when inspected medium parameters are unknown, two practical tests are proposed based on two different local estimations of unknown parameters.

The relevance of the proposed approach is emphasized through numerical experiments. Compared to two state-of-the-art detectors, the proposed practical test achieves a better detection power.

Acknowledgment.

The authors would like to thank reviewer 3 for his/her helpful comments and suggestions as we believe that these have greatly improve the quality of the paper.

Appendix A
Demonstration of Theorems 1 and 2

The Theorem 2 is proved in three steps. First, the exact expression of the LR $\Lambda_R(z_n)$ together with its Taylor series expansion are detailed. Then, the two first moments of $\Lambda_{\text{aump}}(z_n)$ are calculated under both hypotheses $\mathcal{H}_0$ and $\mathcal{H}_1$; this allows us to establish the asymptotic distributions of $\Lambda_{\text{aump}}(z_n)$ under both hypotheses and to calculate the parameters of test δ_{aump}. Finally, the AUMP property of the proposed test δ_{aump} is proved.

A. Expressions of the LR $\Lambda_R(z_n)$

When the embedding rate R and the parameter $\theta_n = (\mu_n, \sigma_n)^T$ are known, the LR $\Lambda_R(z_n)$ can be written from Equation (7) as:

$$\begin{aligned}\Lambda_R(z_n) &= \log \frac{q^R_{\theta_n}[z_n]}{p_{\theta_n}[z_n]} \\ &= \log\left(1+\frac{R}{2}\left(\frac{p_{\theta_n}[z_n-1]+p_{\theta_n}[z_n+1]}{2p_{\theta_n}[z_n]}-1\right)\right).\end{aligned} \tag{37}$$

From the definition of probability $p_{\theta_n}[z_n]$ given in Equations (4) and (5) one obtains:

$$\begin{aligned}\frac{p_{\theta_n}[z_n-1]}{p_{\theta_n}[z_n]} &= \frac{\frac{1}{\sigma_n}\phi\left(\frac{z_n-1-\mu_n}{\sigma_n}\right)}{\frac{1}{\sigma_n}\phi\left(\frac{z_n-\mu_n}{\sigma_n}\right)}+o\left(\sigma_n^{-2}\right) \\ &= \frac{\exp\left(-\frac{(z_n-\mu_n)^2+1-2(z_n-\mu_n)}{2\sigma_n^2}\right)}{\exp\left(-\frac{(z_n-\mu_n)^2}{2\sigma_n^2}\right)}+o\left(\sigma_n^{-2}\right) \\ &= \exp\left(-\frac{1}{2\sigma_n^2}\right)\exp\left(\frac{z_n-\mu_n}{\sigma_n^2}\right)+o\left(\sigma_n^{-2}\right).\end{aligned} \tag{38}$$

The same calculation gives (13):

$$\frac{p_{\theta_n}[z_n+1]}{p_{\theta_n}[z_n]} = \exp\left(-\frac{1}{2\sigma_n^2}\right)\exp\left(\frac{\mu_n-z_n}{\sigma_n^2}\right)+o\left(\sigma_n^{-2}\right).$$

which together with (38) allows us to write (14):

$$\begin{aligned}&\frac{1}{2}\frac{p_{\theta_n}[z_n-1]+p_{\theta_n}[z_n+1]}{p_{\theta_n}[z_n]} = \\ &\frac{1}{2}\exp\left(-\frac{1}{2\sigma_n^2}\right)\left[\exp\left(\frac{\mu_n-z_n}{\sigma_n^2}\right)+\exp\left(\frac{z_n-\mu_n}{\sigma_n^2}\right)\right]+o\left(\sigma_n^{-2}\right).\end{aligned}$$

