Adaptive Steganalysis of Least Significant Bit Replacement in Grayscale Natural Images

Lionel Fillatre, *Member, IEEE*

***Abstract*—This paper deals with the detection of hidden bits in the Least Significant Bit (LSB) plane of a natural image. The mean level and the covariance matrix of the image, considered as a quantized Gaussian random matrix, are unknown. An adaptive statistical test is designed such that its probability distribution is always independent of the unknown image parameters, while ensuring a high probability of hidden bits detection. This test is based on the likelihood ratio test except that the unknown parameters are replaced by estimates based on a local linear regression model. It is shown that this test maximizes the probability of detection as the image size becomes arbitrarily large and the quantization step vanishes. This provides an asymptotic upper-bound for the detection of hidden bits based on the LSB replacement mechanism. Numerical results on real natural images show the relevance of the method and the sharpness of the asymptotic expression for the probability of detection.**

***Index Terms*—Adaptive detection, information hiding, natural image, nuisance parameters, statistical hypotheses testing.**

I. Introduction

SECRET bits embedding concerns the reliable transmission of information embedded into host signals such as image, video and audio. It has an increasingly wide array of applications, from digital watermarking, document authentication to steganography [1]–[4]. Many tools are already available in the public domain and others are easy to create [5]. Unfortunately, all these applications can also be misused and, naturally, there is an interest in knowing if such hiding can be reliably detected. In addition, the huge amount of image available on the Internet shows that there is a real need to use detection algorithms with analytic statistical properties. It is especially crucial to warrant a small prescribed false alarm probability and to know in advance the probability to detect the hidden communication.

A. Information Hiding in Natural Images

The secret message is imbedded into a harmless natural image which is called the cover, or host, image. The resulting image is called the stego-image. Ideally the stego-image is indistinguishable from the original cover image, giving no indication that other information has been encoded. The stego-image is then transmitted to the receiver via an unsecured channel. The stego-image can be decoded by a receiver that knows the hiding scheme and the specific parameters (the secret key), used by the encoder, to retrieve the secret message.

An adversary can detect the hidden communication by observing the unsecured channel. The detection of hidden communication is a difficult problem because, generally, it is an ill-posed problem: the host image, the hiding rate (if data is hidden), and the secret key are unknown. Despite the intrinsic difficulty of the data hiding detection problem, its importance has led to a number of attempts at developing useful tools; see [2]–[4], [6], and [7] for a survey of the methods available in the open literature.

The most studied algorithm is undoubtedly the simple yet popular technique of hiding in the Least Significant Bit (LSB) of the cover image [8], either in the pixel or transform domain, or its variants. There can be no doubt that replacement of LSBs in digital images is a poor choice for steganography [9] but it remains popular in free steganography software. Moreover, this is the mechanism which inspires the majority of existing hiding methods. Broadly, the literature contains three main classes of detectors for LSB replacement. The first, termed structural detectors in [10], includes [10]–[15] among others; they analyze explicitly the combinatorial structure of LSB replacement in pixel groups. The second, known as Weighted Stego-image (WS) detectors, is found in [16] and [17], and involves filtering the stego-image to estimate the cover. Last, the third class contains statistical detectors [18], [19] which are derived by applying statistical techniques to the inspected image.

B. Theoretical Limits of Standard Approaches

The vast majority of methods proposed in the literature have generally unknown theoretical statistical performances, which are evaluated by using numerical experiments from large image databases. This involves three main drawbacks.

First, the performances of detection algorithms are generally evaluated with Receiver Operating Characteristic (ROC) curves. It is crucial to bear in mind that ROC curves are especially relevant for testing two simple hypotheses [20]. In presence of composite hypotheses (due to unknown cover images and unknown hiding rate), a ROC curve is not sufficient to sum up the performances of a detector. Strictly speaking, a ROC curve has to be calculated for each possible cover image content, except when it is theoretically established that the studied test is independent from the image content. This is not the case for the approaches existing in the literature.

Second, when analyzing a large number of images, it is advisable to warrant a prescribed probability of false alarm (de-

Manuscript received March 27, 2011; revised July 27, 2011; accepted October 03, 2011. Date of publication October 31, 2011; date of current version January 13, 2012. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Ta-Hsin Li. This work was supported by the ANR Grant ANR-07-SECU-004.

The author is with the ICD LM2S, Université de technologie de Troyes, UMR STMR CNRS 6279, 10010, Troyes, France (e-mail: lionel.fillatre@utt.fr).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSP.2011.2174231

clare an alarm when inspecting a cover image). Designing a detector whose probability of false alarm is theoretically controlled for all possible cover images is not addressed by standard approaches. This involves designing a test based on a decision function independent of the cover image parameters. This is the well-known concept of Constant False Alarm Rate (CFAR) detection [21]. For a CFAR test, the detection threshold can be set to warrant a prespecified false alarm probability. Such a detector is also referred to as an adaptive detector [22], [23].

Finally, no optimal bound on detection performances has been yet established in the literature, except the square root law [24] which shows that the data-hiding capacity of covers grows only with the square root of the available cover size. Hence there are no theoretical means of evaluating a new challenger test. The most common approach consists in comparing the challenger test to the best tests known in the literature. This is time consuming and not satisfactory from a theoretical point of view. Moreover, although it is intuitively clear that such a bound must depend on the hiding rate and the cover image size (among other possible parameters), this dependence is not clearly established, even in an idealized setting.

C. Main Contributions of the Paper

The goal of this paper is to design a statistical test which addresses the above mentioned drawbacks of standard approaches. For this purpose, this paper considers an original approach to detecting hidden bits in the LSB plane which consists in using a parametric model of natural images together with the theory of statistical hypotheses testing [25], [26]. The main contributions of this paper are the following:

- The proposed approach is based on a parametric model of natural images. Hence, it exploits the physical dependence which naturally exists between the image pixels. These pixels are not supposed to be identically distributed but they admit a joint Gaussian distribution.
- An adaptive Asymptotically Uniformly Most Powerful (AUMP) test is designed (under mild assumptions) to decide if a natural image contains hidden bits. This test maximizes the detection probability of hidden bits, independently of the image parameters, whatever the hiding rate. This test can meet a prescribed false alarm probability whatever the image parameters.
- The detection threshold, the probabilities of false alarm and detection of the adaptive AUMP test are analytically calculated as the size of the inspected image grows to infinity. This provides an asymptotic upper-bound for the detection of hidden bits based on LSB replacement.

To allow a simple mathematical formulation, only the LSB replacement mechanism is studied in this paper. However, since the proposed approach is based on general statistical concepts, it can be extended to more general LSB embedding methods provided that a probabilistic description of the data hiding scheme is available. Compared to the previous published works [27]–[31], this paper presents three main differences: i) it is based on the fact that the quantization step vanishes as the size of the inspected image grows to infinity; ii) it studies the AUMP criterion of optimality; and iii) it explicitly considers that the pixel variance is unknown. Finally, as a corollary of this paper, it is shown that the WS detector [17] coincides with the adaptive AUMP test provided that the tuning parameters of the WS detector are conveniently chosen. Hence, the proposed approach theoretically justifies *a posteriori* the performance of the WS detector.

D. Organization of the Paper

The paper is organized as follows. Section II starts with the problem statement. The problem of hidden bits detection is described in the framework of statistical hypothesis testing theory based on parametric models. Next, Section III proposes a statistical model for natural cover images. The statistical detection approach developed in the paper is based on this model, especially when it is necessary to estimate the unknown cover image parameters. Section IV presents the AUMP criterion of optimality. It proposes a nonadaptive AUMP test which detects hidden bits in natural images when the mean and variance of the pixels are known, i.e., when the parameters of the natural cover model are known. This test provides an asymptotic upper-bound for the detection probability of hidden bits based on the LSB replacement mechanism. In Section V, it is proved that the adaptive version of this test is also AUMP when the mean and variance of the pixels are estimated, provided that the quantization step vanishes and the image size becomes arbitrarily large. In practice, the conditions of asymptotic convergence are not totally satisfied and a theoretical formula, which estimates the error in the asymptotic approximation, is also proposed. Section VI studies the numerical performances of the proposed detection algorithm on artificial and real natural images. Some comparisons with other detectors are also presented. Finally, Section VII concludes this paper. The appendices give the proofs of the two theorems presented in the paper.

E. Main Notations

Matrices are bold capital, vectors are bold lowercase and scalars are not bold. The notation $\bar{\jmath}$ indicates the integer j with LSB flipped [16], i.e., $\bar{\jmath} = j + 1 - 2\,\mathrm{LSB}(j)$ where $\mathrm{LSB}(j)$ is the LSB of j. The main theoretical results of this paper are based on the fact that the number n of pixels is arbitrarily large. Hence, many variables are indexed by n to underline their dependence to n. For example, the quantization step Δ_n vanishes as $n \longrightarrow +\infty$. The notation $x \sim y$, with $y > 0$, means that $\frac{x}{y}$ tends to 1 as $n \longrightarrow +\infty$ (the dependance of x and y with respect to n is implicitly assumed). The notation $x = o(y)$, with $y > 0$, means that $\frac{x}{y}$ tends to 0 as $n \longrightarrow +\infty$.

The notation $X \sim P$ means that the random variable X is distributed according to the probability distribution P. Let $\boldsymbol{\theta} = (\ell, \epsilon)^\top$ be a vector composed of two reals where $\boldsymbol{U}^\top$ denotes the transpose of $\boldsymbol{U}$. The Gaussian probability density function (pdf) is denoted $f_{\boldsymbol{\theta}}(x)$ and is given by

$$f_{\boldsymbol{\theta}}(x) = \frac{1}{\sqrt{2\pi\epsilon^2}} e^{-\frac{(x-\ell)^2}{2\epsilon^2}}, \ \forall x \in \mathbb{R}.$$

The standard Gaussian cumulative distribution function is denoted by $\Phi(\cdot)$ and its inverse is $\Phi^{-1}(\cdot)$.

II. Problem Statement

This section describes the LSB replacement mechanism. It also presents the statistical hypothesis testing problem for hidden bits detection.

A. *Information Hiding Model*

This paper assumes that a cover image is a vector $\boldsymbol{c} = (c_1, \ldots, c_n)$ of n grayscale pixels with N_n levels of intensity, i.e., $c_i \in \{0, 1, \ldots, N_n - 1\}$ for all i (see details in Section III-C). The corresponding stego-image is created by replacing the LSBs of proportion R of the cover pixels. Let $P_{\boldsymbol{\theta}_i}$ be the probability distribution of the cover pixel c_i, which is denoted by

$$P_{\boldsymbol{\theta}_i} = \left\{ p_{\boldsymbol{\theta}_i}[0], p_{\boldsymbol{\theta}_i}[1], \ldots, p_{\boldsymbol{\theta}_i}[N_n - 1] \right\} \tag{1}$$

where $\boldsymbol{\theta}_i$ is a vector parameter that characterizes the distribution of c_i. Hence, the cover image depends on the vector $\boldsymbol{\theta} = (\boldsymbol{\theta}_1, \ldots, \boldsymbol{\theta}_n)$. The secret message (supposed to be encrypted) is first converted in a sequence of bits, called the hidden bits. It is assumed that each hidden bit, either 0 or 1, is equiprobable and the bits are independent and identically distributed. It is also assumed that each hidden bit is statistically independent of the cover pixels. The secret message is inserted in the cover image by using the well-known LSB replacement technique (at most one bit per pixel is modified, the LSB one), whose statistical model is given in [19]. Let T_i be the random variable defined by

$$\Pr(T_i = 0) = \Pr(T_i = 1) = \frac{R}{2} \text{ and}$$
$$\Pr(T_i = \mathrm{NULL}) = 1 - R$$

where $0 < R \leq 1$ is the hiding rate. If $T_i = \mathrm{NULL}$, no secret bit is hidden in the pixel c_i, otherwise the LSB of c_i is replaced with T_i. The probability distribution of the random variable c_i after the LSB replacement is denoted

$$Q^R_{\boldsymbol{\theta}_i} = \{q^R_{\boldsymbol{\theta}_i}[0], q^R_{\boldsymbol{\theta}_i}[1], \ldots, q^R_{\boldsymbol{\theta}_i}[N_n - 1]\}.$$

Calculation shows that

$$q^R_{\boldsymbol{\theta}_i}[j] = \frac{R}{2}\left(p_{\boldsymbol{\theta}_i}[j] + p_{\boldsymbol{\theta}_i}[\bar{j}]\right) + (1 - R)p_{\boldsymbol{\theta}_i}[j]. \tag{2}$$

B. *Hidden Bits Detection Problem*

The inspected image $\boldsymbol{y} = (y_1, \ldots, y_n)$ is either a cover image, i.e., $y_i = c_i$ for all i, or a stego-one, i.e., $y_i = c_i$ if $T_i = \mathrm{NULL}$ and $y_i = c_i$ with $\mathrm{LSB}(y_i) = T_i$ otherwise. Ideally, the goal is to test the two statistical hypotheses $\mathcal{H}_0$: $\{$no hidden bits in $\boldsymbol{y}\}$ and $\mathcal{H}_1$: $\{$presence of hidden bits in $\boldsymbol{y}\}$ formally defined by

$$\begin{aligned} \mathcal{H}_0 &= \{y_i \sim P_{\boldsymbol{\theta}_i}, \forall i \in \{1, \ldots, n\}\} \\ \mathcal{H}_1 &= \left\{y_i \sim Q^R_{\boldsymbol{\theta}_i}, \forall i \in \{1, \ldots, n\}, \forall R \in \mathcal{R}\right\} \end{aligned} \tag{3}$$

where $\mathcal{R} = (0; 1]$. When all the parameters $\boldsymbol{\theta}_i$ are known, the main difficulty in (3) is the fact that R is unknown. Since there are n observed pixels and only one unknown parameter, this problem is theoretically solvable. It must be noted that the analytic calculation of the statistical performances of the optimal solution, namely the likelihood ratio test [25], is still an open problem.

