Signal Processing: *Image Communication* 26 (2011) 567–576

Contents lists available at ScienceDirect

Signal Processing: *Image Communication*

journal homepage: www.elsevier.com/locate/image

How quantization based schemes can be used in image steganographic context

Sofiane Braci *, Claude Delpha *, Rémy Boyer

Laboratoire des Signaux et Systèmes, Université Paris-Sud – CNRS – SUPELEC, 3, rue Joliot-Curie, 91190, Gif-sur-Yvette, France

ARTICLE INFO

Article history:
Received 18 August 2010
Accepted 18 July 2011
Available online 28 July 2011

Keywords:
Image processing for watermarking and steganography
Costa scheme
Spread transform

ABSTRACT

The quantization based embedding systems are widely used in the information hiding applications, thanks to their efficiency and simplicity. Moreover, they are known to be insecure in steganography context according to the Cachins' security definition because they distort the stego-signal probability density function. In this paper, we show that using the well-known spread transform (ST) combining with quantization based embedding systems provides an ε-secure stego-system in the sense of Cachin's security definition. In other words, we show theoretically that this system preserves, in the sense of the relative entropy, the probability density function of the stego-signal as long as the ratio between the quantization step and the square root of the spreading factor is small. This highlights the fundamental tradeoff between these two quantities. Our theoretical conclusions are validated and illustrated on real images. Finally, a comparison with the Solanki et al. blind steganographic scheme is given.

0. Introduction

In data-hiding [1], a very old field named Steganography is used since the antiquity [2,3]. It seeks to provide a covert communication channel between two parties. As defined by Cox et al. [4] steganography denotes "*…the practice of undetectably altering a work to embed a message*". In the classical problem of the prisoners [5], Alice and Bob are in prison and try to escape. They can exchange documents, but these documents are controlled by the warden, a passive opponent who intercepts all communications between the two prisoners and analyzes them (statistical analysis). If he finds that the transmitted documents are suspicious, the communication will be interrupted between Alice and Bob. Thus, the prisoners must use an efficient stego-system to exchange stego-messages secretely and securely. Fig. 1 summarizes the general steganography scheme in passive warden context.

The quantization based embedding systems are widely used in robust watermarking for their robustness against attacks [6–8]. In some situations, there is a need to have a data-hiding scheme which is not only robust but also undetectable [9]. This scenario is realistic when the channel over which the stego-message is transmitted is noisy, corresponding to the case of an active warden. In this case, the methods specifically designed for steganographic applications are not adapted because they are fragile against attacks [10–12]. So, we follow a similar way as Moulin et al. [9,13] and Guillon et al. [14] works. But, in the opposite of these two approaches, we focus our study on the Spread Transform Quantization Index Modulation (ST-QIM) since this scheme is independent of the statistics of the cover-signal [15]. This confers to this method a high degree of flexibility. Another advantage is that the ST-QIM has a relatively low computational cost and can be implemented for real-time applications. More accurately, in this paper we study theoretically the security level in the sense of Cachin's definition [16] of the ST-QIM system. It is well-known that

* Corresponding authors.
E-mail addresses: Sofiane.Braci@lss.supelec.fr (S. Braci), Claude.Delpha@lss.supelec.fr (C. Delpha), Remy.Boyer@lss.supelec.fr (R. Boyer).

0923-5965/$ - see front matter © 2011 Elsevier B.V. All rights reserved.
doi:10.1016/j.image.2011.07.006

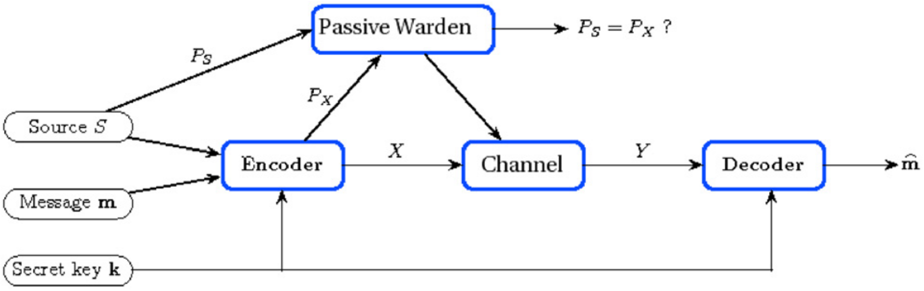

Fig. 1. Communication-theoretic view of steganography in passive warden context.

the QIM [6] is a simple and efficient data-hiding system in the context of robust watermarking but this scheme is known to be insecure in the context of the steganography. This can be explained by the packetization effect during the quantization process leading to discontinuities in the stego-signal probability density function (p.d.f.) [14]. In this paper, we show by means of a theoretical formulation that the Spread Transform (ST) also makes some quantization based stego-systems almost statistically undetectable, called ε-secure in Cachin's terminology. As noted by Cox et al. [4], "*the main requirement of steganography is undetectability*". Another important requirement is the payload, in this work, we assume that the most important characteristic is the undetectability at a possible price of a payload loss. Such an assumption is also used in [10] by Solanki et al. to enhance the algorithm stego-security. Note that the use of the ST in the steganographic context to improve the undetectability at the price of a possible payload loss can be viewed in a similar way as Eggers et al. in the context of robust watermarking [17], where the use of the ST improves the robustness at a possible price of Capacity loss. To illustrate our derivation on real images, we measure the security enhancement by using the 1-D and 2-D relative entropy [18] between the stego-signal and the cover-signal.

In this paper, we try to answer to the question given in the title: how quantization based schemes can be used in steganographic context. Thus, Section 1.1 starts by presenting the security criterions' since the main constraint for using the quantization based scheme in steganography is the induced distortions on stego-signal statistics. In Section 1.2, we introduce the data-hiding schemes based on quantization through a basic one: Quantization Index Modulation (QIM). A steganographic study of the latter data-hiding system is given by analyzing the statistical effects on the stego-signal. A short description of the spread transform approach is afterwards given in Section 1.3. The major contribution of this paper is given in Section 1: *We give the theoretical developments to identify the constraints and conditions to make the quantization based schemes* ε*-secure and perfectly secure.* Then, we use the experiences result on real images in Section 2 to validate and explain the obtained performance given through the theoretical formulations. A comparison with a well-known and efficient steganographic scheme fully described in [10] is also proposed. Finally, we give the conclusions on the obtained results and present some interesting trends to continue the proposed work.