As previously discussed, it is considered in this paper that Δ/ς_n tends to 0, hence, a Taylor series expansion of $\exp(x)$ around $x=0$ immediately gives:

$$\frac{p_{\theta_n}[z_n-1]+p_{\theta_n}[z_n+1]}{2p_{\theta_n}[z_n]}-1 = -\frac{1}{2\sigma_n^2}+\frac{(z_n-\mu_n)^2+1/4}{2\sigma_n^4}+o(\sigma_n^{-4}),$$

which put into the function $\log(1+x\,R/2)$, as given in Equation (37), finally gives the following Taylor series expansion of the LR $\Lambda_R(z_n)$:

$$\Lambda_R(z_n) = -\frac{R}{4\sigma_n^2}+\frac{R}{4\sigma_n^4}\left((z_n-\mu_n)^2+1/4\right)-\frac{R^2}{32\sigma_n^4}+o(\sigma_n^{-4}) \tag{39}$$

which proves Equation (15).

B. Moments of $\Lambda_{\text{aump}}(z_n)$ and Asymptotic Distribution of $\Lambda_{\text{aump}}(\mathbf{Z})$

Let us first recall that the proposed AUMP test δ_{aump}, as defined in Equation (18), is based on:

$$\Lambda_{\text{aump}}(z_n) = \frac{(z_n-\mu_n)^2-1/12-\sigma_n^2}{\sigma_n^4}. \tag{40}$$

Obviously $\Lambda_{\text{aump}}(z_n)$ depends on the observation only through the term $(z_n-\mu_n)^2$.

Under hypothesis $\mathcal{H}_0$, from the properties of Gaussian distribution and from the general results given in [33] one has:

$$\mathbb{E}_0\left[(z_n-\mu_n)^2\right] = \sigma_n^2+1/12+o\left(\sigma_n^{-2}\right). \tag{41}$$

For the variance, it follows from König-Huyghens theorem that:

$$\mathbb{V}ar_0\left[(z_n-\mu_n)^2\right] = \mathbb{E}_0\left[(z_n-\mu_n)^4\right]-\mathbb{E}_0\left[(z_n-\mu_n)^2\right]^2 \tag{42}$$

with:

$$\mathbb{E}_0\left[(z_n-\mu_n)^4\right] = 3\sigma_n^4+o\left(\sigma_n^4\right)$$

Hence it immediately follows that :

$$\mathbb{V}ar_0\left[(z_n-\mu_n)^2\right] = 3\sigma_n^4-\sigma_n^4+o\left(\sigma_n^4\right) = 2\sigma_n^4+o\left(\sigma_n^4\right) \tag{43}$$

From Equations (41) and (43) a short algebra gives:

$$\begin{aligned}&\mathbb{E}_0\left[\Lambda_{\text{aump}}(z_n)\right] = 0+o\left(\sigma_n^{-4}\right) \\ \text{and}\quad &\mathbb{V}ar_0\left[\Lambda_{\text{aump}}(z_n)\right] = \frac{2}{\sigma_n^4}+o\left(\sigma_n^{-4}\right).\end{aligned} \tag{44}$$

Recalling that $\Lambda_{\text{aump}}(\mathbf{Z})$ is defined in Equation (19) as:

$$\begin{aligned}\Lambda_{\text{aump}}(\mathbf{Z}) &= \frac{\bar{\sigma}^2}{\sqrt{2N}}\sum_{n=1}^{N}\Lambda_{\text{aump}}(z_n), \\ \text{with}\quad \bar{\sigma}^{-4} &\stackrel{\text{def.}}{=} N^{-1}\sum_{n=1}^{N}\sigma_n^{-4}.\end{aligned} \tag{45}$$

In virtue of the Lindeberg central limit theorem, as Δ/ς_n tends to 0 and as N tends to infinity, the LR $\Lambda_{\text{aump}}(\mathbf{Z})$ satisfies:

$$\Lambda_{\text{aump}}(\mathbf{Z}) \rightsquigarrow \mathcal{N}(0,1) \tag{46}$$

Finally, it follows from (46) that for any $\tau_{\alpha_0} \in \mathbb{R}$:

$$\alpha_0(\delta_{\text{aump}}) = \mathbb{P}_0\left[\Lambda_{\text{aump}}(\mathbf{Z}) > \tau_{\alpha_0}\right] = 1-\Phi\left(\tau_{\alpha_0}\right).$$

and as Φ is strictly increasing, it asymptotically holds that:

$$(1-\alpha_0(\delta_{\text{aump}})) = \Phi(\tau_{\alpha_0}) \Leftrightarrow \tau_{\alpha_0} = \Phi^{-1}\left(1-\alpha_0(\delta_{\text{aump}})\right), \tag{47}$$

which proves the first part of Theorem 1.