Unfortunately, in practice, the parameters $\boldsymbol{\theta}_i$ are unknown. Let $|\boldsymbol{\theta}_i|$ be the common size of all the vectors $\boldsymbol{\theta}_i$. Thus, there are more unknown parameters, $n|\boldsymbol{\theta}_i| + 1$ in total (n vectors $\boldsymbol{\theta}_i$ and R), than the number n of observed pixels. Hence, the approach proposed in this paper consists in grouping pixels in small subsets, say $\boldsymbol{y}_k$, of size m such that the joint distribution of $\boldsymbol{y}_k$ is statistically characterized by only few parameters, say $q + 1 < m$ (see details in Section III). This reduction in the number of parameters is possible because of the redundancies which exist between the pixels of the same group. Let $\boldsymbol{\omega}_k$ be the unknown parameter vector of size $q{+}1$ describing the kth subset of pixels and let $\boldsymbol{\omega} = (\boldsymbol{\omega}_1, \ldots, \boldsymbol{\omega}_{K_n})$ be the vector composed of all image parameters where K_n is the number of subsets. The domain of definition of $\boldsymbol{\omega}$ is denoted Ω_n. Then, it is proposed to solve the alternative hypotheses testing problem between $\underline{\mathcal{H}}_0$ and $\underline{\mathcal{H}}_1$ defined by

$$\begin{aligned} \underline{\mathcal{H}}_0 &= \{\boldsymbol{y}_k {\sim} P_{\boldsymbol{\omega}_k}, \forall k = 1, \ldots, K_n, \forall \boldsymbol{\omega} \in \Omega_n\}, \\ \underline{\mathcal{H}}_1 &= \{\boldsymbol{y}_k {\sim} Q^R_{\boldsymbol{\omega}_k}, \forall k = 1, \ldots, K_n, \forall \boldsymbol{\omega} \in \Omega_n, \forall R \in \mathcal{R}\} \end{aligned} \tag{4}$$

where $P_{\boldsymbol{\omega}_k}$, respectively, $Q^R_{\boldsymbol{\omega}_k}$, is the joint distribution of $\boldsymbol{y}_k$ in absence, respectively, in presence, of hidden bits. The decision problem (4) is not equivalent to the ideal one (3) except when all the parameters $\boldsymbol{\theta}_i$ are known. If not, they are almost equivalent provided that m is large and q is rather small.

In order to solve (4), it is clear that knowing the distribution of small cover pixel subsets, and especially its parameters $\boldsymbol{\omega}_k$, is crucial. The next section focuses on the definition of such a statistical model for natural images.

III. Statistical Model of the Cover Image

This section deals with the statistical description of subsets of natural cover image pixels, which is central to the design of a statistical test for hidden bits detection. The main goal of this section is to obtain a model with fewer unknown parameters than the number of pixels in the inspected image.

A. *Natural Raw Pixels Model*

This paper deals with natural images, i.e., images which are acquired by a digital imaging sensor. A fundamental model of natural raw images is given in [32] for cameras equipped with a charge-coupled device (CCD). The cover image pixel c_i, which corresponds to the grayscale level at position $s_i \in \mathbb{Z}^2$ of the cover image (considered as a matrix), is obtained by quantizing the raw natural pixel intensity x_i. The raw intensity x_i is the value (proportional to the number of photons collected) recorded by the CCD matrix element at position s_i. Let $\mathcal{S} \subset \mathbb{Z}^2$ be the pixel position set, which is typically described by the enumeration of its n elements with respect to the lexicographic order: $\mathcal{S} = \{s_1, \ldots, s_n\}$. Let x_i be the noisy raw pixel intensity at position s_i given by [33]

$$x_i = \ell_i + \xi_i \tag{5}$$

where ℓ_i is the mathematical expectation of the raw pixel x_i and ξ_i is a zero-mean independent Gaussian random noise with standard deviation $\epsilon_i>0$, which is denoted by $\xi_i \sim \mathcal{N}(0,\epsilon_i^2)$. It is important to note that the raw pixels are statistically independent [33], [34]. As discussed in [33], this model is a suitable approximation of noisy raw images produced by a digital imaging sensor. The random variable x_i follows a Gaussian distribution whose pdf $f_{\boldsymbol{\theta}_i}(x)$ is entirely characterized by the vector $\boldsymbol{\theta}_i = (\ell_i, \epsilon_i)^\top$.

B. Natural Raw Pixels Subset Model

Since $\boldsymbol{\theta}_i$ is unknown for each pixel, there are more unknown parameters than the number n of pixels. Hence the model (5) is not very useful in its present state. For this reason, it is assumed that the image is locally stationary. Thus it is proposed to partition the set $\mathcal{S}$ into K_n nonoverlapping subsets $\mathcal{S}_k = \{s_{k,1},\ldots,s_{k,m}\}$ of size m. A raw pixel x_i (and analogously c_i, ℓ_i, ϵ_i and $\boldsymbol{\theta}_i$) is also denoted $x_{k,j}$ to underline that it is the jth pixel of $\mathcal{S}_k$. The assumption of local stationarity involves that

$$\epsilon_{k,j}^2 \approx \sigma_k^2,\ \forall j \in \{1,\ldots,m\} \tag{6}$$

where σ_k^2 is a constant depending of the subset $\mathcal{S}_k$. The notation K_n indicates that the number of subsets depends on the total number n of pixels. In the following treatment, it will be assumed that $K_n \longrightarrow +\infty$ as $n \longrightarrow +\infty$. In practice, each row is viewed as a "smooth" one-dimensional signal and each subset of pixels corresponds to a segment of m contiguous pixels extracted from the same row. Obviously, according to the image size and the chosen value of m, some pixels can be discarded. For simplicity, it is assumed that the row length is a multiple of m. To allow a simple mathematical formulation, this paper is based on a segment decomposition of the image. But, generally speaking, many other subsets of pixels can be imagined (3 × 3 pixel neighborhood for example). In this case, the main difficulty is to have a good linear approximation of the mean image level over these subsets of pixels. This difficulty is underlined with the choice of the matrix $\mathbf{H}$ in (8). The problem of choosing the best linear approximation (and the corresponding pixel neighborhood) is beyond the scope of this paper.

Even if the variance is constant per segment, there are still too many unknown variables, $n + K_n$ in total, due to the fact that the mean levels ℓ_i are still unknown. Let $\boldsymbol{x}_k = (x_{k,1}, x_{k,2},\ldots,x_{k,m})^\top$ be the kth segment. The mean level $\boldsymbol{\ell}_k$ of $\boldsymbol{x}_k$ is approximated by a linear model with a smaller dimension than m, which is based on redundancies which exist between neighboring pixels. For example, suppose that all the pixels in $\boldsymbol{x}_k$ have the same mean intensity, say $\ell_{k,j} = \mu$ for all j, then the mean level $\boldsymbol{\ell}_k$ of $\boldsymbol{x}_k$ satisfies

$$\boldsymbol{\ell}_k \overset{\text{def}}{=} \begin{pmatrix} \ell_{k,1} \\ \vdots \\ \ell_{k,m} \end{pmatrix} = \mu \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}.$$

More generally, this yields to the parametric model

$$\boldsymbol{\ell}_k = \mathbf{H}\boldsymbol{\mu}_k \tag{7}$$

where the $m \times q$ matrix $\mathbf{H}$ has the form

$$\mathbf{H} \overset{\text{def}}{=} \begin{pmatrix} 1 & \frac{1}{m} & \cdots & \left(\frac{1}{m}\right)^{q-1} \\ 1 & \frac{2}{m} & \cdots & \left(\frac{2}{m}\right)^{q-1} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \frac{m-1}{m} & \cdots & \left(\frac{m-1}{m}\right)^{q-1} \\ 1 & 1 & \cdots & 1 \end{pmatrix} \tag{8}$$

and $\boldsymbol{\mu}_k \in \mathbb{R}^q$ is an unknown parameter vector. It is assumed that $q < m$ and $\mathbf{H}$ has full column rank, i.e., $\operatorname{rank}(\mathbf{H}) = q$. This means that the mean level of the segment is assumed to be sufficiently smooth (following some arguments given in [35]) to be represented by a one-dimensional polynomial function of order $q-1$ (see details in [36]). The choice of $\mathbf{H}$ is a fundamental dilemma for any parametric approach (see Remark 1). The polynomial model can be replaced by other kinds of approximation (see [34], [36] for example). The following results can be easily extended to the more general case where the matrix $\mathbf{H}$ depends on the segment, i.e., $\ell_k = \mathbf{H}_k\boldsymbol{\mu}_k$. The simplified natural image model for the kth subset of pixels is finally given by

$$\boldsymbol{x}_k = \mathbf{H}\,\boldsymbol{\mu}_k + \boldsymbol{\xi}_k \tag{9}$$

where $\boldsymbol{\xi}_k \sim \mathcal{N}(0, \sigma_k^2\,\mathbf{I}_m)$ for all $k = 1,\ldots,K_n$ and $\mathbf{I}_m$ is the identity matrix of order m (see Remark 2). Let $\boldsymbol{\omega}_k = (\boldsymbol{\mu}_k, \sigma_k)$ be the parameter vector characterizing $\boldsymbol{x}_k$. The set of all possible parameters $\boldsymbol{\omega} = (\boldsymbol{\omega}_1,\ldots,\boldsymbol{\omega}_{K_n})$ for a natural image with K_n blocks of pixels, see model (9), is denoted $\Omega_n = \prod_{i=1}^{K_n}\Omega_{n,i}$ where $\Omega_{n,i} \subset (\mathbb{R}^q \times \mathbb{R}_+^*)$. Since the mean value and the variance of real images are always finite, it is assumed that

Assumption A1: The sets $\Omega_{n,1},\ldots,\Omega_{n,K_n}$ are all simultaneously bounded by a common constant.

This assumption is quite natural in practice. It is crucial to ensure that the asymptotic distribution of the adaptive AUMP test can be determined without undue difficulty.

Remark 1: The chosen parametric model may not fit real natural images perfectly. In practice, this mismatch yields to an augmentation of the pixel variance. But, since the variance is considered as an unknown nuisance parameter, the impact of this augmentation is not significant as long as the approximation errors are not too severe.

Remark 2: Strictly speaking, the acquisition step is followed by an image processing pipeline (e.g., de-mosaicing, gamma correction, etc.) which modifies the statistical distribution of the raw pixels [37]. This paper only considers natural images for which this postprocessing is not highly nonlinear. Hence, it is reasonable to assume that the linear model (9) is sufficient to model locally a vast number of natural images.

C. Cover Pixels Subset Model

The subsets of cover image pixels are obtained by quantizing the subsets of raw pixels. It is assumed that all the quantization parameters, namely the number of quantization levels N_n and the quantization step Δ_n, depend on the number n of pixels. In fact, forcing a LSB to change its value is equivalent to changing the corresponding raw pixel value by adding, or subtracting, the quantity Δ_n. The proposed tests are based on an approximation of the discrete probability distribution of the cover pixels having errors up to Δ_n^2. Hence, when inspecting a large number of pixels, it is necessary to have a small quantization step to be sure that the approximation errors of the true discrete probability distribution are negligible with respect to the impact of hidden bits insertion. Some details on this approximation can be found in the proof of Theorem 1. Without any loss of generality, it is assumed that $N_n = 2^p$ (each grayscale level is coded with p bits).

A N_n-level symmetric uniform scalar quantizer [38], [39] is defined as follows (see Remark 3). Let $Q_n(x)$ be the quantization index of x given by

$$Q_n(x) = \begin{cases} 0, & \text{if } x < -(N_n-2)\frac{\Delta_n}{2}, \\ N_n - 1, & \text{if } x \geq (N_n-2)\frac{\Delta_n}{2} \\ \left\lfloor \frac{x + N_n \frac{\Delta_n}{2}}{\Delta_n} \right\rfloor & \text{otherwise .} \end{cases} \tag{10}$$

where $\lfloor x \rfloor$ denotes the integer smaller than or equal to x. In other words, the quantization rule is $Q_n(x) = i$ when $x \in [t_i, t_{i+1})$ where $t_0 = -\infty$, $t_{N_n} = +\infty$ and $t_i = -N_n\frac{\Delta_n}{2} + i\Delta_n$. The quantization value $\tilde{x}$ of x is then given by

$$\tilde{x} \overset{\text{def.}}{=} -(N_n - 1)\frac{\Delta_n}{2} + \Delta_n\, Q_n(x). \tag{11}$$

To sum up the notations, for a real value x, the quantization value $\tilde{x}$ is the real approximation of x and the integer $Q_n(x)$ is the quantization index, i.e., the grayscale level, which is recorded in the image pixel in order to save computer memory and file storage. In addition, it is assumed that

Assumption A2: When the quantization step Δ_n tends to 0, N_n grows to infinity such that

$$\lim_{\Delta_n \longrightarrow 0} \tilde{x} = x \; \forall x \in \mathbb{R}. \tag{12}$$

This assumption is required to avoid the saturation of the quantizer. For example, (12) is satisfied when N_n is the integer part of Δ_n^{-2}.

