Hindawi Publishing Corporation
Journal of Electrical and Computer Engineering
Volume 2016, Article ID 9029745, 16 pages
http://dx.doi.org/10.1155/2016/9029745

Research Article

A New Scalar Quantization Method for Digital Image Watermarking

Yevhen Zolotavkin and Martti Juhola

Computer Science, School of Information Sciences, University of Tampere, Kanslerinrinne 1, 33014 Tampere, Finland

Correspondence should be addressed to Yevhen Zolotavkin; zhzolot@countermail.com

Received 7 October 2015; Revised 18 January 2016; Accepted 24 January 2016

Academic Editor: Mazdak Zamani

A new technique utilizing Scalar Quantization is designed in this paper in order to be used for Digital Image Watermarking (DIW). Efficiency of the technique is measured in terms of distortions of the original image and robustness under different kinds of attacks, with particular focus on Additive White Gaussian Noise (AWGN) and Gain Attack (GA). The proposed technique performance is affirmed by comparing with state-of-the-art methods including Quantization Index Modulation (QIM), Distortion Compensated QIM (DC-QIM), and Rational Dither Modulation (RDM). Considerable improvements demonstrated by the method are due to a new form of distribution of quantized samples and a procedure that recovers a watermark after GA. In contrast to other known quantization methods, the detailed method here stipulates asymmetric distribution of quantized samples. This creates a distinctive feature and is expressed numerically by one of the proposed criteria. In addition, several realizations of quantization are considered and explained using a concept of Initial Data Loss (IDL) which helps to reduce watermarking distortions. The procedure for GA recovery exploits one of the two criteria of asymmetry. The accomplishments of the procedure are due to its simplicity, computational lightness, and sufficient precision of estimation of unknown gain factor.

1. Introduction

In modern communications, multimedia plays significant role. Ownership of multimedia data is important and needs to be protected [1]. As a part of nowadays popular multimedia content, digital images are an important class. A protection of digital rights of an owner is implemented by Digital Image Watermarking (DIW). A watermark that is inserted into an image has to be robust [2] as well as invisible [3].

Among the popular and efficient techniques in DIW, Quantization Index Modulation (QIM) is widely used in blind watermarking where neither original media nor watermark is known to the receiver [4, 5]. One of the aspects of robustness of QIM is evaluated by attacking a watermarked image with Additive White Gaussian Noise (AWGN). Unfortunately, all the known on practice implementations of QIM are far from achieving the channel capacity limit that was first derived in [6].

Several different QIM-related approaches are known. Some state-of-the-art realizations will be outlined briefly. According to QIM, intervals of equal length Δ are mapped on the real number line. The oldest known approach is to replace all the original coefficients inside every interval with one of the two endpoints of that interval. The selection of the endpoint depends on a bit of a watermark [7]. The main disadvantage is that for high intensity of noise and the capacity of the oldest QIM is much lower than the theoretical limit. In a more advanced realization of DC-QIM, coefficients from every original interval are mapped into two disjoint subintervals. The gap between the subintervals is controlled by parameter α, $0 \leq \alpha \leq 1$ [8]. Assuming that initial distribution inside original interval and target distributions in subintervals are uniform, the mapping in accordance to DC-QIM is optimal in terms of Mean Square Error (MSE) of quantization. In order to maximize capacity for a given MSE under AWGN of different intensity, parameters Δ, α have to be adjusted. Nevertheless, the limit defined in [6] is still well above the one achievable by DC-QIM.

Not all the original coefficients in each interval need to be quantized. This idea has been explored by the authors of Forbidden Zone Data Hiding (FZDH) [9]. Another idea was proposed by the authors of Thresholded Constellation

Modulation (TCM) that uses two different quantization rules to modify coefficients inside the original interval [10].

Despite sufficient robustness of QIM under AWGN, the limitation is that synchronization is required in order to reconstruct intervals that are necessary to extract (or decode) a watermark. A type of distortion which scales all the watermarked coefficients is called Gain Attack (GA). The scaling factor might be close to 1 and cause very little visual distortion, but it is unknown to the receiver which causes asynchronous extraction. Retrieval of the watermark is usually complicated by AWGN that follows GA [11].