1. Related work and security criterion

1.1. Security criterion

Guillon et al. [14] present three criterions assessing that a stego-system is secure. The first one is *the embedding distortion* because any perceptual distortion on the stego-signal affects the secrecy of the communication. The second is *Anderson's criterion* which is linked to the encrypted algorithm, where the security depends on the aptitude of the opponent to decrypt the hiding message [2]. The third one is Cachin's criterion [16] which is taken as a security criterion for this paper since it is the most commonly used security criterion.

Cachin [16] uses the relative entropy between the probability density function (p.d.f.) of cover-content and the stego-content to characterize the security in steganographic context.

Let us consider the cover-signal *s* and the stego-signal *x*, respectively, modeled by the random variables *S* and *X*. Cachins' relative entropy $D(S\|X)$ (also called the Kullback–Leibler distance (KLD) or the discrimination) is given by:

$$D(S\|X) = \sum_{c \in \mathcal{C}} p_S(c) \log \frac{p_S(c)}{p_X(c)}, \tag{1}$$

where c is a content which belongs to the set of possible contents $\mathcal{C}$, distributed as $p_S(c)$ when Alice is passive and as $p_X(c)$ when she is active. Cachin [16] defined an ε-secure stego-system against passive warden as

$$D(S\|X) \leq \varepsilon, \tag{2}$$

where ε is real small positive and he considers a system to be perfectly secure when $\varepsilon = 0$. Note that the level of stego-security decreases when the relative entropy increases. In the following section, we use the Cachin criterion to assess if the stego-systems is secure or not.

1.2. Related work: quantization based systems in steganographic context

The quantization based stego-systems [4] are characterized by their simplicity and good performance (see, for example, paper [19]). Especially when the warden becomes active or the transmission channel is noisy (it is more realistic than in steganographic theory which supposes that the environment is noiseless). The good performance of quantization based systems is mostly explained by using the cover-signal as a side information in the same way as Costas' works [20].

Among the first quantization based stego-system, we can find the Quantization Index modulation (QIM) [21] (the QIM was proposed in the robust watermarking context), this scheme is probably the most popular one.

1.2.1. Quantization index modulation (QIM)

Let us describe the QIM stego-system through an example, consider the case where we wish to embed one bit of information per cover-sample. So, the stego-message bit m is in the set 0,1}, meaning that we need two quantifiers. Their corresponding sets of reconstruction points in $\mathcal{R}^n$ are indicated in Fig. 2(a) by yellow color points for the first quantifier and by the red color points for the second quantifier. The denomination QIM systems mean that the index to be transmitted *modulates* the quantization. Namely, if $m=0$, the cover-signal s is quantized with the yellow color points quantifier and with the red color points quantifier if $m=1$. Denoting by $Q(s)$ the reconstruction point of s, the embedded codeword e is set to the quantization error $Q(s)-s$. Hence, the stego-signal $x=s+e$ is represented by yellow color points if $m=0$ and by red color points if $m=1$.

1.2.2. Quantization based stego-systems effects

The blind quantization based data-hiding systems insert the message in the cover-signal by modifying the original samples, the system constructs a number of sets corresponding to the message. In other words, the set of the stego-samples defines the transmitted information. Modifying the stego-samples according to the stego-message increases the amount of samples belonging to the reconstructions points sets of dither quantifiers and eliminates the rest of cover-samples (see Fig. 2(b)). All the points of the quantifiers cells are shifted to the reconstruction points. Statistically and from Fig. 2, the probability that a sample of the stego-signal takes the reconstruction points values is increased and becomes null for the rest of samples which are not quantifiers reconstruction points. Then, many holes appear on the stego-signal histogram Fig. 2(b).

In the steganographic context [4], we suppose that the warden knows the statistics of the host signal. She knows that statistically in some intervals all values appear at least one time in the transmitted signal. If the stego-signal is inserted thanks to the quantization based stego-system, many samples' values do not exist in the stego-signal and the stego-message will be detected from the transmitted signal. According to the Cachin criterion, these systems are not secure since the difference between the p.d.f. of the stego-signal and the p.d.f. of the cover-signal becomes important and the relative entropy will be high.

There exist many variants of the QIM stego-system which may remove the quantization distortions. The Distortion Compensation Quantization Index Modulation (DC-QIM) [6] or Scalar Costa Scheme (SCS) [17] was proposed in context of robust watermarking. They make a compensation of the quantization error in order to increase the capacity of the watermarking system and limit the visual impact. However, Guillon et al. [14] show that the compensation does not make the QIM secure according to Cachins' criterion except with a specific compensation and for uniform distributed cover-signals (not realistic). Thus, they propose in [14] to use a compressor in order to obtain a uniform distributed cover-signal. The proposed method presents a limitation concerning its flexibility, since the compressor depends on the pdf of the stego-signal. Le Guelvouit in [22] proposes to use the Trellis Coded Quantization (TCQ) in order to embed the stego-message by forcing the trellis path according to the transmitted message (see also [15]). Even if the stego-system has interesting steganographic performance, we must use a very important number of trellis states, and increase exponentially the system complexity, to obtain an improved statistical invisibility [15].

1.3. Spread transform (ST) recall

In [6], the authors describe the ST in context of robust watermarking and present this system as a way to improve the robustness of the watermarking technics. In this work, we are interested by the performance of the ST in the

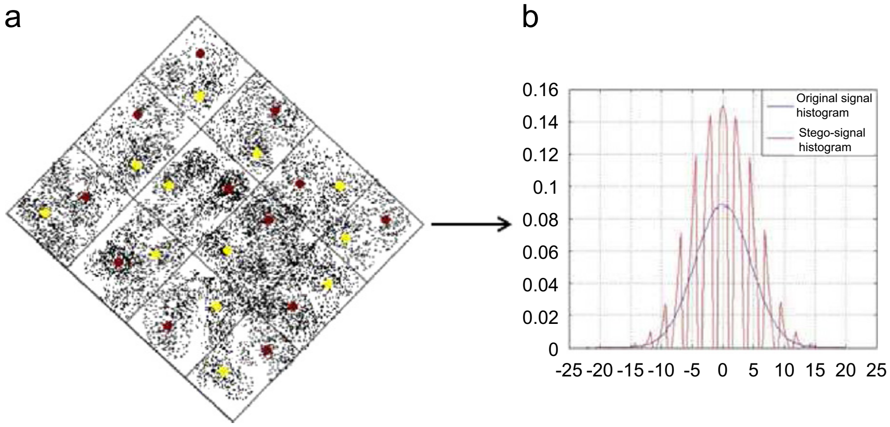

Fig. 2. (a) The quantization index modulation (QIM) stego-system applied to a 2-D signal. The yellow points correspond to the reconstruction points of the quantifier Q_0 which inserts an information bit equal to 0. The red points correspond to the reconstruction points of the quantifier Q_1 which inserts an information bit equals to 1. (b) The histograms of the cover and stego-signal when the QIM is used with 1-D signal (it can be the projection of the 2-D signal of (a)). (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