Let $c_i = Q_n(x_i)$ be the quantization index of the raw pixel x_i. To simplify the notations, $\tilde{c}_i \overset{\text{def.}}{=} -(N_n-1)\frac{\Delta_n}{2} + \Delta_n\, c_i$ is an other notation for $\tilde{x}_i$, see (11). It follows that

$$p_{\boldsymbol{\theta}_i}[j] = \Pr_{\boldsymbol{\theta}_i}(c_i = j) = \int_{t_j}^{t_{j+1}} f_{\boldsymbol{\theta}_i}(x)dx \tag{13}$$

where $\Pr_{\boldsymbol{\theta}_i}(c_i = j)$ denotes the probability of $\{c_i = j\}$ when x_i has the pdf $f_{\boldsymbol{\theta}_i}(\cdot)$ and $j \in \{0, \ldots, N_n - 1\}$. Let $\mathbf{c}_k$ be the quantized index segment obtained by quantizing each component of $\boldsymbol{x}_k$, i.e., $c_{k,j} = Q_n(x_{k,j})$ or, equivalently, $\mathbf{c}_k = Q_n(\boldsymbol{x}_k)$. The cover image $\mathbf{c}$ is given by $\mathbf{c} = (\mathbf{c}_1, \ldots, \mathbf{c}_{K_n})$. The flowchart describing the statistical model from the number of collected photons until the cover image pixels is summed up in Fig. 1. The joint distribution of $\mathbf{c}_k$ is denoted by $P_{\boldsymbol{\omega}_k}$; this is the product of distributions (see notations in [40])

$$P_{\boldsymbol{\omega}_k} \overset{\text{def.}}{=} P_{(\boldsymbol{\mu}_k, \sigma_k)} = P_{\boldsymbol{\theta}_{k,1}} \times \cdots \times P_{\boldsymbol{\theta}_{k,m}}. \tag{14}$$

Analogously, the joint distribution of $\mathbf{c}_k$ after hidden bits insertion is denoted

$$Q^R_{\boldsymbol{\omega}_k} \overset{\text{def.}}{=} Q^R_{(\boldsymbol{\mu}_k, \sigma_k)} = Q^R_{\boldsymbol{\theta}_{k,1}} \times \cdots \times Q^R_{\boldsymbol{\theta}_{k,m}}. \tag{15}$$

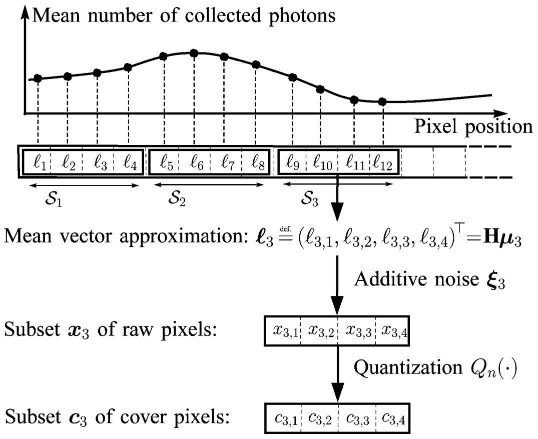
Mean number of collected photons
Pixel position
ℓ_1 ℓ_2 ℓ_3 ℓ_4 ℓ_5 ℓ_6 ℓ_7 ℓ_8 ℓ_9 ℓ_{10} ℓ_{11} ℓ_{12}
$\mathcal{S}_1$
$\mathcal{S}_2$
$\mathcal{S}_3$
Mean vector approximation: $\boldsymbol{\ell}_3 \overset{\text{def.}}{=} (\ell_{3,1}, \ell_{3,2}, \ell_{3,3}, \ell_{3,4})^\top = \mathbf{H}\boldsymbol{\mu}_3$
Additive noise $\boldsymbol{\xi}_3$
Subset $\boldsymbol{x}_3$ of raw pixels:
$x_{3,1}$ $x_{3,2}$ $x_{3,3}$ $x_{3,4}$
Quantization $Q_n(\cdot)$
Subset $\boldsymbol{c}_3$ of cover pixels:
$c_{3,1}$ $c_{3,2}$ $c_{3,3}$ $c_{3,4}$

Fig. 1. Description of the statistical model from the number of collected photons until the cover image pixels. The size of each subset of pixels is $m{=}4$.

Remark 3: Strictly speaking, the mean pixel value ℓ_i is necessarily positive but this constraint is not considered in the paper. It is assumed that the value of ℓ_i, compared to ϵ_i, is large enough to ensure that the positivity constraint is always satisfied when the mean pixel value is estimated. Similarly, it would be possible to use a quantizer adapted to this positivity constraint. But, as long as the assumption A2 is satisfied, the proposed results, based on a symmetric quantizer, can be immediately extended to other kinds of quantization.

IV. AUMP Criterion and Upper-Bound on the Detection Probability

After a brief recall of statistical hypotheses testing theory, this section introduces the AUMP criterion of optimality. Next, a nonadaptive AUMP test is designed under the assumption that the cover image parameters are known. This test provides an asymptotic upper-bound on the detection probability of hidden bits based on the LSB replacement mechanism.

A. AUMP Criterion of Optimality

Let $\boldsymbol{y}$ be the inspected image obtained from a cover image $\mathbf{c}$ modeled in Section III; $\boldsymbol{y}$ is either a cover image or a stego-one (see details in Section II). The goal is to find a test $\varphi\{0, \ldots, N_n - 1\}^n \mapsto \{\underline{\mathcal{H}_0}; \underline{\mathcal{H}_1}\}$ such that hypothesis $\underline{\mathcal{H}_i}$ is accepted if $\varphi(\boldsymbol{y}) = \underline{\mathcal{H}_i}$. Some details on statistical hypotheses testing theory are given in [25] and [26]. Let

$$\mathcal{K}_\alpha = \{\varphi : \sup_{\boldsymbol{\omega} \in \Omega_n} \Pr_{\boldsymbol{\omega}}(\varphi(\boldsymbol{y}) = \underline{\mathcal{H}_1}) \leq \alpha\}$$

be the class of tests with an upper-bounded false alarm probability α, where $\Pr_{\boldsymbol{\omega}}(\cdot)$ stands for $\boldsymbol{y}$ being generated by the joint distribution $P_{\boldsymbol{\omega}_1} \times \cdots \times P_{\boldsymbol{\omega}_{K_n}}$.

The power function $\beta_\varphi(\boldsymbol{\omega}, R)$ is defined by the probability of hidden bits detection

$$\beta_\varphi(\boldsymbol{\omega}, R) = \Pr_{\boldsymbol{\omega}, R}(\varphi(\boldsymbol{y}) = \underline{\mathcal{H}_1})$$

where the probability $\Pr_{\boldsymbol{\omega},R}(\cdot)$ stands for $\boldsymbol{y}$ being generated by the joint distribution $Q^R_{\boldsymbol{\omega}_1} \times \cdots \times Q^R_{\boldsymbol{\omega}_{K_n}}$.

The hypotheses testing problem (4) presents two main difficulties : i) the two hypotheses $\underline{\mathcal{H}_0}$ and $\underline{\mathcal{H}_1}$ are composite and

ii) there is an unknown nuisance parameter $\boldsymbol{\omega}$. Here $\boldsymbol{\omega}$ is considered as a nuisance parameter because it is unknown and it does not contain any information about the presence of hidden bits. There is no general way to design a test between two composite hypotheses, especially with nuisance parameters [25], [26]. A possible approach consists in first eliminating the nuisance parameters. For this purpose, it is tempting to use the invariance principle [25]. In other applications [22], [23], [41], [42], when the pixels are assumed to have nonquantized real values, this principle yields to good results. Here, the quantization operation is not negligible for two main reasons: i) the number of levels N_n is rather small and ii) the hidden bits are directly inserted in the quantization indices. Hence, it is necessary to take into account explicitly the fact that the pixel values are quantized. Since the quantization operation is nonlinear, it becomes very difficult to use the invariance principle. An alternative solution is to design an Uniformly Most Powerful (UMP) test which uniformly maximizes the power function with respect to $\boldsymbol{\omega}$ and R, i.e., the test $\varphi^* \in \mathcal{K}_\alpha$ whose power function $\beta_{\varphi^*}(\boldsymbol{\omega}, R)$ satisfies

$$\beta_{\varphi^*}(\boldsymbol{\omega}, R) = \sup_{\varphi \in \mathcal{K}_\alpha} \beta_\varphi(\boldsymbol{\omega}, R), \ \forall \boldsymbol{\omega} \in \Omega_n, \ \forall R \in \mathcal{R}. \qquad (16)$$

Unfortunately, this test rarely exists in practice [25], [26], especially in the presence of a nonlinear operation like the quantization. For this reason, the remedy consists in designing an asymptotically UMP test based on the assumption that the quantization step vanishes as the number of pixels tends to infinity. The definition of the AUMP test [26] is recalled hereafter.

Definition 1: Let $0 < \alpha < 1$. The test $\varphi^*(\boldsymbol{y})$ is AUMP in the class $\mathcal{D}_\alpha$, given by

$$\mathcal{D}_\alpha = \{\varphi : \limsup_{n \longrightarrow +\infty} \sup_{\boldsymbol{\omega} \in \Omega_n} \Pr_{\boldsymbol{\omega}}(\varphi(\boldsymbol{y}) = \underline{\mathcal{H}}_1) \leq \alpha\},$$

to decide between $\underline{\mathcal{H}}_0$ and $\underline{\mathcal{H}}_1$ if the two following requirements are satisfied:

i) $\varphi^* \in \mathcal{D}_\alpha$;

ii) $\limsup_{n \longrightarrow +\infty} (\beta_\varphi(\boldsymbol{\omega}, R) - \beta_{\varphi^*}(\boldsymbol{\omega}, R)) \leq 0$ for any $\boldsymbol{\omega} \in \Omega_n$ and $R \in \mathcal{R}$, for all other test $\varphi \in \mathcal{D}_\alpha$.

The AUMP test coincides asymptotically with an UMP test as $n \longrightarrow +\infty$. The class $\mathcal{D}_\alpha$ is asymptotically equivalent to $\mathcal{K}_\alpha$. This asymptotic approach is reasonable since there is generally a large number of inspected pixels and the quantization step is often relatively small compared to their natural variability.

B. Upper-Bound on the Detection Probability

In this subsection, it is assumed that $\boldsymbol{\omega}$ is known, which involves hypotheses $\underline{\mathcal{H}}_0$ and $\underline{\mathcal{H}}_1$ being equivalent to hypotheses $\mathcal{H}_0$ and $\mathcal{H}_1$. Since $\boldsymbol{\omega}$ is known, all the notations given in Definition 1 must be understood without the least upper bound over Ω_n. Let $\overline{\sigma}_n^2$ be the mean variance of the image defined by

$$\frac{1}{\overline{\sigma}_n^2} = \frac{1}{n} \sum_{i=1}^{n} \frac{1}{\epsilon_i^2} = \frac{1}{K_n} \sum_{k=1}^{K_n} \frac{1}{\sigma_k^2}. \qquad (17)$$

Let $\varphi^*(\boldsymbol{y})$ be the test defined by

$$\varphi^*(\boldsymbol{y}) = \begin{cases} \mathcal{H}_0 & \text{if } \Lambda^*(\boldsymbol{y}) \leq \lambda^* \\ \mathcal{H}_1 & \text{else .} \end{cases} \qquad (18)$$

where

$$\Lambda^*(\boldsymbol{y}) = \sum_{i=1}^{n} w_i \left(\tilde{y}_i - \ell_i\right) \left(y_i - \bar{y}_i\right) \text{ with } w_i = \frac{\overline{\sigma}_n}{\epsilon_i^2 \sqrt{n}}. \qquad (19)$$

The nonadaptive decision function $\Lambda^*(\boldsymbol{y})$ is derived from the calculation of the likelihood ratio test (see proof of Theorem 1). It is based on residuals $r_i = (\tilde{y}_i - \ell_i)(y_i - \bar{y}_i)$ which indicate the difference between the quantized value $\tilde{y}_i$ and its mean value ℓ_i. The sign of this difference is adjusted by $(y_i - \bar{y}_i)$, which takes value 1 and -1, to take into account the asymmetry in LSB replacement (even pixels could only be incremented, and odd pixels decremented, by overwriting the LSB). The scalar w_i is a weight so that the influence of pixels depends on their noise level. Noisy areas are given less weight than those in flatter areas. The following theorem shows that the test $\varphi^*(\boldsymbol{y})$ is AUMP [26] as $n \longrightarrow +\infty$. To simplify the theoretical results, it is assumed that

Assumption A3: The quantization step Δ_n is chosen such that

$$\varrho_n = \frac{\sqrt{n}\Delta_n}{2\overline{\sigma}_n} \underset{n \to +\infty}{\longrightarrow} \varrho, \ 0 < \varrho < +\infty. \qquad (20)$$

This assumption is useful to avoid some theoretical difficulties in the asymptotic study of the power function which yield to noninteresting degenerate cases, i.e., the power function tends to 0 or 1. It involves that $\Delta_n \longrightarrow 0$ as $n \longrightarrow +\infty$. For example, $\Delta_n = \frac{1}{\sqrt{n}}$ and $N_n = \lfloor n \rfloor$ satisfy both assumptions A2 and A3.

Theorem 1: Assume A1, A2, and A3. Let $\lambda^* = \Phi^{-1}(1 - \alpha)$ where $0 < \alpha < 1$. Then, as $n \longrightarrow +\infty$, the test $\varphi^*(\boldsymbol{y})$ is AUMP in the class $\mathcal{D}_\alpha$ to decide between $\mathcal{H}_0$ and $\mathcal{H}_1$. The false alarm probability satisfies $\lim_{n \longrightarrow +\infty} \Pr_{\boldsymbol{\omega}}(\Lambda^*(\boldsymbol{y}) > \lambda^*) = \alpha$. The power function $R \mapsto \beta_{\varphi^*}(\boldsymbol{\omega}, R)$ is asymptotically given by

$$\lim_{n \longrightarrow +\infty} \beta_{\varphi^*}(\boldsymbol{\omega}, R) = 1 - \Phi\left(\lambda^* - R\varrho\right) \overset{\text{def.}}{=} \beta_\infty(\varrho, R). \qquad (21)$$

Proof: The proof is given in Appendix A. ■

This theorem yields to some important observations. First, the structure of the test clearly depends on the mean level of the cover image and also on its variance. This test is quite similar to the WS detector initially proposed by [16] and revisited by [17]. The WS detector is known to have good performances. Contrary to the approach followed by [16], [17], this paper derives this test from the statistical theory of hypotheses testing. Theorem 1 theoretically establishes both the structure of the test and the form of the weights when the cover image parameters are known.

Next, the power function (21) only depends on the hiding rate and the "mean variance" $\overline{\sigma}_n^2$(17), not on the mean level of the image. This power function $\beta_\infty(\varrho, R)$ can serve as an upper-bound for the probability of detection of any detector dedicated to the problem of hidden bits detection based on LSB replacement. Hence, $R\,\varrho$, which can be viewed as an hiding-to-noise ratio, is a good indicator of the test performances: the smaller this ratio is, the more undetectable the hidden bits are. This is also directly related to the square-root law of [24].

Finally, it must be noted that the power of the test tends to α if $R\varrho_n$ tends to 0. In fact, if the quantization step is very small compared to the cover image variance, then a change in the LSB is not significant compared to the noise level. The secret message becomes less detectable. This observation is also true for other detectors. For example, the chi-square attack [18] is based on the histogram of the image. When the quantization step is small compared to the cover image variance, the support of the histogram is very large and the difference between pairs of values, i.e., the values of couples $(2k, 2k+1)$ with $k \in \{0, \dots, 2^{p-1}-1\}$, is very small. Hence, it becomes more difficult for the detector to take its decision based on the differences between pairs of values.