Under hypothesis $\mathcal{H}_1$, from the general results given in [33], it follows that:

$$\mathbb{E}_0\left[(z_n+1-\mu_n)^2\right] = \mathbb{E}_0\left[(z_n-1-\mu_n)^2\right] = \sigma_n^2+1+o\left(\sigma_n^{-2}\right)$$

Hence, it follows that :

$$\mathbb{E}_1\left[(z_n-\mu_n)^2\right] = \sigma_n^2+\frac{R}{2}+\frac{1}{12}+o\left(\sigma_n^{-2}\right). \tag{48}$$

Similarly, for the variance a short algebra shows that :

$$\mathbb{E}_0\left[(z_n+1-\mu_n)^4\right] = \mathbb{E}_0\left[(z_n-1-\mu_n)^4\right] = 3\sigma_n^4+o\left(\sigma_n^{-4}\right)$$

Hence, it follows from the König-Huyghens theorem that:

$$\mathbb{V}ar_1\left[(z_n-\mu_n)^2\right] = 2\sigma_n^4+o\left(\sigma_n^4\right) \tag{49}$$

From Equations (48) and (49) a short algebra gives:

$$\begin{aligned}&\mathbb{E}_1\left[\Lambda_{\text{aump}}(z_n)\right] = \frac{R}{2\sigma_n^4}+o\left(\sigma_n^{-4}\right) \\ \text{and}\quad &\mathbb{V}ar_1\left[\Lambda_{\text{aump}}(z_n)\right] = \frac{2}{\sigma_n^4}+o\left(\sigma_n^{-4}\right).\end{aligned} \tag{50}$$

From Lindeberg's central limit theorem, from the definition of $\varrho = \frac{R}{\sqrt{8}\bar{\sigma}^2}$, and from (50), it follows that the LR $\Lambda_{\text{aump}}(\mathbf{Z})$ satisfies, under hypothesis $\mathcal{H}_1$:

$$\Lambda_{\text{aump}}(\mathbf{Z}) \rightsquigarrow \mathcal{N}(\sqrt{N}\varrho, 1). \tag{51}$$

Hence, it follows from (51) that, for any decision threshold $\tau_{\alpha_0} \in \mathbb{R}$, the power of the test δ_{aump} is given by:

$$\beta_{\text{aump}}(\varrho) = \mathbb{P}_1\left[\Lambda_{\text{aump}}(\mathbf{Z}) > \tau_{\alpha_0}\right] = 1 - \Phi\left(\tau_{\alpha_0} - \sqrt{N}\varrho\right).$$

By substituting $\widetilde{\tau}_{\alpha_0}$ by the value given in Theorem 1 and in Equation (47), it is obvious that:

$$\beta_{\text{aump}}(\varrho) = 1 - \Phi\left(\Phi^{-1}(1-\alpha_0) - \sqrt{N}\varrho\right) \tag{52}$$

which proves Theorem 1

C. AUMP property of the test δ_{aump}

The easiest way to prove that the proposed test δ_{aump} is AUMP is given by the following relation between the exact expression (39) of $\Lambda_R(z_n)$ and $\Lambda_{\text{aump}}(z_n)$ (40):

$$\Lambda_R(z_n) = R\Lambda_{\text{aump}}(z_n)\frac{R}{16\sigma_n^4}\left(1 - \frac{R}{2}\right) + o(\sigma_n^{-4}). \tag{53}$$

Roughly speaking, scaling by a constant factor and/or adding a constant only changes *mutatis mutandis* the decision threshold, but does not change the detection power as a function of false-alarm probability $\beta(\alpha_0)$ on which the AUMP criterion is based.