Improvement of QIM performance under GA is the task of numerous known approaches [12]. Most of them can be classified into two groups where the main idea of the first group is to estimate the unknown factor [13] while the idea of the second is to quantize coefficients of a different kind that are invariant to scaling of original signal.

The solution proposed in [11] contributes to robustness enhancement in case of GA and a constant offset attack followed by AWGN. A pilot signal is embedded for this purpose. Fourier analysis is used during extraction to estimate the gain factor and the offset. Another method of recovery after GA and AWGN is proposed in [14]. It uses information about dither sequence and applies Maximum Likelihood (ML) procedure to estimate the scaling factor.

Watermarking that is invariant to GA demands more complex transform of original signal (e.g., nonlinear) to obtain coefficients. One of the most popular watermarking methods in that category is Rational Dither Modulation (RDM) [15]. For a particular coefficient, a ratio that depends on a norm of other coefficients is being quantized instead of a coefficient itself. In order to quantize the ratio, RDM utilizes the simplest QIM scheme. This implies that the performance of RDM under AWGN (without GA) is close to the simplest QIM. Among others recent blind watermarking methods robust to GA are, for example, detailed in [16–18].

A new scalar QIM-based watermarking method is proposed in this paper. It provides high robustness under conditions of AWGN and GA. Among the new features of the method are IDL and a new form of distribution of quantized samples.

The organization of the rest of the paper is as follows. Section 2 explains the choice of the distribution of quantized samples and contains description of the procedure of recovery after GA. Concept of IDL and quantization model are described in Section 3 using formal logic approach. The aspects of analytic-based estimation of robustness under AWGN are discussed in Section 4. Next, Section 5 contains experimental results obtained under AWGN and GA. Discussion of the details of the experiment and comparison of the performance are given in Section 6. Section 7 concludes the paper. The list of the key variables and their meaning is given in Nomenclature section.

2. Distribution of Quantized Samples and Procedure for Recovery after GA

An asymmetric distribution of quantized samples is proposed and parametrized in this section. Asymmetry is the quality that can be easily expressed quantitatively. Under symmetric attack, like AWGN, such quantitative index remains sufficiently indicative. On the other hand, it can be affected by GA. Such semifragility is favorable for restoration of the right condition for decoding. The restoration is done by the procedure for recovery after GA which uses criterion of asymmetry. Compared to the known estimation procedures [14], the one proposed in this section depends on a single variable which is the unknown gain factor. This makes the technique simple and more precise.

For encoding, in our case, asymmetric distribution requires substantially more variables for description compared to common QIM methods. Because of that, it is advisable to refer to Nomenclature section.

2.1. Distribution of Quantized Samples. Symbol Σ will be used to denote a random variable whose domain is the space of original coefficients of a host. A particular realization of Σ will be denoted as ς. We will further consider manipulation of original values ς that are in some kth interval of size Δ and its left endpoint is l_Δ^k. Such an interval is referred further as embedding interval. For any $\varsigma \in [l_\Delta^k, l_\Delta^k + \Delta]$ we define $x = \varsigma - l_\Delta^k$ and X will be used to denote a random variable which represents x. The value of Δ should be small enough so that the distribution of X can be considered uniform. A random variable that represents quantized coefficients inside kth interval is denoted as X' and its realization is denoted as x'. Each pair of an original x and corresponding quantized x' belongs to the same kth embedding interval so that an absolute shift is never larger than Δ. Correspondingly, a random variable that represents quantized coefficients on the whole real number line is denoted as Σ' and its realization is denoted as ς'.