V. Adaptive AUMP Test

This section considers a cover image whose parameter vector $\boldsymbol{\omega}$ is unknown. In this case, the true parameter $\boldsymbol{\omega}$ is replaced in Theorem 1 by its estimate $\hat{\boldsymbol{\omega}}$, i.e., the adaptive version of the test described in Theorem 1 is based on the estimates $\hat{\ell}_i$ and $\hat{w}_i$ instead of ℓ_i and w_i.

A. Estimation of Cover Image Parameters

Suppose that the quantization has negligible effects on the estimation of the image parameters ℓ_k and σ_k^2. Then, these parameters can be estimated by using their well-known maximum likelihood estimates for nonquantized observations (see details in [43]). This yields to

$$\hat{\boldsymbol{\ell}}_k = \mathbf{H}\left(\mathbf{H}^\top\mathbf{H}\right)^{-1}\mathbf{H}^\top\tilde{\boldsymbol{y}}_k \text{ and } \hat{\sigma}_k^2 = \frac{1}{m-q}\left\|\mathbf{P}^\perp\,\tilde{\boldsymbol{y}}_k\right\|^2. \quad (22)$$

Here, $\tilde{\boldsymbol{y}}_k$ denotes the vector obtained by calculating the quantization value of each component of $\boldsymbol{y}_k$, $\|\boldsymbol{y}\|$ is the Euclidean norm of $\boldsymbol{y}$, $\mathbf{P}^\perp = \mathbf{I}_m - \mathbf{H}(\mathbf{H}^\top\mathbf{H})^{-1}\mathbf{H}^\top$ and $\mathbf{A}^{-1}$ is the inverse of the square matrix $\mathbf{A}$. The estimate of the mean variance is given by

$$\frac{1}{\hat{\hat{\sigma}}_n^2} = \frac{1}{K_n}\sum_{k=1}^{K_n}\frac{1}{\hat{\sigma}_k^2}. \quad (23)$$

Then it follows from (22) that the estimates $\hat{\ell}_i$ and $\hat{w}_i$ of pixel y_i are given by

$$\hat{\ell}_i = \hat{\ell}_{k,j} \text{ and } \hat{w}_i = \frac{\hat{\hat{\sigma}}_n}{\hat{\sigma}_k^2\sqrt{K_n(m-q)}} \quad (24)$$

where it is supposed that y_i is the jth pixel of subset $\mathcal{S}_k$. The difference between the denominators of $\hat{w}_i$ and w_i, $K_n(m-q)$ instead of n, is required to ensure that the adaptive decision function, presented in (26), converges in distribution toward the standard Gaussian distribution under $\mathcal{H}_0$. A flowchart summing up the steps for the calculation of the adaptive test parameters $\hat{r}_i = (\tilde{y}_i - \hat{\ell}_i)(y_i - \bar{y}_i)$ and $\hat{w}_i$, used in the decision function (26), is given in Fig. 2. The adaptive version $\hat{r}_i$ of residuals r_i is obtained by replacing ℓ_i by its estimate $\hat{\ell}_i$ (see Remark 4).

Remark 4: The proposed adaptive AUMP test, see (25) and (26), seems to coincide with the well-known Generalized Likelihood Ratio Test (GLRT) since the unknown cover parameters are replaced by estimates. Strictly speaking, to prove that the two tests are equivalent, it is necessary to derive the GLRT from (4). This derivation is difficult because the pixels are quantized random variables. Hence, the proposed approach is a shortcut to avoid complicated calculations. Theorem 2 shows that using this shortcut does not involve any loss of optimality (at least in the asymptotic sense).

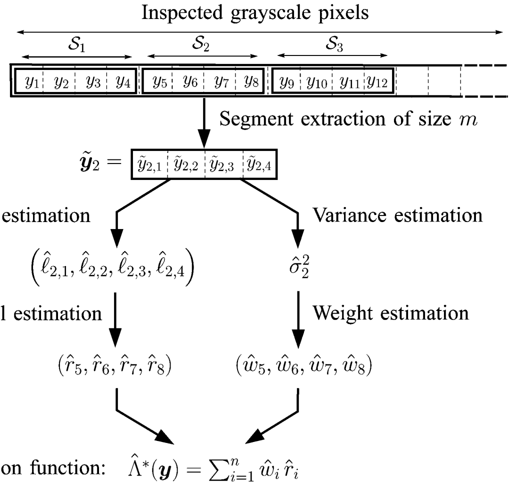
Inspected grayscale pixels
$\mathcal{S}_1$
$\mathcal{S}_2$
$\mathcal{S}_3$
y_1 y_2 y_3 y_4 y_5 y_6 y_7 y_8 y_9 y_{10} y_{11} y_{12}
Segment extraction of size m
$\tilde{\boldsymbol{y}}_2 =$ $\tilde{y}_{2,1}$ $\tilde{y}_{2,2}$ $\tilde{y}_{2,3}$ $\tilde{y}_{2,4}$
Mean estimation
Variance estimation
$\left(\hat{\ell}_{2,1}, \hat{\ell}_{2,2}, \hat{\ell}_{2,3}, \hat{\ell}_{2,4}\right)$
$\hat{\sigma}_2^2$
Residual estimation
Weight estimation
$(\hat{r}_5, \hat{r}_6, \hat{r}_7, \hat{r}_8)$
$(\hat{w}_5, \hat{w}_6, \hat{w}_7, \hat{w}_8)$
Decision function: $\hat{\Lambda}^*(\boldsymbol{y}) = \sum_{i=1}^n \hat{w}_i \hat{r}_i$

Fig. 2. Calculation of test adaptive test parameters $\hat{r}_i$ and $\hat{w}_i$ for a subset of pixels with m=4.

B. Asymptotically Optimal Adaptive Test

Let $\hat{\varphi}^*(\boldsymbol{y})$ be the adaptive test defined by

$$\hat{\varphi}^*(\boldsymbol{y}) = \begin{cases} \mathcal{H}_0 & \text{if } \hat{\Lambda}^*(\boldsymbol{y}) \le \hat{\lambda}^* \\ \mathcal{H}_1 & \text{else .} \end{cases} \quad (25)$$

where

$$\hat{\Lambda}^*(\boldsymbol{y}) = \sum_{i=1}^n \hat{w}_i \hat{r}_i = \sum_{i=1}^n \hat{w}_i\left(\tilde{y}_i - \hat{\ell}_i\right)(y_i - \bar{y}_i). \quad (26)$$

The following theorem shows that this adaptive test is AUMP in the class $\mathcal{D}_\alpha$ provided that $\hat{\lambda}^*$ is conveniently chosen.

Theorem 2: Assume A1, A2, A3, $m = o(n)$ and $q = o(m)$. Then, as $n \longrightarrow +\infty$, the test $\hat{\varphi}^*(\boldsymbol{y})$ to decide between $\mathcal{H}_0$ and $\mathcal{H}_1$ is such that $\lim_{n\longrightarrow+\infty}\sup_{\boldsymbol{\omega}\in\Omega_n}\Pr_{\boldsymbol{\omega}}(\hat{\Lambda}^*(\boldsymbol{y}) > \hat{\lambda}^*) = \alpha$ provided that $\hat{\lambda}^* = \Phi^{-1}(1-\alpha)$. Moreover, the test $\hat{\varphi}^*(\boldsymbol{y})$ is AUMP in the class $\mathcal{D}_\alpha$ to decide between $\mathcal{H}_0$ and $\mathcal{H}_1$. Its power function satisfies

$$\lim_{n\longrightarrow+\infty}\beta_{\hat{\varphi}^*}(\boldsymbol{\omega}, R) = 1 - \Phi\left(\hat{\lambda}^* - R\varrho\right) = \beta_\infty(\varrho, R) \quad (27)$$

for all $\boldsymbol{\omega} \in \Omega_n$ and $R \in \mathcal{R}$.

Proof: The proof is given in Appendix B. ■

The assumptions about the parameters Δ_n, m and q are very important. They ensure that the impact of the nuisance parameters and the nonlinearity of the quantization operation on the test performances is asymptotically negligible as $n \longrightarrow +\infty$. It is necessary to have a small number q of nuisance parameters per subset of pixels. Finally, compared with the decision function of the WS detector described in [16], [17], Theorem 2 gives the estimates $\hat{\ell}_i$ and the weights $\hat{w}_i$ which ensure that the test has both the CFAR property and the maximum detection probability. Theorem 2 is undoubtedly a theoretical justification of the performances of the WS detector (see Remark 5).

Results given in Theorem 2 are based on the convergence in distribution of $\hat{\Lambda}^*(\boldsymbol{y})$ to the Gaussian distribution as $n \longrightarrow +\infty$. In practice, the value of Δ_n is not sufficiently small and the size of m is not sufficiently large to ensure that this convergence is completely achieved, especially under hypothesis $\underline{\mathcal{H}}_1$. In fact, under $\underline{\mathcal{H}}_1$, the quantization step Δ_n and the difference $m - q$ are directly involved in the mean of the asymptotic pdf of $\hat{\Lambda}^*(\boldsymbol{y})$. Hence, these parameters may have some impact of the detection performances of the test. The following corollary presents a useful approximation of the mean of the decision function $\hat{\Lambda}^*(\boldsymbol{y})$ under $\underline{\mathcal{H}}_1$. Strictly speaking, the variance of $\hat{\Lambda}^*(\boldsymbol{y})$ should be also corrected but, in practice, this correction is negligible with respect to the correction of the expectation.

Corollary 1: Assume A1, A2, A3, $m = o(n)$ and $q = o(m)$. Under hypothesis $\underline{\mathcal{H}}_1$, the decision function $\hat{\Lambda}^*(\boldsymbol{y})$ satisfies

$$\mathbb{E}_{\boldsymbol{\omega},R}[\hat{\Lambda}^*(\boldsymbol{y})] \sim R\varrho\sqrt{\frac{m-q-2}{m}} \overset{\text{def.}}{=} R\,\tilde{\varrho} \qquad (28)$$

where $\mathbb{E}_{\boldsymbol{\omega},R}[\cdot]$ denotes the expectation when $\boldsymbol{y}_k \sim Q^R_{\boldsymbol{\omega}_k}$ for all $k{=}1,\ldots,K_n$.

Proof: From (41), (57), and (78), it follows that

$$\mathbb{E}_{\boldsymbol{\omega},R}[\hat{\Lambda}^*(\boldsymbol{y})] \sim \frac{R\,\Delta_n\sqrt{K_n\,(m-q)}}{2\overline{\sigma}_n}\sqrt{\frac{m-q-2}{m-q}}$$

which yields to (28) and ends the proof. ■

Due to this corollary, the optimal asymptotic power function $\beta_\infty(\varrho, R)$ given in (27) can be approximated by the corrected power function

$$\beta_\infty(\tilde{\varrho}, R) = 1 - \Phi\left(\Phi^{-1}(1-\alpha) - R\tilde{\varrho}\right). \qquad (29)$$

From (28), it is obvious that $\tilde{\varrho} < \varrho$. Hence, when $m - q$ is not sufficiently large to ensure that $\tilde{\varrho} \approx \varrho$, there is a small loss of optimality. In practice, the size of m must not be too large; the local approximation of a nonstationary cover image is generally only acceptable for a small m. This loss of optimality reflects the difficulty to approximate a cover image with a parsimonious linear model, i.e., with a regression model characterized by a small number q of parameters.

Remark 5: The algorithm WS [16] has been introduced as an estimate $\hat{R}$ of R; the detection step consists of comparing $\hat{R}$ to a threshold. In this paper, the decision function $\hat{\Lambda}^*(\boldsymbol{y})$ can be viewed as an estimate of R since its expected value is 0 when $R = 0$ and $R\,\tilde{\varrho}$ when $R > 0$. However, in practice, the parameter $\tilde{\varrho}$ is unknown since its depend on $\overline{\sigma}_n$. Hence the estimate $\hat{\Lambda}^*(\boldsymbol{y})$ has necessarily a bias when $R > 0$. For the detection purpose, this bias has no matter since the test is almost optimal. For the estimation purpose (which is clearly out of the scope of this paper), this bias must be corrected. Hence, for the WS algorithm, a bias correction is required [17] and a special attention must be devoted to the mean level estimate (the estimate must be independent on the pixel of interest to avoid a bias augmentation). These two requirements are not necessary for the proposed test.

VI. Numerical Experiments

This section shows the relevance of the model (9), the performances of the test $\hat{\varphi}^*(\boldsymbol{y})$ given in Theorem 2 and the quality of the asymptotic approximation (29). First, the theoretical results are illustrated by using simulated data. Next, the adaptive AUMP test is applied to real images and it is compared with several other detection algorithms, namely the Generalized Category Attack (GCA), the Sample Pairs Analysis-Least Square Method (SPA-LSM) method and the WS detector.

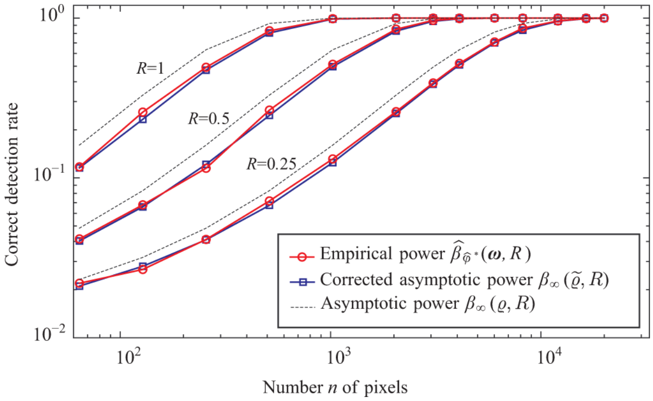

Fig. 3. Power curves in logarithmic scale for 3 hiding rates $R = 0.25, R = 0.5$ and $R = 1$: empirical curve (full line with circles), corrected asymptotic one (full line with squares) and asymptotic one (dotted line).

A. Simulated Data

This subsection deals with an artificial image which follows the simplified natural image model (9) with $q = 4$, $\boldsymbol{\mu}_k{=}(10;-10;40;-30)^\top$ and $\sigma_k{=}\sigma{=}1.5$ for all $1 \leq k \leq K_n$. The cover segments $\mathbf{c}_k$ are quantized with $N_n = 256$ levels. The matrix $\mathbf{H}$ is given by (8).