However, the formal proof of AUMP property of proposed test δ_{aump} serves as a formalization of the assumption refered to Δ/ς_n tends to 0. This situation is captured by adopting the notation that quantization step Δ_j depends on some index j such that $\Delta_j \to 0$ as $j \to \infty$. Theoretically, the following conditions should be satisfied, in order to avoid mathematical complications:

- A-1 The set $\{\mu_n\}_{n=1}^N$ is uniformly bounded, *i.e.* $\exists M \in \mathbb{R} \,/\, \sup_n |\mu_n| < M$.
- A-2 The number of quantization levels, here denoted q_j, also depends on index j such that the $\Delta_j q_j \to \infty$ as $j \to \infty$.

Those two assumptions ensure that, first, the probability of exceeding quantizer bounds tends to 0 as j tends to infinity and, second, that $Q_{\Delta_j}(x) \to x$. In this framework z_n should be replaced with $z_{n,j}$ and some results given in this Appendix A should formally be read as the limit of such sequences, see [24]. For clarity those notations were dramatically simplified.

Finally, in this framework, it can be noted that from Equation (53) that in virtue of Slutsky's theorem [31, Theorem 11.2.11], the test δ_{aump} is AUMP as $j \to \infty$ under assumptions A-1 and A-2.

APPENDIX B
DEMONSTRATION OF THEOREM 3: ASYMPTOTIC DISTRIBUTION OF $\Lambda_{\text{glr}}(\mathbf{Z})$

The demonstration of Theorem 3 is limited to the establishment of asymptotic distribution of $\Lambda_{\text{glr}}(\mathbf{Z})$; the expression of the proposed test's, $\delta_{\text{glr}}(\mathbf{Z})$, asymptotic false-alarm probability and detection power are immediate using the results from Appendix A-B.

For the sake of clarity, let us define $\gamma_k = \sum_{l=1}^{L}(\widehat{\theta}_{k,l} - z_{k,l})^2$ such that from Equation (31):

$$\Lambda_{\text{glr}}(\mathbf{z}_k) = \gamma_k - (L-p)\frac{1/12 + \sigma_k^2}{\widehat{\sigma}_k^4}.$$

The asymptotic distribution of $\Lambda_{\text{glr}}(\mathbf{Z})$ under both hypotheses is established by calculating the two first moments of $\Lambda_{\text{glr}}(\mathbf{z}_k)$ and then applying Lindeberg's central limits theorem. Under hypothesis $\mathcal{H}_0$ it follows from properties of Gaussian random variables and [33] that:

$$\mathbb{E}\left[\gamma_k\right] = \text{trace}(\mathbf{I}_L - \mathbf{P}_H)\left(\sigma_n^2 + 1/12 + o\left(\sigma_n^{-2}\right)\right), \tag{54}$$

where $\mathbf{I}_L$ represents the identity matrix of size L, $\text{trace}(\cdot)$ denotes the trace operator and $\text{trace}(\mathbf{I}_L - \mathbf{P}_H) = L - p$. It also follows from the König-Huyghens theorem that:

$$\mathbb{V}ar\left[\gamma_k\right] = \text{trace}(\mathbf{I}_L - \mathbf{P}_H)\left(2\sigma_n^4 + o\left(\sigma_n^4\right)\right), \tag{55}$$