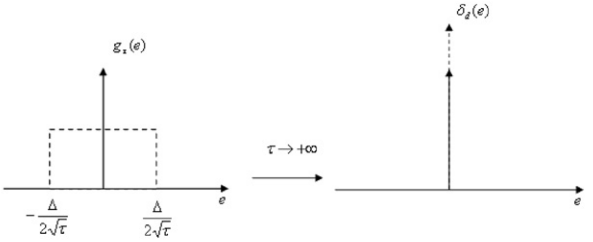

Fig. 3. The uniform density function tends to the dirac function when the spreading factor tends to the infinity.

steganographic context. The transformation of the cover-signal s is given by $s_l^{st} = \sum_{i=\tau l}^{\tau l+\tau-1} s_i t_i$ (see [17] for more details), where $\tau \in \mathcal{N}^\star$ is the spreading factor. We consider that the ith spreading parameter t_i takes only two possible values $\pm 1/\sqrt{\tau}$ as in [17] to obtain a normalized projection vector and spread uniformly the embedding distortion over all cover-samples. Then, the inverse transformation is applied to the transformed stego-signal: $x^{st} = s^{st} + e^{st}$, where e^{st} is the embedding signal (generated from the stego-message) in the transformed domain and we obtain

$$x = s + \underbrace{e^{st} \times t}_{e}, \tag{3}$$

where e is a sample of the embedded signal.

2. Spread transform in steganography: main theoretical contribution

Let us consider the case of high resolution quantization scheme, i.e. the quantization step Δ is very small comparing to the cover-signal variance σ_S^2, which is a very common case due to perceptual constraints. Thus, we know that the quantization error has a uniform p.d.f. and belongs to the interval $[-\frac{\Delta}{2}, \frac{\Delta}{2}]$ (see [23]). Since the embedding procedure, in the quantization based system, is an addition of a quantization error (produced by the QIM [6] for example) or a weighted quantization error (produced by the SCS [17]), the embedded signal density function will be uniform. Since the spreading parameter t takes two possible values $\pm 1/\sqrt{\tau}$, the embedding signal e has also a uniform p.d.f. but varies into the interval $[-\frac{\Delta}{2\sqrt{\tau}}, \frac{\Delta}{2\sqrt{\tau}}]$. Thus, the embedded signal p.d.f. can be written as:

$$p_E(x) = \frac{\sqrt{\tau}}{\Delta} 1_{[-\Delta/(2\sqrt{\tau}), \Delta/(2\sqrt{\tau})]}(x), \tag{4}$$

since $1_{[.]}(.)$ represents a unit indicator function and the embedded signal in the transformed domain e^{st}, is considered as independent from the original signal in the transformed domain s^{st}, in addition the spreading parameter t is independent from the cover-signal s. The embedded signal e and the cover-signal s are independent. Then, the p.d.f. of the stego-signal p_X is the convolution between the host-signal p.d.f. p_S and the embedded signal p.d.f. p_E, i.e.,

$$p_X(x) = (p_S * p_E)(x) = \frac{\sqrt{\tau}}{\Delta} \int_{-\infty}^{\infty} p_S(z) p_E(x-z)\, dz. \tag{5}$$

Using Eq. (4 and the obvious property: $1_{[-\Delta/(2\sqrt{\tau}), \Delta/(2\sqrt{\tau})]}(x-z) = 1_{[x-\Delta/(2\sqrt{\tau}), x+\Delta/(2\sqrt{\tau})]}(z)$, we have

$$p_X(x) = \frac{\sqrt{\tau}}{\Delta} \int_{-\infty}^{\infty} p_S(z) 1_{[x-\Delta/(2\sqrt{\tau}), x+\Delta/(2\sqrt{\tau})]}(z)\, dz \tag{6}$$

$$p_X(x) = \frac{\sqrt{\tau}}{\Delta} \int_{x-\Delta/(2\sqrt{\tau})}^{x+\Delta/(2\sqrt{\tau})} p_S(z)\, dz. \tag{7}$$

So, the p.d.f. of the stego-signal p_X can be viewed as the area of the region bounded by the host-signal p.d.f. p_S in the interval $[x-\Delta/(2\sqrt{\tau}), x+\Delta/(2\sqrt{\tau})]$. If this interval is tight, i.e., the right and left bounds are close to x, we can closely approximate p_X using the trapezoidal rule [24] over this interval. Then we obtain

$$p_X(x) \simeq \frac{1}{2}\left(p_S\left(x + \frac{\Delta}{2\sqrt{\tau}}\right) + p_S\left(x - \frac{\Delta}{2\sqrt{\tau}}\right)\right), \tag{8}$$

thus, we have two cases:

2.0.1. *Infinite spreading factor*

when the spreading factor τ is large (considered infinite), the uniform p.d.f. g_τ of the embedded-signal becomes a dirac function δ_d (as illustrated in Fig. 3) defined as follows:

$$\delta_d = \begin{cases} +\infty & \text{if } e = 0 \\ 0 & \text{if } e \neq 0 \end{cases} \quad \text{and} \quad \int_{-\infty}^{\infty} \delta_d(e)\, de = 1. \tag{9}$$

Therefore, the p.d.f. of the stego-signal is given by:

$$p_X(x) = (p_S * \delta_d)(x) = p_S(x). \tag{10}$$

We can readily check that the embedding does not induce any modification on the stego-signal p.d.f. thanks to the ST. In Cachin framework, this means $D(p_S \| p_X) = 0$ (perfectly secure stego-system). Note that this result is easily generalized with a non-uniform quantifier with limited cells size and high dimensional signal. In practical case, such an infinite factor is not useful. In fact, assuming that factor means that the stego-system payload is very small (close to zero) but such a value cannot be accepted in steganographic applications. For this reason, a more realistic case is the case of a finite spreading factor.