To evaluate the quality of the asymptotic approximation, Fig. 3 shows the power function associated to $\hat{\Lambda}^*(\boldsymbol{y})$ as a function of the number n of pixels for $\alpha = 0.01$. The quantization step is $\Delta_n = 0.5$, $m = 32$ and the hiding rate is $R \in \{0.25; 0.5; 1\}$. The integer K_n increases as the number n of pixels increases. The number of samples used to estimate each point of the empirical curve is sufficiently high to ensure that the 95%-confidence interval (which is not plotted to ensure legibility of the figure) almost coincides with the estimated curve. The empirical power function $\hat{\beta}^*_{\hat{\varphi}}(\boldsymbol{\omega}, R)$ is closely approximated by the corrected theoretical power function $\beta_\infty(\tilde{\varrho}, R)$ given in (29). Moreover, this figure shows the gap between $\beta_\infty(\tilde{\varrho}, R)$ and $\beta_\infty(\varrho, R)$ given in (27): this loss of optimality is due to the fact that $\sqrt{\frac{(m-q-2)}{m}} \approx 0.9 < 1$, i.e., $\tilde{\varrho} < \varrho$.

Finally, Fig. 4 shows the impact of the couple (m, q) on the asymptotic performance of the AUMP test $\hat{\varphi}^*(\boldsymbol{y})$. The number of inspected pixels is either $n_1{=}2^{10}$ or $n_2{=}2^{16}$. The parameter m is either $m_1{=}32$ or $m_2{=}64$. The quantized step is $\Delta_{n_1}{=}\Delta_{n_2}{=}0.5$ and the pixel variance is $\sigma_k{=}\sigma{=}1.5$ for all k. The hiding rate is $R{=}0.2$ and $\alpha{=}0.01$. The asymptotic power of the test is $\beta_\infty(\varrho_n, R)$ where ϱ_n is given in (20). The corrected asymptotic power is $\beta_\infty(\tilde{\varrho}_{n,m}, R)$ where $\tilde{\varrho}_{n,m} = \varrho_n\sqrt{\frac{(m-q-2)}{m}}$, $n \in \{n_1, n_2\}$, $m \in \{m_1, m_2\}$, and q varies between 0 and $m{-}2$. Clearly, the asymptotic detection probabilities $\beta_\infty(\varrho_{n_1}, R)$ and $\beta_\infty(\varrho_{n_2}, R)$ do not depend on m and q. The corrected asymptotic detection probabilities

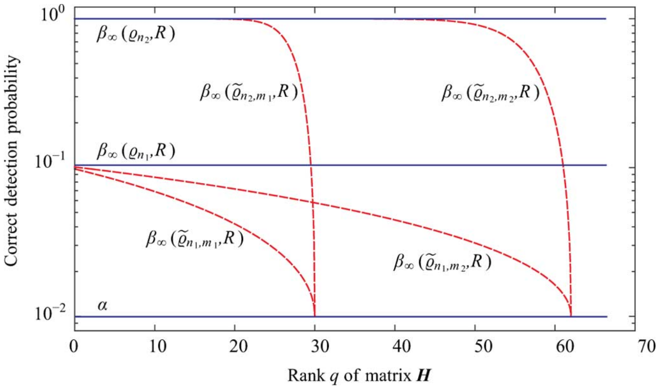

Fig. 4. Power curves in logarithmic scale, for four different values (n_1, m_1), (n_1, m_2), (n_2, m_1), and (n_2, m_2) of the couple (n, m), as a function of q.

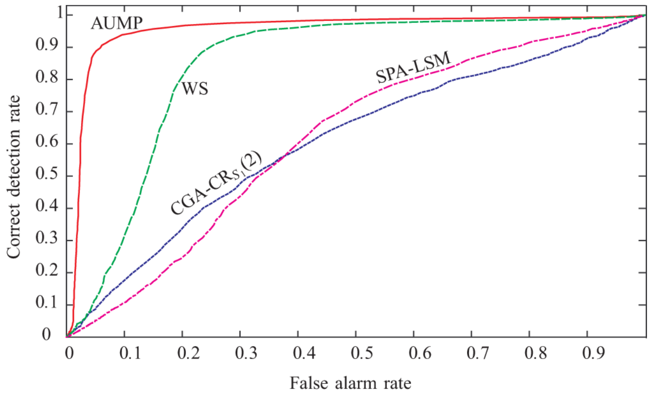

Fig. 5. Comparison between the SPA-LSM, CGA-CR $_{S_1}$(2), WS and AUMP algorithms for the BOSS base.

are some decreasing functions of q. When m is small, i.e., $m = m_1$, the loss of power due to the choice of a large q is greater when n is small. On the contrary, when n is large, i.e., $n = n_2$, it is possible to choose a large value of q without any significant loss of optimality, especially if m is large. In practice, the value of q is mainly limited by the choice of m. As explained in the rest of this section, a large value of m is generally not reasonable for real images.

B. *Comparison With Other Algorithms on the BOSS Base*

The results in this subsection are drawn from the BOSS base of real cover images [44]. This set consists of 9074 grayscale cover images of size 512 × 512 in the portable graymap format with $N_n = 256$ and $\Delta_n = 1$ (the true value of Δ_n is unknown). When secret bits are hidden in images, the hiding rate is $R = 0.05$. This subsection compares the proposed adaptive AUMP test with several other detection methods. First, the GCA method [15] is included in the comparison because it is the generalization of the Chi-Square attack [18]. Several versions of the GCA method, named combined relativities, are proposed in [15]. For the BOSS base, the best performance was obtained for the combined relativities $\mathrm{CR}_{S_1}(2)$. Hence, the proposed AUMP test is compared with the CGA-CR $_{S_1}$(2) method. The structural detector SPA-LSM method [45] is also studied. It is simple and efficient (more powerful than the RS scheme [46]). Finally, the revisited version of the WS detector is used as a natural competitor for the adaptive AUMP test. The parameters proposed in [17] are used to tune the WS detector, i.e., the WS detector is based on a filtering window of size 3 × 3 with moderate weights [17, eqs. 5 and 9].

The parameters of the AUMP test are $q = 6$ and $m = 16$ (hence K_n=16 384). The choice of m is made to get good performances (several values have been tested). When m is large ($m \geq 32$, for example), the polynomial approximation may be inaccurate (even with a high order $q-1$). Hence, it is preferable to use a small value of m ($m \leq 16$ is recommended in practice). In such a situation, the estimation of mean and variance is certainly not very accurate but it is generally sufficient to detect hidden bits. The decision function $\widehat{\Lambda}^*(\boldsymbol{y})$ given in (26) is then computed. To avoid numerical instabilities, each segment with a very small variance, i.e., a segment which satisfies the empirical rule $\hat{\sigma}_k < 1$, is scaled to obtain the minimum variance value 1. This empirical rule can be viewed as a kind of regularization. A pixel with a very small variance estimate may have a serious impact on the decision function. Hence, it is necessary to limit this impact by increasing artificially the estimated variance of this pixel. This astuteness is very similar to the one used for choosing the weighting coefficients in the WS algorithm (see details in [17]): the estimated variance in flat regions must be corrected to stabilize the behavior of the WS algorithm. Fig. 5 shows the detection rate plotted as a function of the false alarm rate for all the analyzed methods. To obtain these curves, the decision function of each method is compared to a threshold which varies continuously. According to Theorem 2, the power function of the AUMP test is independent of the image parameters. For this reason, when the hiding rate R is fixed, the power of the test is just a function of the false alarm probability α and, consequently, the ROC curve for the proposed AUMP test is properly defined, as shown in (27) and (29). From Fig. 5, it is clear that the proposed adaptive AUMP test outperforms all the other tests, whatever the false alarm rate.

VII. Conclusion

This paper proposes an original approach to detect hidden bits in grayscale natural images. The proposed approach is based on a simplified parametric model of natural images and it exploits the image structure. When the parameters of the model are known, Theorem 1 proposes a nonadaptive AUMP test which maximizes the probability of detection, whatever the hiding rate, when the quantization step vanishes as the number of pixels becomes arbitrarily large. Hence, it provides an asymptotic upper-bound for the detection of hidden bits based on the LSB replacement mechanism. In real situations, the image parameters are estimated and Theorem 2 proposes an adaptive AUMP test which maximizes the probability of detection whatever the hiding rate and the true image parameters. Numerical experiments on real images and comparisons with existing detection algorithms confirm the statistical performances of the test.

Appendix A
Proof of Theorem 1

The proof is broken down into four steps. First, the decision function, denoted $\Lambda_{\mathrm{np}}^{(R^\star)}(\boldsymbol{y})$, of the Likelihood Ratio Test (LRT) is calculated when the hiding rate $R^\star$ is known. It is expressed as a function of the decision function $\Lambda^*(\boldsymbol{y})$ of the AUMP test. Second, the statistical distribution of $\Lambda^*(\boldsymbol{y})$ under $\mathcal{H}_0$ is established. Third, the statistical distribution of $\Lambda^*(\boldsymbol{y})$ under $\mathcal{H}_1$ is established when the hiding rate $R^\star$ is known. Finally, based on the results obtained from the previous steps, it is proved that the LRT is statistically equivalent to the AUMP test, which establishes the optimality of the AUMP test.

For a sequence of numbers x_n and y_n, the notation $x_n = O(y_n)$ means that $\frac{x_n}{y_n}$ is bounded as $n \to +\infty$. For random variables X_n and Y_n, the notation $X_n = o_P(Y_n)$ means that $\frac{X_n}{Y_n} \to 0$ in probability, which is also denoted $\frac{X_n}{Y_n} \xrightarrow{p} 0$. The convergence in distribution (or in law) is denoted by $\xrightarrow{d}$. Strictly speaking, in the following proof, some of the notations $O(\cdot)$, $o(\cdot)$ and $o_P(\cdot)$ should depend on the inspected pixel y_i, i.e., these notations should be replaced by $O_i(\cdot)$, $o_i(\cdot)$, and $o_{P,i}(\cdot)$. But, according to assumption A1 and since all the function $O_i(\cdot)$, $o_i(\cdot)$, and $o_{P,i}(\cdot)$ have the same limiting behavior for all i, the index i is omitted to simplify the notations.

A. Asymptotic Likelihood Ratio Test

Suppose that $R^\star \in \mathcal{R}$ is fixed. The optimal test $\varphi_{\text{np}}^{(R^\star)}$ solving the decision problem between the two simple hypotheses

$$\begin{aligned} \mathcal{H}_0 &= \{y_i \sim P_{\boldsymbol{\theta}_i}\ , \forall i = 1, \ldots, n\} \\ \mathcal{H}_1(R^\star) &= \{y_i \sim Q_{\boldsymbol{\theta}_i}^{R^\star}\ , \forall i = 1, \ldots, n\} \end{aligned} \tag{30}$$

is given by the Neyman-Pearson lemma [25]; this is the well-known LRT defined by

$$\varphi_{\text{np}}^{(R^\star)}(\boldsymbol{y}) = \begin{cases} \mathcal{H}_0 & \text{if } \Lambda_{\text{np}}^{(R^\star)}(\boldsymbol{y}) \le \lambda_\alpha \\ \mathcal{H}_1 & \text{else} \end{cases} \tag{31}$$

where

$$\begin{aligned} \Lambda_{\text{np}}^{(R^\star)}(\boldsymbol{y}) &= \sum_{i=1}^{n} \ln \frac{q_{\boldsymbol{\theta}_i}^{R^\star}[y_i]}{p_{\boldsymbol{\theta}_i}[y_i]} \\ &= \sum_{i=1}^{n} \ln \left(\frac{R^\star}{2} \frac{p_{\boldsymbol{\theta}_i}[y_i] + p_{\boldsymbol{\theta}_i}[\bar{y}_i]}{p_{\boldsymbol{\theta}_i}[y_i]} + 1 - R^\star \right) \\ &= \sum_{i=1}^{n} \Lambda_{\boldsymbol{\theta}_i}(y_i; \Delta_n, R^\star). \end{aligned} \tag{32}$$

Here, λ_α is a threshold such that $\Pr_{\boldsymbol{\omega}}(\Lambda_{\text{np}}^{(R^\star)}(\boldsymbol{y}) > \lambda_\alpha) = \alpha$.

A direct calculation shows that

$$p_{\boldsymbol{\theta}_i}[k] = \Delta_n f_{\boldsymbol{\theta}_i}\left(\tilde{k}\right) + o(\Delta_n^2), \tag{33}$$

$$p_{\boldsymbol{\theta}_i}[k] + p_{\boldsymbol{\theta}_i}[\bar{k}\,] = 2\Delta_n f_{\boldsymbol{\theta}_i}\left(\frac{\tilde{k} + \tilde{\bar{k}}}{2}\right) + o(\Delta_n^2) \tag{34}$$

where $o(\Delta_n^2)$ is an infinitely differentiable function with respect to Δ_n. In fact, for $k \in \{1, \ldots, N_n - 2\}$, (33) and (34) are obtained by using (13) and the Taylor series expansion of $f_{\boldsymbol{\theta}_i}(x)$ around $\tilde{k} = t_k + \frac{\Delta_n}{2}$ for (33) and around $\frac{(\tilde{k}+\tilde{\bar{k}})}{2} = \frac{(t_k+t_{\bar{k}})}{2} + \frac{\Delta_n}{2}$ for (34). For $k = 0$ and $k = N_n - 1$, (33) and (34) are obtained by using an asymptotic approximation of the Gaussian distribution tail (provided that (12) is satisfied). It follows from (33) and (34) that

$$\frac{p_{\boldsymbol{\theta}_i}[y_i] + p_{\boldsymbol{\theta}_i}[\bar{y}_i]}{p_{\boldsymbol{\theta}_i}[y_i]} = 2\exp\left(\frac{\Delta_n}{2\epsilon_i^2}\eta_i(\tilde{y}_i - \ell_i)\right) + o_P(\Delta_n^2) \tag{35}$$

where $\eta_i = y_i - \bar{y}_i$. The fact that the sets $\Omega_{n,i}$ are simultaneously bounded is necessary to derive (35), especially the term $o_P(\Delta_n^2)$. From (32) and (35), one obtains

$$\begin{aligned} &\Lambda_{\boldsymbol{\theta}_i}(y_i; \Delta_n, R^\star) \\ &\qquad = \ln\left[1 + R^\star\left(\exp\left(\frac{\Delta_n}{2\,\epsilon_i^2}\eta_i(\tilde{y}_i - \ell_i)\right) - 1\right) + o_P(\Delta_n^2)\right]. \end{aligned}$$

Whichever is the true hypothesis, $\mathcal{H}_0$ or $\mathcal{H}_1(R^\star)$, it is clear that (see (37)–(40) for technical details)

$$\frac{\Delta_n}{2\,\epsilon_i^2}\eta_i(\tilde{y}_i - \ell_i) \xrightarrow{P} 0 \text{ as } \Delta_n \to 0.$$

Hence, the second-order Taylor series expansion of $\ln(1 + x)$ around $x = 0$ yields to

$$\Lambda_{\boldsymbol{\theta}_i}(y_i; \Delta_n, R^\star) = \frac{R^\star \Delta_n}{2\,\epsilon_i{}^2}\eta_i\,(\tilde{y}_i - \ell_i)) + o_P(\Delta_n^2).$$

Equation (31) and (32) show that the test $\varphi_{\text{np}}^{(R^\star)}(\boldsymbol{y})$ is related to the test $\varphi^*(\boldsymbol{y})$ via the equality

$$\Lambda_{\text{np}}^{(R^\star)}(\boldsymbol{y}) = \frac{R^\star \Delta_n \sqrt{n}}{2\,\overline{\sigma}_n}\Lambda^*(\boldsymbol{y}) + o_P(n\,\Delta_n^2) \tag{36}$$

where $\Lambda^*(\boldsymbol{y})$ is given in (26).