Hence a short algebra immediately established that:

$$\begin{aligned} &\mathbb{E}_0\left[\Lambda_{\text{glr}}(\mathbf{z}_k)\right] = 0 + o\left((L-p)\sigma_n^{-4}\right), \\ \text{and} \quad &\mathbb{V}ar_0\left[\Lambda_{\text{glr}}(\mathbf{z}_k)\right] = (L-p)\left(\frac{2}{\sigma_n^4} + o\left(\sigma_n^{-4}\right)\right). \end{aligned} \tag{56}$$

and from the definition of $\Lambda_{\text{glr}}(\mathbf{Z})$ (31) and ϱ (23) it finally follows that under hypothesis $\mathcal{H}_0$:

$$\Lambda_{\text{glr}}(\mathbf{Z}) \rightsquigarrow \mathcal{N}(0,1).$$

Similarly, under hypothesis $\mathcal{H}_1$, one has

$$\mathbb{E}\left[\gamma_k\right] = \text{trace}(\mathbf{I}_L - \mathbf{P}_H)\left(\frac{R}{2} + \sigma_n^2 + \frac{1}{12} + o\left(\sigma_n^{-2}\right)\right), \tag{57}$$

where $\mathbf{I}_L$ represents the identity matrix of size L, $\text{trace}(\cdot)$ denotes the trace operator and $\text{trace}(\mathbf{I}_L - \mathbf{P}_H) = L - p$. It also follows from the König-Huyghens theorem that:

$$\mathbb{V}ar\left[\gamma_k\right] = \text{trace}(\mathbf{I}_L - \mathbf{P}_H)\left(2\sigma_n^4 + o\left(\sigma_n^4\right)\right), \tag{58}$$

Hence a short algebra immediately established that:

$$\begin{aligned} &\mathbb{E}_0\left[\Lambda_{\text{glr}}(\mathbf{z}_k)\right] = (L-p)\left(\frac{R}{2\sigma_k^4} + o\left(\sigma_n^{-4}\right)\right), \\ \text{and} \quad &\mathbb{V}ar_0\left[\Lambda_{\text{glr}}(\mathbf{z}_k)\right] = (L-p)\left(\frac{2}{\sigma_n^4} + o\left(\sigma_n^{-4}\right)\right). \end{aligned} \tag{59}$$

and from the definition of $\Lambda_{\text{glr}}(\mathbf{Z})$ and ϱ it finally follows from Lindeberg's central limit theorem that:

$$\Lambda_{\text{glr}}(\mathbf{Z}) \rightsquigarrow \mathcal{N}(\sqrt{K(L-p)}\varrho, 1).$$

Theorem 3 immediately follows from the asymptotic distributions of $\Lambda_{\text{glr}}(\mathbf{Z})$ under both hypotheses and a short probability calculus, see Appendix A-B.

REFERENCES

[1] G. Simmons, "The prisoners problem and the subliminal channel," *CRYPTO*, pp. 51–67, 1983.

[2] J. Fridrich and J. Kodovský, "Steganalysis of LSB replacement using parity-aware features," to be published in *Information Hiding*, LNCS, Springer, 2012.

[3] R. Böhme, *Advanced Statistical Steganalysis*, 1st ed. Springer Publishing Company, Incorporated, 2010.

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

[5] J. Fridrich, *Steganography in Digital Media: Principles, Algorithms, and Applications*, 1st ed. Cambridge University Press, 2009.

[6] G. Cancelli, G. Doerr, M. Barni, and I. Cox, "A comparative study of ± 1 steganalyzers," in *Multimedia Signal Processing, IEEE Workshop on*, 2008, pp. 791 –796.

[7] J. Zhang, I. Cox, and G. Doerr, "Steganalysis for LSB matching in images with high-frequency noise," in *Multimedia Signal Processing, IEEE Workshop on*, 2007, pp. 385 –388.

[8] J. Fridrich, M. Goljan, and D. Soukal, "Wet paper codes with improved embedding efficiency," *Information Forensics and Security, IEEE Transactions on*, vol. 1, no. 1, pp. 102 – 110, 2006.

[9] C. Munuera, "Steganography and error-correcting codes," *Signal Processing*, vol. 87, no. 6, pp. 1528 – 1533, 2007.