2.0.2. *Finite spreading factor*

Condition to satisfy. Inspecting Eq. (8), we can verified that $p_X(x) \simeq p_S(x)$ if $\Delta/2\sqrt{\tau} \ll 1$. This means that the ST permits to preserve, in the sense of the relative entropy, the probability density function of the stego-signal as long as the ratio between the quantization step and the square root of the spreading factor is small.

We know that the error I_{Err} induced by the integral approximation [24] is given by

$$I_{Err} = \frac{\Delta^3}{12\tau\sqrt{\tau}} p_S''(\theta), \tag{11}$$

where $p_S''(\theta)$ is the second order derivative of the probability density function p_S considered on θ which can take any values in the interval $[x-\Delta/(2\sqrt{\tau}), x+\Delta/(2\sqrt{\tau})]$.

Analysis of the expression of the error if case of i.i.d. Gaussian signals. If the cover-signal samples modeled by the random variable S are independent and identically distributed (i.i.d) and have a gaussian distribution[1] with mean γ_S and variance σ_S^2 defined as follows,

$$p_S(s)=\frac{1}{\sqrt{2\pi\sigma_S^2}}\cdot e^{-(s-\gamma_S)^2/2\sigma_S^2}, \tag{12}$$

then, a simple development shows that the second derivation is given by

$$p''_S(s)=\frac{1}{\sigma_S^2}\left(\frac{(s-\gamma_S)^2}{\sigma_S^2}-1\right)\cdot p_S(s). \tag{13}$$

Thus, when the cover-signal samples are modeled by an i.i.d gaussian variable, Eq. (11) becomes[2]

$$I_{Err}=\frac{\Delta^3}{12\tau\sqrt{\tau}}\frac{1}{\sigma_S^2}\left(\frac{(\theta-\gamma_S)^2}{\sigma_S^2}-1\right)\cdot p_S(\theta). \tag{14}$$

We studied the behavior of the integration error function—given in Eq. (14). We find that the first derivation of the error function of Eq. (14) equals to zero in three points, thus, it accepts three extremum:

- *two maximum*: for $\theta=\gamma_S\pm\sqrt{\sigma_S^2+2}$ and the integration error is
$$I_{Err}^{max}=\frac{\Delta^3}{12\tau\sqrt{\tau}}\frac{2}{\sigma_S^4\sqrt{2\pi\sigma_S^2}}\cdot e^{-\sigma_S^2+2/2\sigma_S^2} \tag{15}$$
- *one minimum*: for $\theta=\gamma_S$ and the integration error can be given by,
$$I_{Err}^{min}=-\frac{\Delta^3}{12\tau\sqrt{\tau}}\frac{1}{\sigma_S^2\sqrt{2\pi\sigma_S^2}}. \tag{16}$$

Fig. 4(a) shows that the maximum error (the maximum overestimation of the integration) and the minimum error (the maximum underestimation of the integration) converges quickly to 0 when the ratio $\Delta/\sqrt{\tau}$ decreases. Note that the variation interval used to compute the curves of Fig. 4(a) is close to the practical case, especially, for an image cover-signal. In the latter, the quantifier step Δ is generally limited to preserve the perceptual quality since it affects the embedding strength and the Document to Watermark Ratio (d.w.r.) (see [6] for more details). Also, the spreading factor τ must be as important as possible to resist against attacks. Thus, the integration error depends only on the cover-signal variance. When the cover-signal variance is large, the maximum error becomes very small (even if the quantity $\Delta^3/(12\tau\sqrt{\tau})$ has not a small value).

For an assumed gaussian cover-signal, Fig. 4(b) shows that beyond approximatively $\tau=8$ the ST-QIM has relatively small and constant relative entropy corresponding meaning a high security level according to Cachins' criterion. In this paragraph, we explain how the ST removes the distortion in the limit case (which is close to the reality).

3. Experimental results

3.1. Steganographic performances of our proposal

To validate our theoretical conclusions, let us consider the synthetic image given in Fig. 6(a), it is composed of 16 similar blocks of pixels gray level evolving along the diagonal. Each blocks contains one information bit. The QIM stego-systems with a document-to-watermark ratio (d.w.r.) equals to 30 dB is used. We insert the message given by the following matrix:

$$\mathbf{M}=\begin{pmatrix}1&1&0&0\\1&0&1&1\\1&0&0&0\\1&0&0&0\end{pmatrix}.$$

From Fig. 6(b) we clearly see the effects of the stego-message embedding on the stego-image. The first effect is the "packetization" of the stego-image pixels provided by the quantifiers. Since all the pixels of the quantization cell take the value of the reconstruction points. The second effect is that the warden Eve is able to make the difference between the hidden bits of the stego-messages and she can read the transmitted message. If we analyze the stego-message and the corresponding message matrix, it appears that there is two kinds of stego-blocks. In the blocks corresponding to a hidden bits equal to 1, the band of pixels with high value (the white pixels) is larger than the band with low pixels values (the black pixels). In opposite, the blocks with a black band larger than the white one corresponds to a hidden message bit equals to 0.

Fig. 6(c) shows the histogram of the stego-image given in Fig. 6(b). Note that the histogram of a stego-signal becomes "spiky". Thus, the presence of some values becomes very probable and other values becomes impossible. This is because the QIM enhances the occurrence of the reconstruction points of the quantifiers and removes a number of values sample from the stego-signal. Fig. 6(d) shows a stego-image where the ST-QIM is used with a spreading factor τ equals to 8 (from Fig. 4(b) beyond approximatively $\tau=8$ the security level becomes invariant when τ increases). We note that with the ST, the variation becomes smoother than with the classic QIM, in addition, the stego-image histogram (see Fig. 6(e)) follows the cover-image one, even if there is some slight distortions. The explanation of these performances is that the ST inserts the stego-message in a transformed domain and the transformation is made on several pixels. From the formulation of a cover-signal transformation [17], we note that the ST-QIM generates the stego-signal by using a weighted mean of several cover-samples values. Thus, the quantization error will be limited since the reconstruction

[1] The assumption if i.i.d. gaussian signal is realistic because it is well-known that when considering real images, DCT (Discrete Cosine Transform) is often considered. The DCT coefficients distribution is well-approximated by a gaussian when taking the assumption of the central limit theorem [25,26]. Because of the nature of the DCT coefficients, the variance of the gaussian distribution by invoking the central limit theorem is directly proportional to the variance of the DCT considered block.