B. Asymptotic False Alarm Probability for $\Lambda^*(\boldsymbol{y})$

For brevity, let $\gamma(y_i; \boldsymbol{\theta}_i) = \frac{1}{\epsilon_i^2}\eta_i(\tilde{y}_i - \ell_i)$ such that $\Lambda^*(\boldsymbol{y}) = \frac{\overline{\sigma}_n}{\sqrt{n}}\sum_{i=1}^{n}\gamma(y_i; \boldsymbol{\theta}_i)$. Under hypothesis $\mathcal{H}_0$, $y_i \sim P_{\boldsymbol{\theta}_i}$. Based on (33) and the definitions of the mathematical expectation and the variance, a direct calculation yields to

$$\begin{aligned} \mathbb{E}_{\boldsymbol{\theta}_i}[\gamma(y_i; \boldsymbol{\theta}_i)] &= \Pr(\eta_i = 1)\mathbb{E}_{\boldsymbol{\theta}_i}\left[\frac{1}{\epsilon_i^2}(\tilde{y}_i - \ell_i)\middle|\eta_i = 1\right] \\ &\quad - \Pr(\eta_i = -1)\mathbb{E}_{\boldsymbol{\theta}_i}\left[\frac{1}{\epsilon_i^2}(\tilde{y}_i - \ell_i)\middle|\eta_i = -1\right] = o(\Delta_n^2) \end{aligned} \tag{37}$$

$$\mathbb{V}\text{ar}_{\boldsymbol{\theta}_i}[\gamma(y_i; \boldsymbol{\theta}_i)] = \frac{\epsilon_i^2 + \frac{\Delta_n^2}{12}}{\epsilon_i^4} + o(\Delta_n^2) = \frac{1}{\epsilon_i^2} + O(\Delta_n^2) \tag{38}$$

where $\mathbb{E}_{\boldsymbol{\theta}_i}[\cdot]$, $\mathbb{E}_{\boldsymbol{\theta}_i}[\cdot|\cdot]$ and $\mathbb{V}\text{ar}_{\boldsymbol{\theta}_i}[\cdot]$ denotes, respectively, the expectation, the conditional expectation and the variance when $y_i \sim P_{\boldsymbol{\theta}_i}$.

Hence, from the Lindeberg central limit theorem [25, Theorem 11.2.5] and the definition of $\overline{\sigma}_n$(17), it follows that $\Lambda^*(\boldsymbol{y}) \xrightarrow{d} \mathcal{N}(0, 1)$ as $n \to +\infty$. It must be noted that the Lindeberg condition is easily satisfied for the random variables $\gamma(y_i; \boldsymbol{\theta}_i)$. Hence, the threshold $\lambda^* = \Phi^{-1}(1 - \alpha)$ asymptotically warrants the false alarm probability α.

C. *Asymptotic Correct Detection Probability for* $\Lambda^*(\boldsymbol{y})$

Similarly, under hypothesis $\mathcal{H}_1(R^\star)$, $y_i \sim Q_{\boldsymbol{\theta}_i}^{R^\star}$. Based on (2) and (33), one obtains

$$\mathbb{E}_{\boldsymbol{\theta}_i,R^\star}[\gamma(y_i;\boldsymbol{\theta}_i)] = \frac{R^\star\Delta_n}{2\epsilon_i^2} + o(\Delta_n^2), \tag{39}$$

$$\begin{aligned}\mathbb{V}\mathrm{ar}_{\boldsymbol{\theta}_i,R^\star}[\gamma(y_i;\boldsymbol{\theta}_i)] &= \frac{\epsilon_i^2 + \frac{\Delta_n^2}{12} + R^\star\frac{\Delta_n^2}{2}(1-\frac{R^\star}{2})}{\epsilon_i^4} \\ &+o(\Delta_n^2) = \frac{1}{\epsilon_i^2} + O(\Delta_n^2).\end{aligned} \tag{40}$$

Hence, from the Lindeberg central limit theorem, it follows that $\Lambda^*(\boldsymbol{y}) \xrightarrow{d} \mathcal{N}(R^\star\varrho, 1)$. The asymptotic power of the test is then

$$\lim_{n\longrightarrow+\infty} \beta_{\varphi^*}(\boldsymbol{\omega}, R^\star) = 1 - \Phi\left(\lambda^* - R^\star\varrho\right).$$

D. *Asymptotic AUMP Optimality*

According to (20), it follows that $\Delta_n\sqrt{n}{=}O(1)$. Hence, using (36) and the asymptotic convergence results of the two previous subsections, the Slutsky's Theorem [25, Theorem 11.2.11] shows that the test $\varphi_{\mathrm{np}}^{(R^\star)}(\boldsymbol{y})$ is asymptotically equivalent to the test $\varphi^*(\boldsymbol{y})$.

Neither the decision function $\Lambda^*(\boldsymbol{y})$ nor the threshold λ^* depend on $R^\star$. Hence, the test $\varphi^*(\boldsymbol{y})$ is equivalent to the Neyman-Pearson test $\varphi_{\mathrm{np}}^{(R^\star)}(\boldsymbol{y})$ whatever the value of $R^\star \in \mathcal{R}$, which ends the proof.

APPENDIX B
PROOF OF THEOREM 2

For brevity, let $\eta_{k,j} = y_{k,j} - \bar{y}_{k,j}$, $\hat{\gamma}_{k,j} = \eta_{k,j}(\tilde{y}_{k,j} - \hat{\ell}_{k,j})$, $\hat{S}_k = \sum_{j=1}^m \hat{\gamma}_{k,j}$ and $\hat{\gamma}_k = \frac{1}{\hat{\sigma}_k^2\,\sqrt{m-q}}\hat{S}_k$ such that (26) is rewritten as

$$\hat{\Lambda}^*(\boldsymbol{y}) = \frac{\hat{\bar{\sigma}}_n}{\sqrt{K_n}}\sum_{k=1}^{K_n}\hat{\gamma}_k. \tag{41}$$

Let $\mathbf{P} = \mathbf{H}(\mathbf{H}^\top\mathbf{H})^{-1}\mathbf{H}^\top$ be the projection matrix onto the linear space spanned by the matrix $\mathbf{H}$ whose elements are denoted $p_{i,j}$ for $1 \leq i,j \leq m$.

The main difficulty in the proof is due to the quantization of the $y_{k,j}$'s. This nonlinear operation generates some correlations between $\hat{S}_k$ and $\hat{\sigma}_k^2$, which makes difficult the study of $\hat{\gamma}_k$. Moreover, the asymptotic behavior of $\hat{\bar{\sigma}}_n$ needs a special attention because the quantization also has an impact on it. Hence, the proof is broken down into four steps: 1) the asymptotic study of $\hat{\bar{\sigma}}_n$ under $\underline{\mathcal{H}}_0$ and 2) under $\underline{\mathcal{H}}_1$, 3) the calculation of the probability distribution of $\hat{\Lambda}^*(\boldsymbol{y})$ under $\underline{\mathcal{H}}_0$ and 4) under $\underline{\mathcal{H}}_1$. Based on these four results, the asymptotic probability of detection of $\hat{\varphi}^*(\boldsymbol{y})$ is calculated, which proves its asymptotic optimality. Although the notations $O(\cdot)$, $o(\cdot)$, and $o_P(\cdot)$ may depend on the inspected pixel y_i or the inspected segment $\boldsymbol{y}_k$, this dependence is not mentioned in the proof to simplicity the notations (see the discussion at the beginning of Appendix A).

A. *Asymptotic Study of* $\hat{\bar{\sigma}}_n$ *Under Hypothesis* $\underline{\mathcal{H}}_0$

By definition, $\hat{\sigma}_k^2$ can be rewritten as

$$\hat{\sigma}_k^2 = \frac{\sigma_k^2}{m-q}\,U_{n,k} \text{ with } U_{n,k} = \frac{\left\|\mathbf{P}^\perp\,\tilde{\boldsymbol{y}}_k\right\|^2}{\sigma_k^2}. \tag{42}$$

Let $\boldsymbol{y}_k$ be the Gaussian "raw" vector such that $\boldsymbol{y}_k = Q_n(\boldsymbol{y}_k)$. The variance estimate based on the nonquantized vector $\boldsymbol{y}_k$ is given by

$$\overset{\hat{\circ}}{\sigma}{}_k^{2} \overset{\mathrm{def.}}{=} \frac{1}{m-q}\left\|\mathbf{P}^\perp\,\boldsymbol{y}_k\right\|^2 = \frac{\sigma_k^2}{m-q}V_{n,k}. \tag{43}$$

It is well known that $V_{n,k} = \nu_2\,\frac{\overset{\hat{\circ}}{\sigma}{}_k^{2}}{\sigma_k^2}$ follows a central chi-square law with $\nu = m-q$ degrees of freedom [41]. From (42) and (43), it follows that:

$$U_{n,k} = V_{n,k} + \frac{1}{\sigma_k^2}\left(\left\|\mathbf{P}^\perp\,\boldsymbol{\epsilon}_k\right\|^2 + 2\boldsymbol{\epsilon}_k^\top\,\mathbf{P}^\perp\boldsymbol{y}_k\right) \tag{44}$$

where $\boldsymbol{\epsilon}_k \overset{\mathrm{def.}}{=} \tilde{\boldsymbol{y}}_k - \boldsymbol{y}_k$. The following formula is obtained by using the well-known results about the expectation of a quadratic form [47] and the results about quantization [48]

$$\begin{aligned}\mathbb{E}\left[\left\|\mathbf{P}^\perp\boldsymbol{\epsilon}_k\right\|^2\right] &= \mathbb{E}\left[\boldsymbol{\epsilon}_k^\top\mathbf{P}^\perp\boldsymbol{\epsilon}_k\right] \\ &= \left(\frac{\Delta_n^2}{12} + o(\Delta_n^2)\right)\mathrm{trace}\left(\mathbf{P}^\perp\right) \\ &= O(m\,\Delta_n^2)\end{aligned} \tag{45}$$

where $\mathrm{trace}\left(\mathbf{P}^\perp\right) = m-q$ is the trace of $\mathbf{P}^\perp$.

Expanding $\boldsymbol{\epsilon}_k^\top\,\mathbf{P}^\perp\boldsymbol{y}_k$ and using the results of [48] about the quantization of Gaussian variables together with the Cauchy-Schwarz inequality [43] gives that

$$\mathbb{E}\left[\left(\boldsymbol{\epsilon}_k^\top\mathbf{P}^\perp\boldsymbol{y}_k\right)^2\right] = O(m\,\Delta_n^2). \tag{46}$$

Moreover, the Cauchy-Schwarz inequality also yields to

$$\begin{aligned}&\mathbb{E}\left[\left|\frac{1}{U_{n,k}} - \frac{1}{V_{n,k}}\right|\right]^2 \\ &\quad\leq \mathbb{E}\left[\left|V_{n,k} - U_{n,k}\right|^2\right]\mathbb{E}\left[\frac{1}{V_{n,k}^2\,U_{n,k}^2}\right] \\ &\quad\leq \mathbb{E}\left[\left|V_{n,k} - U_{n,k}\right|^2\right]\sqrt{\mathbb{E}\left[\frac{1}{V_{n,k}^4}\right]\mathbb{E}\left[\frac{1}{U_{n,k}^4}\right]}.\end{aligned} \tag{47}$$

From [49], for large value of m, it is known that

$$\mathbb{E}\left[\frac{1}{V_{n,k}^4}\right] = \frac{1}{m^4} + O\left(\frac{1}{m^5}\right) \tag{48}$$

since $V_{n,k}$ follows a central chi-square law [41]. Thus, for n sufficiently large, using (44), (45), and (46), it is clear that

$$\mathbb{E}\left[\frac{1}{U_{n,k}^4}\right] < 1. \tag{49}$$

From (47), (48), and (49), it follows that:

$$\mathbb{E}\left[\left|\frac{1}{U_{n,k}}-\frac{1}{V_{n,k}}\right|\right]^2=O(\Delta_n^4). \tag{50}$$

Hence, (42) and (43) yields to

$$\mathbb{E}\left[\left|\frac{1}{\hat{\mathring{\sigma}}_k^2}-\frac{1}{\hat{\sigma}_k^2}\right|\right]=(m-q)\,O(\Delta_n^2). \tag{51}$$

Using the triangle inequality and the fact that $m=o(n)$, one obtains

$$\frac{1}{K_n}\mathbb{E}\left[\left|\sum_{k=1}^{K_n}\frac{1}{\hat{\mathring{\sigma}}_k^2}-\sum_{k=1}^{K_n}\frac{1}{\hat{\sigma}_k^2}\right|\right]=o\left(m\Delta_n^2\right). \tag{52}$$