[10] C.-H. Yang, C.-Y. Weng, S.-J. Wang, and H.-M. Sun, "Adaptive data hiding in edge areas of images with spatial LSB domain systems," *Information Forensics and Security, IEEE Transactions on*, vol. 3, no. 3, pp. 488 –497, 2008.

[11] W. Luo, F. Huang, and J. Huang, "Edge adaptive image steganography based on LSB matching revisited," *Information Forensics and Security, IEEE Transactions on*, vol. 5, no. 2, pp. 201 –214, 2010.

[12] T. Pevný, T. Filler, and P. Bas, "Using high-dimensional image models to perform highly undetectable steganography," in *Information Hiding*, LNCS vol.6387, Springer, 2010, pp. 161–177.

[13] G. Cancelli, G. Doerr, I. Cox, and M. Barni, "Detection of ± 1 LSB steganography based on the amplitude of histogram local extrema," in *Image Processing, 2008, IEEE International Conference on*, 2008, pp. 1288 –1291.

[14] K. Sullivan, U. Madhow, S. Ch, and B. S. Manjunath, "Steganalysis for markov cover data with applications to images," *IEEE Trans. Inform. Forensics and Security*, vol. 1, no. 2, pp. 275–287, 2006.

[15] M. Goljan, J. Fridrich, and T. Holotyak, "New blind steganalysis and its implications," in *Security, Steganography, and Watermarking of Multimedia Contents VIII*, Proc. SPIE, 2006, pp. 1–13.

[16] S. Lyu and H. Farid, "Steganalysis using higher-order image statistics," *Information Forensics and Security, IEEE Transactions on*, vol. 1, no. 1, pp. 111 – 119, 2006.

[17] C. Scott, "Performance measures for Neyman-Pearson classification," *IEEE Trans. Inform. Theory*, vol. 53, no. 8, pp. 2852–2863, 2007.

[18] J. Harmsen and W. Pearlman, "Higher-order statistical steganalysis of palette images," in *Security, Steganography, and Watermarking of Multimedia Contents V*, Proc. SPIE, vol. 5020, 2005.

[19] A. Ker, "Steganalysis of LSB matching in grayscale images," *Signal Processing Letters, IEEE*, vol. 12, no. 6, pp. 441 – 444, 2005.

[20] P. Bas, T. Filler, and T. Pevný, "Break our steganographic system — the ins and outs of organizing boss," in *Information Hiding*, LNCS vol.6958, Springer, 2011, pp. 59–70.

[21] J. Fridrich and J. Kodovsky, "Rich models for steganalysis of digital images," *Information Forensics and Security, IEEE Transactions on*, vol. 7, no. 3, pp. 868 –882, june 2012.

[22] O. Dabeer, K. Sullivan, U. Madhow, S. Chandrasekaran, and B. Manjunath, "Detection of hiding in the least significant bit," *Signal Processing, IEEE Transactions on*, vol. 52, no. 10, pp. 3046 – 3058, 2004.

[23] R. Cogranne, C. Zitzmann, L. Fillatre, F. Retraint, I. Nikiforov, and P. Cornu, "Statistical decision by using quantized observations," in *IEEE International Symposium on Information Theory*, 2011, pp. 1135 – 1139.

[24] L. Fillatre, "Adaptive Steganalysis of Least Significant Bit Replacement in Grayscale Natural Images," *Image Processing, IEEE Transactions on*, vol. 60, no. 2, pp. 556–569, 2012.

[25] R. Cogranne, C. Zitzmann, L. Fillatre, I. Nikiforov, F. Retraint, and P. Cornu, "A cover image model for reliable steganalysis," in *Information Hiding*, LNCS vol.6958, Springer, 2011, pp. 178–192.

[26] A. Foi, M. Trimeche, V. Katkovnik, and K. Egiazarian, "Practical poissonian-gaussian noise modeling and fitting for single-image raw-data," *Image Processing, IEEE Transactions on*, vol. 17, no. 10, pp. 1737–1754, 2008.