[2] Nevertheless, if the central limit theorem cannot be applied, an assumption of a Laplacian modeling can be proposed. Eq. (12) for a Laplacian function becomes $p_S(s)=(1/2b)\cdot e^{-|s-\gamma_S|/b}$, with b a scaling factor. Thus Eq. (13) for a Laplacian case becomes $p''_S(s)=(1/b^2)\times p_S(s)$ and the error can be computed.

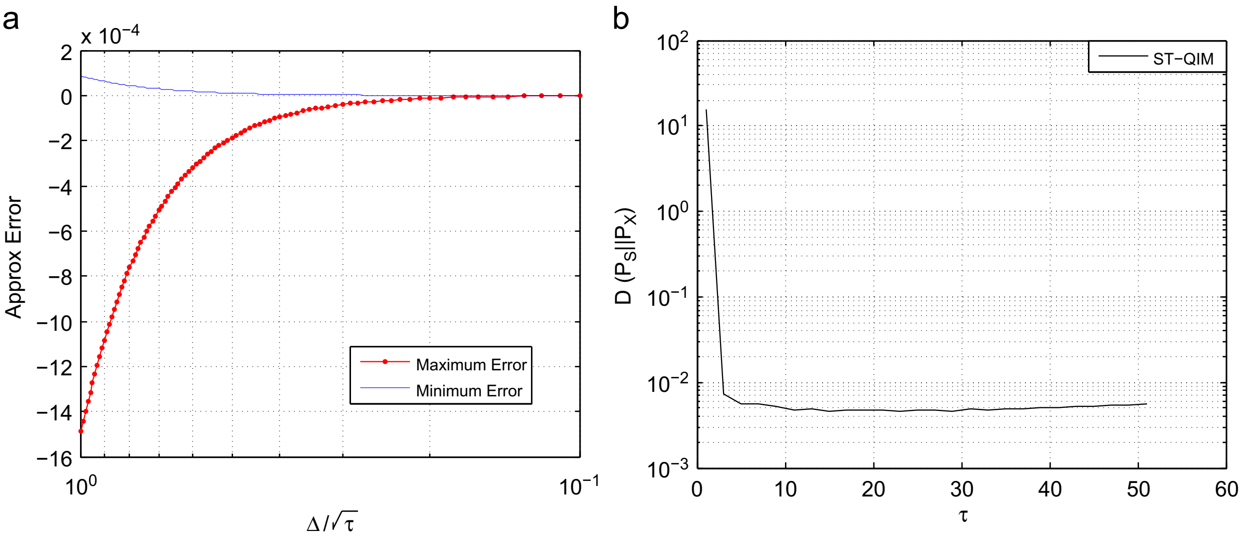

Fig. 4. (a) Minimum and maximum error (given by Eqs. (15) and (16)) as function of $\Delta/\sqrt{\tau}$ for $\sigma_S^2=20$. (b) The relative entropy between the probability density functions of the cover-signal and the stego-signal as function of τ for an ST-QIM stego-system (Document to watermark ratio equal to 15 dB).

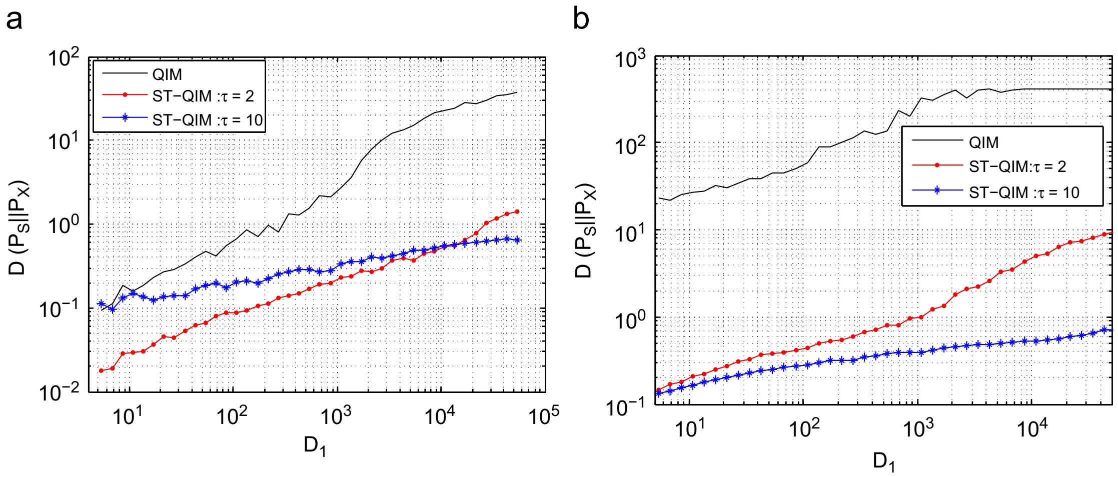

Fig. 5. (a) The 1-D relative entropy between the density functions of the cover and stego-signal with respect to the embedding strength D_1, for the QIM and ST-QIM stego-system; we use 100 different real images of size 350 × 350 pixels. (b) The 2-D relative entropy between the density functions of the cover and the stego-signals with respect to the embedding strength D_1, for the QIM and ST-QIM stego-system; we use 100 different real images of size 350 × 350 pixels.

points of the quantifiers are close to the mean of the sample values which belong to quantization cells. In addition, the spreading parameter $t=\pm 1/\sqrt{\tau}$ permits to limit the statistical effects of the quantization errors on the stego-signals. In the opposite to the QIM, which moves all cell samples to one reconstructed point, the ST-QIM translates the cover-samples but the moving samples do not converge to a particular point, they are scatted thanks to the spreading parameter. Thus, it is possible that many samples' values change but it is very probable that one moving sample takes the place of another one. Globally, the occurrence of each sample value does not change drastically and makes the histogram of the stego-signal very close to the histogram of the cover-signal and enhances the security according to Cachins' criterion. In Erika image on Fig. 7, the effect is more important since the real images has generally a smooth histogram and the pixels are highly correlated. We see that the QIM stego-system makes the image visually very poor (see Fig. 7(b)) since the QIM inserts holes in the histogram stego-signal. Nevertheless, the ST-QIM makes the visual quality of the stego-image, in Fig. 7(d), very close to the original one given by Fig. 7(a) and preserve the histograms of the stego-image as shown in Fig. 7(e). The 1-D (Fig. 5(a)) and 2-D (Fig. 5(b)) relative entropy $D(P_S\|P_X)$ between the probability distribution of the cover and the stego images diverge when the ST is not used. However, when the ST-QIM stego-system is used the difference between the simple (1-D)/joint (2-D) distribution of the cover and stego-image (the relative entropy) is maintained under limit. Note that we compute the 1-D and 2-D k.l.d. by using an estimation of the probability density functions of 100 real images of size 350 × 350 pixels and we limit our study to the simple and joint images probability distribution.