Hence, since convergence in mean implies convergence in probability, (52) yields to

$$\frac{1}{K_n}\sum_{k=1}^{K_n}\frac{1}{\hat{\mathring{\sigma}}_k^2}\xrightarrow{P}\frac{1}{\hat{\overline{\sigma}}_n^2}<+\infty. \tag{53}$$

Using (43) and (46), for $\nu=m-q>4$, it is clear that

$$\mathbb{E}_{\boldsymbol{\omega}_k}[\hat{\mathring{\sigma}}_k^{-2}]=\frac{\nu}{\sigma_k^2(\nu-2)}\text{ and}$$
$$\mathbb{V}\mathrm{ar}_{\boldsymbol{\omega}_k}\left[\hat{\mathring{\sigma}}_k^{-2}\right]=\frac{2\nu^2}{\sigma_k^4(\nu-2)^2(\nu-4)}.$$

It follows that:

$$\mathbb{E}_{\boldsymbol{\omega}_k}\left[\frac{1}{K_n}\sum_{k=1}^{K_n}\frac{1}{\hat{\mathring{\sigma}}_k^2}\right]=\frac{1}{\overline{\sigma}_n^2}\frac{\nu}{(\nu-2)} \tag{54}$$
$$\mathbb{V}\mathrm{ar}_{\boldsymbol{\omega}_k}\left[\frac{1}{K_n}\sum_{k=1}^{K_n}\frac{1}{\hat{\mathring{\sigma}}_k^2}\right]=\frac{2\,\nu^2}{(\nu-2)\,(\nu-4)K_n^2}\sum_{k=1}^{K_n}\frac{1}{\sigma_k^4}. \tag{55}$$

Since σ_k^2 is bounded for all $1\le k\le K_n$, the random variables $\hat{\mathring{\sigma}}_k^2$ are clearly uniformly integrable [40] and $\sup_{n\geq 1}\mathbb{E}\left[\left|\hat{\mathring{\sigma}}_k\right|^6\right]<+\infty$. Hence, the moments of $\frac{1}{\hat{\overline{\sigma}}_n^2}$ converge toward the moments of $K_n^{-1}\sum_{k=1}^{K_n}\frac{1}{\hat{\mathring{\sigma}}_k^2}$. According to (53), the expectation and variance of $\frac{1}{\hat{\overline{\sigma}}_n^2}$ can be, respectively, approximated by (54) and (55). Thus, as $n\longrightarrow+\infty$, one obtains

$$\frac{1}{\hat{\overline{\sigma}}_n^2}\xrightarrow{p}\frac{1}{\overline{\sigma}_n^2}. \tag{56}$$

It follows that $\hat{\overline{\sigma}}_n\xrightarrow{p}\overline{\sigma}_n$. When ν is not sufficiently large to ensure that $\frac{\nu}{(\nu-2)}\approx 1$, (54) yields to the following alternative formula:

$$\hat{\overline{\sigma}}_n\xrightarrow{p}\overline{\sigma}_n\sqrt{\frac{\nu-2}{\nu}}. \tag{57}$$

B. Asymptotic Study of $\hat{\overline{\sigma}}_n$ Under Hypothesis $\underline{\mathcal{H}}_1$

Under hypothesis $\underline{\mathcal{H}}_1$, the estimates $\hat{\sigma}_k^2$ are obviously contaminated by the hidden bits. Fortunately, from (76) and (77), it is clear that the impact of the hidden bits on the variance estimate is negligible; this impact is entirely included in a residual term $O(\Delta_n^2)$. Hence, it is straightforward to prove that $\hat{\overline{\sigma}}_n\xrightarrow{p}\overline{\sigma}_n$. In fact, the proof is similar to the one derived under hypothesis $\underline{\mathcal{H}}_0$ provided that $\boldsymbol{y}_k$, used in the definition of $\boldsymbol{\epsilon}_k$, corresponds to the "raw" vector before the insertion of hidden bits. The results (45) and (46) remain unchanged under $\underline{\mathcal{H}}_1$. The convergences (56) and (57) are still satisfied.

C. Asymptotic False Alarm Probability

Under hypothesis $\underline{\mathcal{H}}_0$, $\boldsymbol{y}_k\sim P_{\boldsymbol{\omega}_k}$. A direct calculation immediately shows that

$$\mathbb{E}_{\boldsymbol{\omega}_k}[\hat{\gamma}_{k,j}]=o(\Delta_n^2) \tag{58}$$
$$\begin{aligned}\mathbb{V}\mathrm{ar}_{\boldsymbol{\omega}_k}[\hat{\gamma}_{k,j}]&=(1-p_{j,j})\left(\sigma_k^2+\frac{\Delta_n^2}{12}\right)+o(\Delta_n^2)\\&=(1-p_{j,j})\,\sigma_k^2+O(\Delta_n^2)\end{aligned} \tag{59}$$

where $\mathbb{E}_{\boldsymbol{\omega}_k}[\cdot]$, respectively, $\mathbb{V}\mathrm{ar}_{\boldsymbol{\omega}_k}[\cdot]$, denotes the expectation, respectively, the variance, when $\boldsymbol{y}_k\sim P_{\boldsymbol{\omega}_k}$. It follows that:

$$\mathbb{E}_{\boldsymbol{\omega}_k}[\hat{S}_k]=\mathbb{E}_{\boldsymbol{\omega}_k}[\sum_{j=1}^{m}\hat{\gamma}_{k,j}]=m\,o(\Delta_n^2), \tag{60}$$
$$\mathbb{V}\mathrm{ar}_{\boldsymbol{\omega}_k}[\hat{S}_k]=(m-q)\sigma_k^2+m\,O(\Delta_n^2) \tag{61}$$

where $\sum_{j=1}^{m}p_{j,j}=\mathrm{trace}\,(\mathbf{P})=q$.

In order to use again the Lindeberg central limit theorem, it is necessary to calculate the expectation and variance of $\hat{\gamma}_k$. This is the ratio of two (possibly dependents) random variables. Using the fact that $\mathbf{P}^{\perp}=\mathbf{I}_m-\mathbf{P}$, the definitions of $\hat{\ell}_{k,j}$ and $\ell_{k,j}$ yield to

$$\begin{aligned}\hat{\gamma}_{k,j}&=\eta_{k,j}\sum_{t=1}^{m}p_{j,t}^{\perp}\tilde{y}_{k,t}\\&=\eta_{k,j}\sum_{t=1}^{m}p_{j,t}^{\perp}(\tilde{y}_{k,t}-\ell_{k,t})\overset{\text{def.}}{=}z_{k,j}\end{aligned} \tag{62}$$
$$\hat{\sigma}_k^2=\frac{1}{m-q}\sum_{j=1}^{m}\left(\sum_{t=1}^{m}p_{j,t}^{\perp}\tilde{y}_{k,t}\right)^2=\frac{1}{m-q}\sum_{j=1}^{m}z_{k,j}^2 \tag{63}$$

where $p_{j,t}^{\perp}$ denotes the element of $\mathbf{P}^{\perp}$ at position (j,t). A short calculation shows that

$$\mathbb{C}\mathrm{ov}_{\boldsymbol{\omega}_k}[z_{k,i},z_{k,j}]=o(\Delta_n^4)$$

for $i\neq j$ where $\mathbb{C}\mathrm{ov}_{\boldsymbol{\omega}_k}[\cdot,\cdot]$ denotes the covariance when $\boldsymbol{y}_k\sim P_{\boldsymbol{\omega}_k}$. Let $\mathbf{z}_k=(z_{k,1},\ldots,z_{k,m})^{\top}$, $\sum_{j=1}^{m}z_{k,j}=\mathbf{1}^{\top}\mathbf{z}_k$ and $\sum_{j=1}^{m}z_{k,j}^2=\mathbf{z}_k^{\top}\mathbf{z}_k$ where $\mathbf{1}=(1,\ldots,1)^{\top}$ has the length m. Using again the results about the expectation and variance of a quadratic form [47], one obtains

$$\begin{aligned}\mathbb{C}\mathrm{ov}_{\boldsymbol{\omega}_k}\left[\sum_{j=1}^{m}z_{k,j},\sum_{j=1}^{m}z_{k,j}^2\right]&=\mathbb{C}\mathrm{ov}_{\boldsymbol{\omega}_k}\left[\mathbf{1}^{\top}\mathbf{z}_k,\mathbf{z}_k^{\top}\mathbf{z}_k\right]\\&=(m-q)\sigma_k^2\,O(\Delta_n^2).\end{aligned}$$

It follows that:

$$\mathbb{C}\mathrm{ov}_{\boldsymbol{\omega}_k}\left[\hat{S}_k, \hat{\sigma}_k^2\right] = O(\Delta_n^2). \tag{64}$$

In addition, a direct calculation shows that

$$\mathbb{E}_{\boldsymbol{\omega}_k}\left[\hat{\sigma}_k^2\right] = \sigma_k^2 + \frac{\Delta_n^2}{12} + o(\Delta_n^2) = \sigma_k^2 + O(\Delta_n^2) \tag{65}$$

$$\mathbb{V}\mathrm{ar}_{\boldsymbol{\omega}_k}\left[\hat{\sigma}_k^2\right] = \frac{2\left(\sigma_k^2 + \frac{\Delta_n^2}{12}\right)^2}{m-q} + o(\Delta_n^2) = o(\Delta_n^2). \tag{66}$$

Hence, as $n \longrightarrow +\infty$, $\hat{\sigma}_k^2 \xrightarrow{p} \sigma_k^2$ and the well-known Delta method [40], [50] yield to

$$\begin{aligned}\mathbb{E}_{\boldsymbol{\omega}_k}[\hat{\gamma}_k] &= \frac{1}{\sqrt{m-q}} \frac{\mathbb{E}_{\boldsymbol{\omega}_k}\left[\hat{S}_k\right]}{\mathbb{E}_{\boldsymbol{\omega}_k}\left[\hat{\sigma}_k^2\right]} \\ &\quad - \frac{1}{\sqrt{m-q}\,\mathbb{E}_{\boldsymbol{\omega}_k}\left[\hat{\sigma}_k^2\right]^2}\,\mathbb{C}\mathrm{ov}_{\boldsymbol{\omega}_k}\left[\hat{S}_k, \hat{\sigma}_k^2\right] \qquad (67) \\ &= \sqrt{m}\, o(\Delta_n^2). \qquad (68)\end{aligned}$$

The Delta method [40], [50] yields also to the well-known formula

$$\begin{aligned}\mathbb{V}\mathrm{ar}_{\boldsymbol{\omega}_k}\left[\frac{\hat{S}_k}{\hat{\sigma}_k^2}\right] &= \frac{\mathbb{V}\mathrm{ar}_{\boldsymbol{\omega}_k}[\hat{S}_k]}{\mathbb{E}_{\boldsymbol{\omega}_k}\left[\hat{\sigma}_k^2\right]^2} - \frac{2\mathbb{E}_{\boldsymbol{\omega}_k}\left[\hat{S}_k\right]}{\mathbb{E}_{\boldsymbol{\omega}_k}\left[\hat{\sigma}_k^2\right]^3} \\ &\quad \times \mathbb{C}\mathrm{ov}_{\boldsymbol{\omega}_k}\left[\hat{S}_k, \hat{\sigma}_k^2\right] \\ &\quad + \frac{\mathbb{E}_{\boldsymbol{\omega}_k}\left[\hat{S}_k\right]^2}{\mathbb{E}_{\boldsymbol{\omega}_k}\left[\hat{\sigma}_k^2\right]^4}\mathbb{V}\mathrm{ar}_{\boldsymbol{\omega}_k}\left[\hat{\sigma}_k^2\right] + o(\Delta_n^2).\end{aligned}$$

Using (61), (64), and (65), it follows that:

$$\begin{aligned}\mathbb{V}\mathrm{ar}_{\boldsymbol{\omega}_k}\left[\hat{\gamma}_k\right] &= \frac{1}{m-q} \frac{\mathbb{V}\mathrm{ar}_{\boldsymbol{\omega}_k}\left[\hat{S}_k\right]}{\mathbb{E}_{\boldsymbol{\omega}_k}\left[\hat{\sigma}_k^2\right]^2} + o(\Delta_n^2) \qquad (69) \\ &= \frac{1}{\sigma_k^2} + O(\Delta_n^2). \qquad (70)\end{aligned}$$

Hence, from (41), (68), (70), $n \sim (m-q)\,K_n$ and the Lindeberg central limit theorem, one obtains

$$\frac{\overline{\sigma}_n}{\sqrt{K_n}} \sum_{k=1}^{K_n} \hat{\gamma}_k \xrightarrow{d} \mathcal{N}(0,1).$$

From (56) and the Slutsky's Theorem [25, Theorem 11.2.11], it follows that $\hat{\Lambda}^* \xrightarrow{d} \mathcal{N}(0,1)$. To warrant the false alarm probability α, the threshold $\hat{\lambda}^*$ must be chosen such that $\hat{\lambda}^* = \Phi^{-1}(1-\alpha)$.