In order to provide efficient recovery after GA, we propose the following asymmetric distribution of quantized samples x' inside kth embedding interval (Figure 1(a)):

$$f(x') = \begin{cases} (\gamma_0 + \eta_1) f_0(x'), & \text{if } x' \in [0, \Delta(\beta - \alpha)], \\ (\varphi_1 + \vartheta_0) f_1(x'), & \text{if } x' \in [\Delta\beta, \Delta], \\ 0, & \text{otherwise}, \end{cases} \quad (1)$$

where $f_0(x')$ and $f_1(x')$ are two different kinds of truncated distributions defined as

$$f_0(x') = \begin{cases} cx' + \tau, & \text{if } x' \in [0, \Delta(\beta - \alpha)], \\ 0, & \text{otherwise}, \end{cases} \quad (2)$$

$$f_1(x') = \begin{cases} g, & \text{if } x' \in [\Delta\beta, \Delta], \\ 0, & \text{otherwise}. \end{cases} \quad (3)$$

The other parameters are constrained in the following way: $0 \le \alpha \le \beta \le 1$, $\gamma_0 + \vartheta_0 + \varphi_1 + \eta_1 = 1$ (see Nomenclature section). The meaning of parameters $\gamma_0, \vartheta_0, \varphi_1, \eta_1$ will be discussed later in Section 3. In Figure 1(b) we can see the distribution of the quantized coefficients outside kth embedding interval as well.

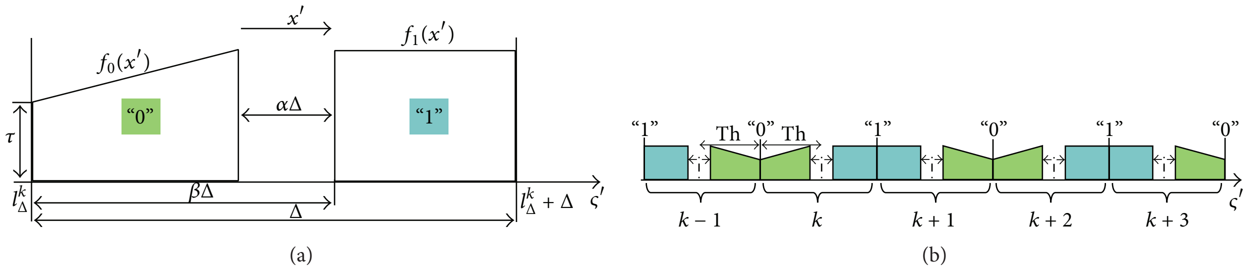


Figure 1: Distribution of the quantized coefficients: (a) Inside kth embedding interval. (b) In five consecutive intervals.

2.2. Procedure for GA Recovery. It is assumed that under GA the original length of embedding interval Δ is altered by unknown gain factor λ and the resulting length is $\widetilde{\Delta} = \lambda\Delta$. In addition to that, AWGN attack is applied. The procedure for GA recovery is the estimator whose result is based on a criterion having higher values for the right length $\widetilde{\Delta}$ of embedding interval. The uniqueness of the distribution of quantized samples is exploited by two different criteria C_1 and C_2. The procedure itself represents a brute force approach that substitutes guessed values $\widetilde{\Delta}'$ of the length of embedding interval into a criterion. Guessed value of $\widetilde{\Delta}'$ which maximizes it (C_1 or C_2) should be selected:

$$\widetilde{\Delta}'' = \arg\max_{\{\widetilde{\Delta}'\}} C_{1,2}\left(\widetilde{\Delta}'\right), \tag{4}$$

where $\widetilde{\Delta}''$ is the final output of the procedure. Some interval $[\widetilde{\Delta}'_{\min}, \widetilde{\Delta}'_{\max}]$ for guessed values $\widetilde{\Delta}'$ should be defined in advance. For instance, $\widetilde{\Delta}'_{\min} = 0.9\Delta$ and $\widetilde{\Delta}'_{\max} = 1.1\Delta$ works well in most cases because the diapason of scaling factor λ is quite limited on practice.