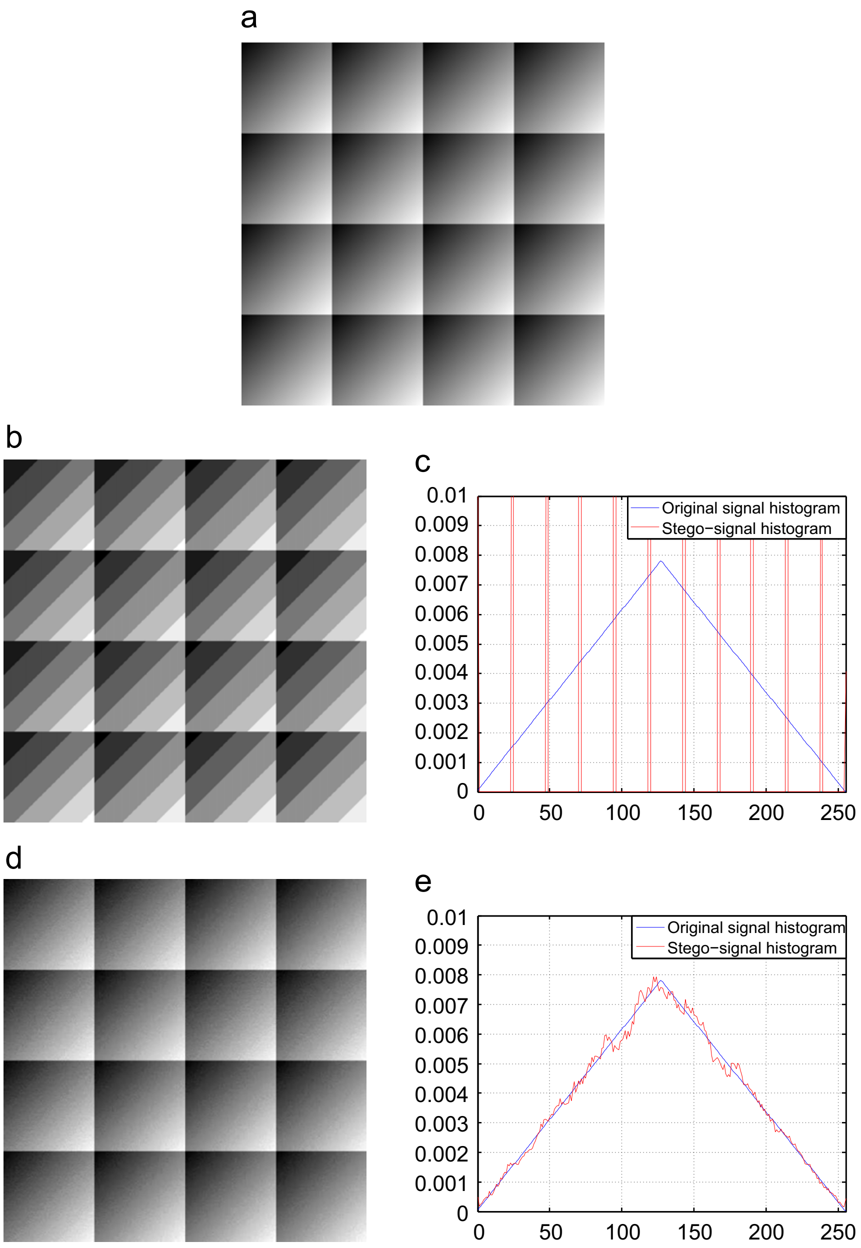

Fig. 6. Stego-message embedding effects on the stego-image. (a) Cover-image, (b) stego-image with QIM, (c) histogram of the cover and stego-image with QIM, (d) stego-image with ST-QIM, (e) histogram of the cover and stego-image with ST-QIM.

This is due to the high computational cost of processing more than joint probability distributions and (as usually) the attacker computation resources are supposed not unlimited.

3.2. Comparison with the blind steganographic scheme of Solanki et al.

In this paragraph, we compare our method to the scheme proposed by Solanki et al. [10]. This approach is based on the statistical restoration principle called histogram-preserving data mapping and can achieve zero KLD. We also show that our method can reach the same interesting property in similar conditions as the Solanki et al. method. In the two approaches the goal is to embed in a JPEG compressed image at a particular quality factor, such that the stego-image is also a JPEG image at the same quality factor. The host image is divided into 8 × 8 non-overlapping blocks and its 2-D DCT is taken. Nineteen AC DCT coefficients are used per block that occur in zigzag scan order. These coefficients are selected if their magnitudes are lower or equal to a given threshold. The payload of the two methods is approximatively the same. Specifically, we have hidden 3106 bits for the Solanki et al. method and 3842 bits for the proposed one with a spreading factor $\tau = 20$. In Fig. 8(a) and (b), the stego-images with the same output quality are shown. In Fig. 8(c), (e) and (f) the histograms of the original image,