D. Asymptotic Correct Detection Probability

Under hypothesis $\underline{\mathcal{H}}_1$, $y_{k,j} \sim Q^R_{\boldsymbol{\theta}_{k,j}}$. A direct calculation shows that

$$\mathbb{E}_{\boldsymbol{\omega}_k,R}[\hat{\gamma}_{k,j}] = (1-p_{j,j}) R \frac{\Delta_n}{2} + o(\Delta_n^2), \tag{71}$$

$$\begin{aligned}\mathbb{V}\mathrm{ar}_{\boldsymbol{\omega}_k,R}[\hat{\gamma}_{k,j}] &= (1-p_{j,j}) \left(\sigma_k^2 + \frac{\Delta_n^2}{12} + R\frac{\Delta_n^2}{2}\right) \\ &\quad - (1-p_{j,j})^2 R^2 \frac{\Delta_n^2}{4} \\ &= (1-p_{j,j})\,\sigma_k^2 + O(\Delta_n^2) \qquad (72)\end{aligned}$$

where $\mathbb{E}_{\boldsymbol{\omega}_k,R}[\cdot]$, respectively, $\mathbb{V}\mathrm{ar}_{\boldsymbol{\omega}_k,R}[\cdot]$, denotes the expectation, respectively, the variance, when $\boldsymbol{y}_k \sim Q^R_{\boldsymbol{\omega}_k}$. It follows that:

$$\mathbb{E}_{\boldsymbol{\omega}_k,R}[\hat{S}_k] = R(m-q)\,\frac{\Delta_n}{2} + m\,o(\Delta_n^2) \tag{73}$$

$$\mathbb{V}\mathrm{ar}_{\boldsymbol{\omega}_k,R}[\hat{S}_k] = (m-q)\sigma_k^2 + m\,O(\Delta_n^2). \tag{74}$$

For $i \neq j$, a direct calculation shows that $\mathbb{C}\mathrm{ov}_{\boldsymbol{\omega}_k,R}[z_{k,i}, z_{k,j}] = p^{\perp}_{i,j}\, p^{\perp}_{j,i} \frac{R^2 \Delta_n^2}{4} + o(\Delta_n^2) = O(\Delta_n^2)$ where $\mathbb{C}\mathrm{ov}_{\boldsymbol{\omega}_k,R}[\cdot,\cdot]$ denotes the covariance when $\boldsymbol{y}_k \sim Q^R_{\boldsymbol{\omega}_k}$. Using again the results about the expectation and variance of a quadratic form [47], one obtains $\mathbb{C}\mathrm{ov}_{\boldsymbol{\omega}_k,R}[\sum_{j=1}^m z_{k,j}, \sum_{j=1}^m z^2_{k,j}] = (m-q)\sigma_k^2\, O(\Delta_n)$. It follows that:

$$\mathbb{C}\mathrm{ov}_{\boldsymbol{\omega}_k,R}\left[\hat{S}_k, \hat{\sigma}_k^2\right] = O(\Delta_n). \tag{75}$$

In addition, it is easily shown that

$$\begin{aligned}\mathbb{E}_{\boldsymbol{\omega}_k,R}[\hat{\sigma}_k^2] &= R\left(\sigma_k^2 + \frac{7\Delta_n^2}{12}\right) + (1-R)\left(\sigma_k^2 + \frac{\Delta_n^2}{12}\right) \\ &\quad + o(\Delta_n^2) \\ &= \sigma_k^2 + O(\Delta_n^2) \qquad (76) \\ \mathbb{V}\mathrm{ar}_{\boldsymbol{\omega}_k,R}[\hat{\sigma}_k^2] &= \frac{2\left(\sigma_k^2 + O(\Delta_n^2)\right)^2}{m-q} + o(\Delta_n^2) \\ &= o(\Delta_n^2). \qquad (77)\end{aligned}$$

Hence, using (67) adapted to hypothesis $\underline{\mathcal{H}}_1$ ($\mathbb{E}_{\boldsymbol{\omega}_k}[\cdot]$ and $\mathbb{C}\mathrm{ov}_{\boldsymbol{\omega}_k}[\cdot,\cdot]$ are replaced by $\mathbb{E}_{\boldsymbol{\omega}_k,R}[\cdot]$ and $\mathbb{C}\mathrm{ov}_{\boldsymbol{\omega}_k,R}[\cdot,\cdot]$), the Delta method yields to

$$\mathbb{E}_{\boldsymbol{\omega}_k,R}[\hat{\gamma}_k] = R\sqrt{m-q}\frac{\Delta_n}{2\sigma_k^2} + O(\Delta_n^2). \tag{78}$$

Using (75), (76), (77), and (69) adapted to hypothesis $\underline{\mathcal{H}}_1$, one obtains

$$\mathbb{V}\mathrm{ar}_{\boldsymbol{\omega}_k,R}[\hat{\gamma}_k] = \frac{1}{\sigma_k^2} + O(\Delta_n^2). \tag{79}$$

Hence, from the Lindeberg central limit theorem and the fact that $(m-q)\,K_n \sim n$, it follows that $\frac{\bar{\sigma}_n}{\sqrt{K_n}} \sum_{k=1}^{K_n} \hat{\gamma}_k \xrightarrow{d} \mathcal{N}(R\varrho, 1)$. From (56) and the Slutsky's Theorem, one obtains $\hat{\Lambda}^* \xrightarrow{d} \mathcal{N}(R\varrho, 1)$. This yields to $\lim_{n \longrightarrow +\infty} \beta_{\hat{\varphi}^*}(\boldsymbol{\omega}, R) = 1 - \Phi\left(\hat{\lambda}^* - R\varrho\right)$, $\forall \boldsymbol{\omega} \in \Omega_n$, $\forall R \in \mathcal{R}$. Using Theorem 1, the test $\hat{\varphi}^*(\boldsymbol{y}) \in \mathcal{D}_\alpha$ is AUMP since i) the structure of $\hat{\Lambda}^*(\boldsymbol{y})$ given in (41) does not depend on $\boldsymbol{\omega}$ and R and ii) $\beta_{\hat{\varphi}^*}(\boldsymbol{\omega}, R) \sim \beta_{\varphi^*}(\boldsymbol{\omega}, R)$, $\forall \boldsymbol{\omega} \in \Omega_n$, $\forall R \in \mathcal{R}$.

ACKNOWLEDGMENT

The author would like to thank P. Cornu, I. Nikiforov, F. Retraint, R. Cogranne, and C. Zitzmann from the Troyes

University of Technology (UTT), France, for our fruitful discussions. The author is grateful to the anonymous reviewers for their suggestions to improve the quality of the paper.

REFERENCES

[1] H. Sencar, M. Ramkumar, and A. Akansu, *Data Hiding Fundamentals and Applications: Content Security in Digital Multimedia*. Elsevier: Academic, 2004.

[2] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, *Digital Watermarking and Steganography*. San Francisco, CA: Morgan Kaufmann, 2007.

[3] J. Fridrich, *Steganography in Digital Media—Principles, Algorithms, and Applications*. New York: Cambridge Univ. Press, 2009.

[4] R. Böhme, *Advanced Statistical Steganalysis*. New York: Springer, 2010.

[5] N. Provos and P. Honeyman, "Hide and seek: An introduction to steganography," *IEEE Secur. Priv. J.*, vol. 1, no. 3, pp. 32–44, 2003.

[6] X.-Y. Luo, D.-S. Wang, P. Wang, and F.-L. Liu, "A review on blind detection for image steganography," *Signal Process.*, vol. 88, no. 9, pp. 2138–2157, Sep. 2008.

[7] A. Nissar and A. Mir, "Classification of steganalysis techniques: A study," *Digit. Signal Process.*, vol. 20, no. 6, pp. 1758–1770, 2010.

[8] X. X. Qin and M. Wang, "A review on detection of LSB matching steganography," *Inf. Technol. J.*, vol. 9, pp. 1725–1738, 2010.

[9] A. D. Ker, "Locating steganographic payload via WS residuals," in *ACM Proc. 10th Multimed. Secur. Workshop*, 2008, pp. 27–31.

[10] A. D. Ker, "A general framework for the structural steganalysis of LSB replacement," in *Proc. 7th Inf. Hiding Workshop, ser. Springer LNCS*, 2005, vol. 3727, pp. 296–311.

[11] J. Fridrich, M. Goljan, and R. Du, "Detecting LSB steganography in color and grayscale images," *IEEE Multimedia*, vol. 8, no. 4, pp. 22–28, 2001.

[12] S. Dumitrescu, X. Wu, and Z. Wang, "Detection of LSB steganography via sample pair analysis," *IEEE Trans. Signal Process.*, vol. 51, pp. 1995–2007, Jun. 2003.

[13] A. Ker, "Steganalysis of LSB matching in grayscale images," *Signal Process. Lett.*, vol. 12, no. 6, pp. 441–444, Jun. 2005.

[14] A. D. Ker, "A fusion of maximum likelihood and structural steganalysis," in *Proc. 9th Inf. Hiding Workshop, ser. Springer LNCS*, 2007, vol. 4567, pp. 204–219.

[15] K. Lee, A. Westfeld, and S. Lee, "Generalised category attack—Improving histogram-based attack on JPEG LSB embedding," *Inf. Hiding'07*, pp. 378–391, 2007.

[16] J. Fridrich and M. Goljan, "On estimation of secret message length in LSB steganography in spatial domain," in *Secur., Steganogr. Watermarking of Multimed. Contents VI, ser. Proc. SPIE*, 2004, vol. 5306, pp. 23–34.

[17] A. D. Ker and R. Böhme, "Revisiting weighted stego-image steganalysis," in *Proc. SPIE 6819 Secur., Forens., Steganogr. Watermarking of Multimed. Contents X*, 2008, pp. 501–517.

[18] A. Westfeld and A. Pfitzmann, "Attacks on steganographic systems," *Inf. Hiding'99*, pp. 61–76, 1999.

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

[20] H. V. Poor, *An introduction to Signal Detection and Estimation*. New York: Springer-Verlag, 1988.

[21] L. L. Scharf, *Statistical Signal Processing: Detection, Estimation, and Time-series Analysis*. Reading, MA: Addison-Welsey, 1993.

[22] L. Scharf and B. Friedlander, "Matched subspace detectors," *IEEE Trans. Signal Process.*, vol. 42, no. 8, pp. 2146–2157, 1994.

[23] S. Kraut, L. Scharf, and L. McWhorter, "Adaptive subspace detectors," *IEEE Trans. Signal Process.*, vol. 49, no. 1, pp. 1–16, 2001.

[24] A. D. Ker, "The square root law does not require a linear key," in *ACM Proc. 12th Multimed. Secur. Workshop*, 2010, pp. 213–223.

[25] E. L. Lehmann and J. P. Romano, "Testing statistical hypotheses," in *Ser. Springer Texts in Statistics*, 3rd ed. New York: Springer, 2005.

[26] A. A. Borovkov, *Mathematical Statistics*. Amsterdam: Gordon and Breach Sciences, 1998.

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

[28] C. Zitzmann, R. Cogranne, F. Retraint, I. Nikiforov, L. Fillatre, and P. Cornu, "Statistical decision methods in hidden information detection," in *Inf. Hiding'2011*, Prague, Czech Republic, 2011, vol. LNCS 6958, pp. 163–177.

[29] R. Cogranne, C. Zitzmann, L. Fillatre, I. Nikiforov, F. Retraint, and P. Cornu, "Reliable detection of hidden information based on a non-linear local model," in *Proc. Stat. Signal Process. Workshop*, Nice, France, 2011, pp. 493–496.

[30] C. Zitzmann, R. Cogranne, F. Retraint, I. Nikiforov, L. Fillatre, and P. Cornu, "Hypothesis testing by using quantized observations," in *Proc. Stat. Signal Process. Workshop*, Nice, France, 2011, pp. 501–504.

[31] R. Cogranne, C. Zitzmann, L. Fillatre, F. Retraint, I. Nikiforov, and P. Cornu, "Statistical decision by using quantized observation," in *Proc. Int. Symp. Inf. Theory*, St. Petersburg, Russian, 2011, pp. 1135–1139.

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

[33] A. Foi, M. Trimeche, V. Katkovnik, and K. Egiazarian, "Practical Poissonian-Gaussian noise modeling and fitting for single-image raw-data," *IEEE Trans. Image Process.*, vol. 17, no. 10, pp. 1737–1754, 2008.

[34] H. H. Barrett and K. J. Myers, *Foundations of Image Science*. New York: Wiley, 2004.

[35] A. Blake and A. Zisserman, *Visual Reconstruction*. Cambridge, MA: MIT Press, 1987.

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

[37] R. Ramanath, W. E. Snyder, Y. Yoo, and M. S. Drew, "Color image processing pipeline," *IEEE Signal Process. Mag.*, vol. 22, pp. 34–43, 2005.

[38] R. Gray and D. Neuhoff, "Quantization," *IEEE Trans. Inf. Theory*, vol. 44, pp. 2325–2384, 1998.

[39] D. Hui and D. Neuhoff, "Asymptotic analysis of optimal fixed-rate uniform scalar quantization," *IEEE Trans. Inf. Theory*, vol. 47, no. 3, pp. 957–977, 2001.

[40] P. Billingsley, "Probability and measure," in *Ser. Wiley Series in Probability and Mathematical Statistics*. New York: Wiley, 1995.

[41] L. Fillatre and I. Nikiforov, "Non-Bayesian detection and detectability of anomalies from a few noisy tomographic projections," *IEEE Trans. Signal Process.*, vol. 55, no. 2, pp. 401–413, 2007.

[42] L. Fillatre, I. Nikiforov, and F. Retraint, "Epsilon-optimal non-Bayesian anomaly detection for parametric tomography," *IEEE Trans. Image Process.*, vol. 17, no. 11, pp. 1985–1999, 2008.

[43] C. Rao, *Linear Statistical Inference and Its Applications*, 2nd ed. New York: Wiley, 1973.

[44] BOSS 2010, Break Our Steganography System, 2010 [Online]. Available: http://boss.gipsa-lab.grenoble-inp.fr/BOSSRank

[45] P. Lu, X. Luo, Q. Tang, and L. Shan, "An improved sample pairs method for detection of LSB embedding," in *Proc. Int. Workshop on Inf. Hiding*, 2004, vol. 3200, pp. 116–127.

[46] J. Fridrich, M. Goljan, and R. Du, "Reliable detection of LSB steganography in color and grayscale images," in *ACM Proc. Multimed. Secur. Workshop*, 2001, pp. 27–30.

[47] A. C. Rencher and B. G. Schaalje, *Linear Models in Statistics*, 2nd ed. New York: Wiley-Interscience, 2008.

[48] A. B. Sripad and D. L. Snyder, "A necessary and sufficient condition for quantization errors to be uniform and white," *IEEE Trans. Signal Process.*, vol. 25, no. 5, pp. 442–448, 1977.

[49] T. Fujioka, "Asymptotic approximations of the inverse moment of the noncentral chi-squared variable," *J. Japan Statist. Soc.*, vol. 31, no. 1, pp. 99–109, 2001.

[50] C. G. Small, *Expansions and Asymptotics for Statistics*. London, U.K.: Chapman and Hall, 2010.

Lionel Fillatre (M'11) received the M.Sc. degree in decision and information engineering and the Ph.D. degree in systems optimization from the Troyes University of Technology (UTT), France, in 2001 and 2004, respectively.

From 2005 to 2007, he was with Télécom Bretagne, Brest, France. Since 2007, he has been an Associate Professor with the Systems Modelling and Dependability Laboratory, UTT. His current research interests include statistical decision theory, signal and image processing, and network monitoring.