For each particular value $\widetilde{\Delta}'$, the index defined according to the criterion is calculated by projecting noisy quantized samples ς'_n on a single embedding interval:

$$x'_n = \begin{cases} \varsigma'_n \bmod \widetilde{\Delta}', & \text{if } \left\lfloor \dfrac{\varsigma'_n - l_\Delta^k}{\widetilde{\Delta}'} \right\rfloor \bmod 2 = 0, \\ \widetilde{\Delta}' - \left(\varsigma'_n \bmod \widetilde{\Delta}'\right), & \text{otherwise.} \end{cases} \tag{5}$$

This is needed to reconstruct the distribution of quantized samples inside embedding interval.

Two criteria are proposed for the assessment of the distribution of random variable $X'_n \in [0, \widetilde{\Delta}']$ (subscript "n" means affected by noise):

$$\begin{aligned} C_1\left(\widetilde{\Delta}'\right) &= \left| \frac{\operatorname{median}\left(X'_n\right)}{\widetilde{\Delta}'} - 0.5 \right|, \\ C_2\left(\widetilde{\Delta}'\right) &= \left| \frac{\mu_w\left(X'_n\right)}{\left(\widetilde{\Delta}'\right)^w} \right|, \quad w = 2m+1, \ m \in \mathbb{N}. \end{aligned} \tag{6}$$

Here, μ_w is the wth central moment. Odd moments are zero for symmetric distributions, but for asymmetric distributions their values can be sufficiently large. If the assumption about $\widetilde{\Delta}$ is wrong, then the values of both criteria are low. In that case the distribution of X'_n is very close to uniform (which is symmetric). This is because of the effect caused by GA on calculation of x'_n in (5). Nevertheless, the distribution of X'_n demonstrates asymmetry in case $\widetilde{\Delta}'$ is close to $\widetilde{\Delta}$. The explanation is that the distribution of quantized samples inside embedding interval (before GA is introduced) is indeed asymmetric. In spite of utilization of brute force optimization, the procedure is simple and the computational demand is low. On practice, the number of brute force steps is much smaller than the number of quantized elements. Therefore, the complexity is $O(n)$ in that case. For instance, for recovery with high accuracy it is enough to perform 10^3 brute force steps with values from the interval $[\widetilde{\Delta}'_{\min}, \widetilde{\Delta}'_{\max}]$.

3. Quantization

A quantization model is introduced in this section. In order to represent it in a compact form, we combine all the quantization conditions in a single logical expression. Previously proposed distribution of quantized samples is assured. However, additional parameter of the quantization model implies different distribution of the samples associated with labels "0" and "1."

3.1. Two Approaches for Quantization. Quantized samples are modified according to the model described in this subsection. A watermark bit is denoted as b. Each sample with value x inside kth embedding interval has index $i \in \mathbb{N}$ according to its order in the host sequence. During watermarking a bit is assigned to each index i. Different frameworks might be used for description of the quantization model. We will use first order predicate logic to describe our approach. This choice can be reasoned as follows. A closed-from expression has to be defined for quantization and it is important to show that the derived solution minimizes MSE between initial and target distribution. The kind of proposed target distribution is not common for QIM-based watermarking methods. Therefore, we find it necessary to explain in detail the process of derivation of quantization expression. Also, samples interpreting "0" should be quantized in a different way to samples interpreting "1." Predicate logic is a suitable

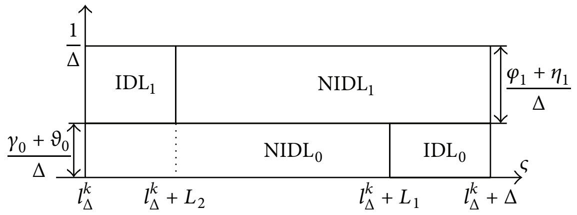


FIGURE 2: Scheme of labeling and distribution of original samples prior to quantization.

tool for description of embedding because logical construction can incorporate all the possible quantization conditions in a compact form.