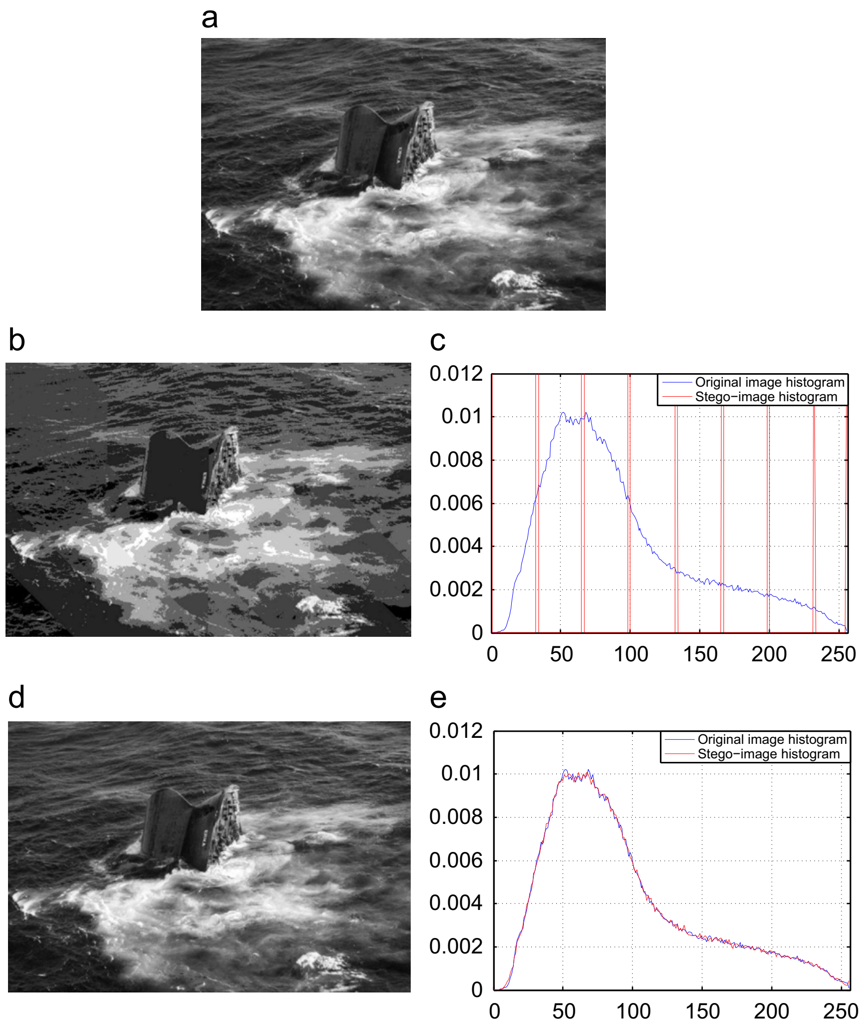

Fig. 7. Stego-message embedding effects on the stego-image. (a) Cover-image (Erika), (b) stego-image with QIM, (c) histogram of the cover and stego-image with QIM (d) stego-image with ST-QIM, (e) histogram of the cover and stego-image with ST-QIM.

the stego-image with the Solanki et al. method and the stego-image with the proposed method are given, respectively. Finally, we can see in Fig. 8(d) that the difference between the original and the stego-histograms is exactly zero for the two methods.

Finally in the context of robust (active) steganography, it makes sense to argue that the proposed method is more robust to the perturbation of the attack since in the proposed method the stego-message is spread in a much larger number of stego-image-symbols. This implies that the ratio between the power of the stego-message over the power of the attack distortion is enhanced by an additive term equal to $10\log_{10}\tau$ [17], or approximatively 13 dB for $\tau = 20$.

4. Conclusion

It is well-known that the quantization based stego-schemes, as the QIM, distort the statistics of stego-signal and are not secure in Cachin's sense. At an intuitive level, we can explained that these systems aggregate the samples values of stego-signal only in the reconstruction points set of the quantifiers. This constitutes a major drawback in the context of secure communications. These methods widely studied in the context of the robust watermarking share several interesting properties. Namely, they are informed (independent of the statistics of the cover-signal), have, in an active context, a high robustness against attacks and can be implemented for real-time applications. So, it is interesting to increase the security of these methods. In this paper, we show that the well-known Spread Transform (ST) associated with the QIM embedding method enhances the stego-message undetectability and thus the security in the sense of Cachin. So, the ST-QIM can be a valuable and flexible solution in the steganographic context. We explain that the message spreading in the ST smoothes the stego-signal probability density function and makes it close to the cover-signal density function. Our theoretical analysis, confirmed by some experiments of real images, allows to identify a tradeoff between the quantization step and the square root of the spreading factor such as the ratio of these two quantities is small.