[27] G. Healey and R. Kondepudy, "Radiometric CCD camera calibration and noise estimation," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 16, no. 3, pp. 267–276, 1994.

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

[29] C. Zitzmann, R. Cogranne, F. Retraint, I. Nikiforov, L. Fillatre, and P. Cornu, "Statistical decision methods in hidden information detection," in *Information Hiding*, LNCS vol.6958 Springer, 2011, pp. 163–177.

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

[31] E. Lehmann and J. Romano, *Testing Statistical Hypotheses, Second Edition*, 3rd ed. Springer, 2005.

[32] R. Cogranne, C. Zitzmann, I. Nikiforov, F. Retraint, L. Fillatre, and P. Cornu, "Statistical Detection of LSB Matching in the Presence of Nuisance Parameters," to be published in *Statistical Signal Processing, Proc. of IEEE Workshop on* , 2012.

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

[34] A. D. Ker, "A capacity result for batch steganography," *Signal Processing Letters*, vol. 14, no. 8, pp. 525–528, 2007.

[35] V. Katkovnik, K. Egiazarian, and J. Astola, *Local Approximation Techniques in Signal and Image Processing*. SPIE Press, 2006.

[36] R. Dubes and A. Jain, "Random field models in image analysis," *Journal of applied statistics*, vol. 16, no. 2, pp. 131–164, 1989.

[37] A. D. Ker and R. Böhme, "Revisiting weighted stego-image steganalysis," in *Security, Forensics, Steganography, and Watermarking of Multimedia Contents X, Proc. SPIE 6819*, 2008, pp. 501–517.

[38] R. Cogranne, C. Zitzmann, F. Retraint, I. Nikiforov, L. Fillatre, and P. Cornu, "Statistical Detection of LSB Matching Using Hypothesis Testing Theory," to be published in *Information Hiding*, LNCS, Springer, 2012.

[39] D. Donoho, M. Elad, and V. Temlyakov, "Stable recovery of sparse overcomplete representations in the presence of noise," *Information Theory, IEEE Transactions on*, vol. 52, no. 1, pp. 6 – 18, 2006.

[40] M. Elad and M. Aharon, "Image denoising via sparse and redundant representations over learned dictionaries," *Image Processing, IEEE Transactions on*, vol. 15, no. 12, pp. 3736 –3745, 2006.

[41] N. Ahmed, T. Natarajan, and K. Rao, "Discrete cosine transform," *Computers, IEEE Transactions on*, vol. C-23, no. 1, pp. 90 –93, 1974.

[42] T.H. Thai, R. Cogranne, and F. Retraint, "Statistical model of natural images," *IEEE International Conference on Image Processing*, 2012.

Rémi Cogranne received an engineering diploma / M.S. degree in computer science and telecommunication in 2008 and a PhD in systems security and optimization in 2011 both from the Troyes University of Technology. During his studies, he took a semester off to work as a volunteer teacher in Senegal and studied one semester at Jönköping, Sweden. His is currently a post-doctoral fellow in Troyes University of Technology, Lab. of system modeling and dependability. His main researches focus on statistical decision theory, with a particular application for information forensics, linear and non-linear signal and image modeling, photographic image acquisition modeling, statistical image processing ; he is currently working on applications related to digital media forensics such as hidden data detection, imaging device identification, image forgeries detection and authenticity certification.

Florent Retraint received an engineering diploma in computer science from Compiègne University of Technology in 1993, a M.S. degree in applied mathematics from ENSIMAG in 1994 and a PhD degree in applied mathematics (???) in 1998 from INSA Lyon and CEA at Grenoble. Then he held a post-doctoral position during one year at CEA Lyon and worked during two years as a research engineer in Thomsom CSF (nowadays Thales S.A). Since 2001 (???) he is an associate professor in Troyes University of Technology, Lab. of system modeling and dependability. His researches focus on image modeling, statistical image processing, hypothesis testing theory, anomaly detection and localization, with a main application to digital images forensics.