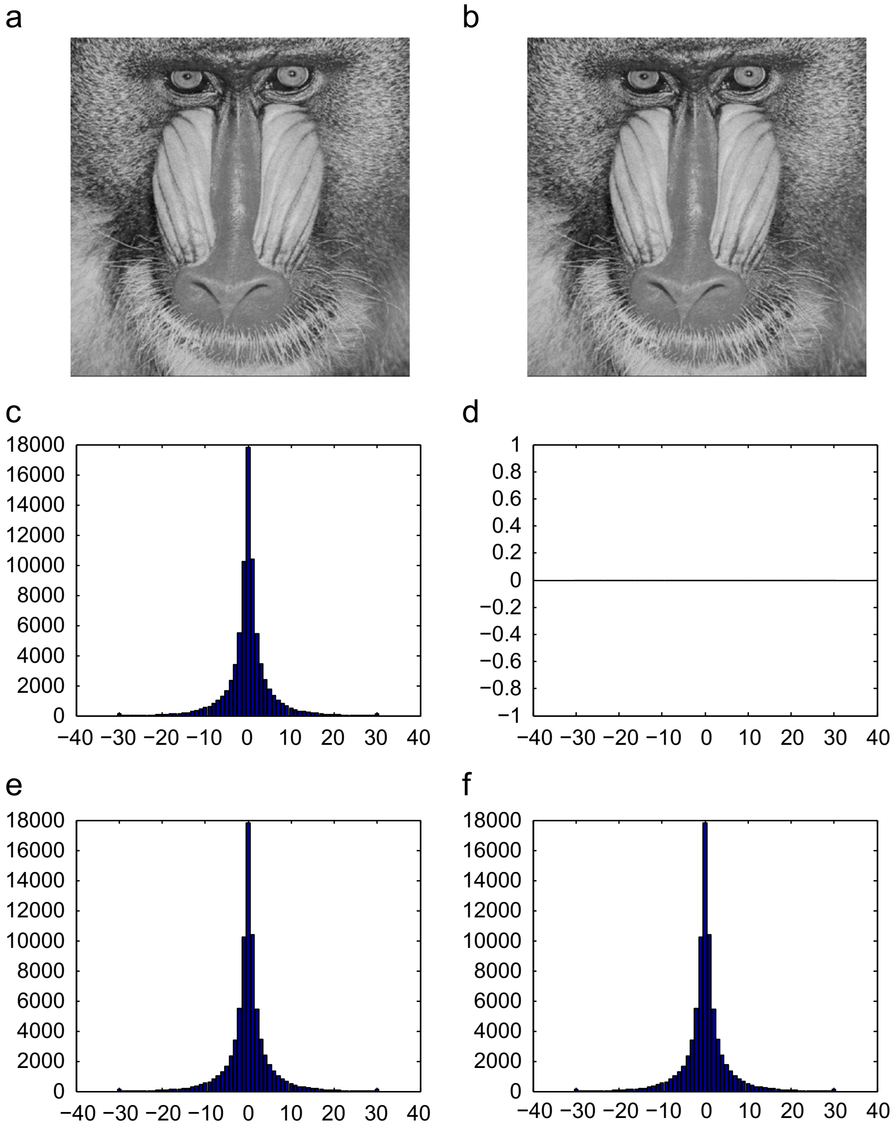

Fig. 8. (a) Stego-image with the Solanki et al. method, (b) Stego-image with the proposed method, (c) histogram of the original image in the DCT domain, (d) differences between the original and the stego-histograms, (e) histogram of the stego-image for the Solanki et al. method, (f) histogram of the stego-image in the DCT domain for the proposed method with $\tau = 20$.

A comparison of the performances of our proposed method is also done with an efficient known steganographic method on real images in the DCT domain. We show that the stego-performances (statistical undetectability) are reached in our case with a finite spreading factor value not so high in similar experimental conditions.

Acknowledgments

The authors would like to thank Professor Pierre Duhamel for his help and collaboration to this paper. The author would like to thank the reviewers and the editor for their valuable comments that led to the improvement of this paper. Also, we thank ESTIVALE and MEDIEVALS projects from ANR (French national agency of research) for funding.

References

[1] F.A.P. Petitcolas, R.J. Anderson, M.G. Kuhn, Information hiding a survey, Proceedings of the IEEE, Special Issue on Protection of Multimedia Content 87 (1999) 1062–1078.

[2] R.J. Anderson, F.A.P. Petitcolas, On the limits of steganography, IEEE Journal of Selected Areas in Communication 16 (1998) 474–481.

[3] Herodotus, The Histories, Penguin books, 1996.

[4] I.J. Cox, M.L. Miller, J.A. Bloom, J. Fridrich, T. Kalker, Digital Watermarking and Steganography, Morgan Kaufmann, 2008.

[5] G.J. Simmons, The Prisonners' Problem and the Subliminal Channel, Plenum Press, 1984, pp. 51–67.

[6] B. Chen, G.W. Wornell, Quantization index modulation: a class of provably good methods for digital watermarking and information embedding, IEEE Transactions on Information Theory 47 (2001) 1423–1443.

[7] S. Pateux, G. Le Guelvouit, Practical watermarking scheme based on wide spread spectrum and game theory, Elsevier Journal on Signal Processing: Image Communication 18 (4) (2003) 283–296.

[8] G. Doërr, J.-L. Dugelay, A guide tour of video watermarking, Elsevier Journal on Signal Processing: Image Communication 18 (4) (2003) 263–282.

[9] P. Moulin, A. Briassouli, A stochastic QIM algorithm for robust, undetectable image watermarking, in: IEEE International Conference on Image Processing, 2004, pp. 1173–1176.

[10] K. Solanki, K. Sullivan, U. Madhow, B.S. Manjunath, S. Chandrasekaran, Provably secure steganography: achieving zero $k-l$ divergence using statistical restoration, in: IEEE International Conference on Image Processing, 2006, pp. 125–128.

[11] J. Fridrich, Steganography in Digital Media, Principles, Algorithms and Applications, Cambridge University Press, 2010.

[12] A. Cheddad, J. Condell, K. Curran, P.M. Kevitt, Digital image steganography: Survey and analysis of current methods, Elsevier, Signal Processing Journal 90 (2010) 727–752.

[13] Y. Wang, P. Moulin, Perfectly secure steganography: capacity, error exponents, and code constructions, IEEE Transactions on Information Theory (2008) 2706–2722.

[14] P. Guillon, T. Furon, P. Duhamel, Applied public-key steganography, Proceedings of the SPIE 3710 (2002) 38–49.

[15] S. Braci, C. Delpha, R. Boyer, G.L. Guelvouit, Informed stego-systems in active warden context: statistical undetectability and capacity, in: IEEE Proceedings of Multimedia Signal Processing, 2008, pp. 707–712.

[16] C. Cachin, An information-theoretic model for steganography, Information Hiding Proceedings, vol. 1525, Springer, 1998, pp. 306–318.

[17] J.J. Eggers, R. Bauml, R. Tzchoppe, B. Girod, Scalar costa scheme for information embedding, IEEE Transactions on Signal Processing 51 (2003) 1003–1019.

[18] T. Cover, J. Thomas, Elements of Information Theory, Wiley, 1991.

[19] O.J. Koval, S. Voloshynovskiy, F. Perez-Gonzalez, F. Deguillaume, T. Pun, Quantization-based watermarking performance improvement using host statistics: Awgn attack case, in: Proceedings of Workshop on Multimedia and Security, 2004, pp. 35–39.

[20] M.H.M. Costa, Writing on dirty paper, IEEE Transactions on Information Theory 29 (1983) 439–441.

[21] S. Kazenbeisser, F. Petitcolas, Information Hiding Techniques for Steganograpy and Digital Watermarking, Artech House, 1999.

[22] G. Le Guelvouit, Trellis-coded quantization for public-key steganography, in: IEEE Conference on Acoustics, Speech and Signal Processing, 2005.

[23] A. Gersho, R.M. Gray, Vector Quantization and Signal Compression, Kluwer Academic Publishers, 1992.

[24] A. Kendall, An Introduction to Numerical Analysis, John Wiley and Sons, 1989.

[25] E.Y. Lam, J.W. Goodman, A mathematical analysis of the DCT coefficient distributions for images, IEEE Transactions on Image Processing 9 (2000) 1661–1666.

[26] W.K. Pratt, Digital Image Processing, Wiley, 1978.