Two-place predicate E is to denote correspondence between some index and the value of coefficient. For example, Eix is true if a coefficient with order i has value x. We will further use notation of the set $\mathbf{E}$ which contains all the pairs (x, i) that provide true value of Eix. One-place predicate B is to denote bit value assigned to a coefficient with particular index. For instance, Bi is true if watermark bit $b = 1$ is assigned to a coefficient with index i and $\sim Bi$ is true if $b = 0$. Two-place predicates X_0 or X_1 will be used to define that some ith sample with value x has label "0" or "1," respectively:

$$\left(X_0 ix \equiv (Eix \& \sim Bi)\right), \quad (\forall i)(\forall x), \tag{7}$$

$$\left(X_1 ix \equiv (Eix \& Bi)\right), \quad (\forall i)(\forall x). \tag{8}$$

Sets $\mathbf{X}_0$ and $\mathbf{X}_1$ contain all the pairs (x, i) that provide true values of $X_0 ix$ and $X_1 ix$, respectively. Initial PDFs of X inside $\mathbf{X}_0$, $\mathbf{X}_1$, and $\mathbf{E}$ are considered to be uniform: $f_{\mathbf{X}_0}(x) = f_{\mathbf{X}_1}(x) = f_{\mathbf{E}}(x) = 1/\Delta$ (Figure 2).

Also, each coefficient is labeled either as IDL or non-IDL depending on its value x and index i. Samples labeled as IDL are quantized in a different way which reduces the total embedding distortion. Both types of coefficients (IDL and non-IDL) are being modified during quantization. However, after quantization, interpretation of a bit of each IDL coefficient is incorrect. The purpose of quantization is to provide that all the non-IDL samples can be extracted correctly and the resulting distribution of all the samples is the one depicted in Figure 1(a). Parameters η_1 and ϑ_0 represent fractions of IDL for $b = 1$ and $b = 0$, respectively. Parameters φ_1 and γ_0 represent fractions of non-IDL samples for $b = 1$ and $b = 0$, respectively. The fraction of zeros in a watermark data is $\gamma_0 + \vartheta_0$ and fraction of ones is $\varphi_1 + \eta_1$. It is required that $\gamma_0 + \vartheta_0 + \varphi_1 + \eta_1 = 1$.

We define IDL and non-IDL samples using two-place predicates IDL$_0$, IDL$_1$, NIDL$_0$, and NIDL$_1$ in the following way (Figure 2):

$$\begin{gathered}
\left(\mathrm{IDL}_0 ix \equiv \left(X_0 ix \& \left(x > L_1\right)\right)\right), \quad (\forall i)(\forall x), \\
\left(\mathrm{IDL}_1 ix \equiv \left(X_1 ix \& \left(x < L_2\right)\right)\right), \quad (\forall i)(\forall x), \\
\left(\mathrm{NIDL}_0 ix \equiv \left(X_0 ix \& \left(x \leq L_1\right)\right)\right), \quad (\forall i)(\forall x), \\
\left(\mathrm{NIDL}_1 ix \equiv \left(X_1 ix \& \left(x \geq L_2\right)\right)\right), \quad (\forall i)(\forall x),
\end{gathered} \tag{9}$$

where $L_1 = \Delta\gamma_0/(\gamma_0 + \vartheta_0)$, $L_2 = \Delta\eta_1/(\varphi_1 + \eta_1)$, and $L_1 \geq L_2$.

Sets $\mathbf{IDL}_0$, $\mathbf{IDL}_1$, $\mathbf{NIDL}_0$, and $\mathbf{NIDL}_1$ will be used in order to specify all the coefficients that satisfy IDL$_0$, IDL$_1$, NIDL$_0$, and NIDL$_1$, respectively. Fractions γ_0, ϑ_0, φ_1, and η_1 can be expressed in terms of cardinalities of sets $\mathbf{IDL}_0$, $\mathbf{IDL}_1$, $\mathbf{NIDL}_0$, $\mathbf{NIDL}_1$, and $\mathbf{E}$. For example, $|\mathbf{IDL}_0|/|\mathbf{E}| = \vartheta_0$.

In this paper, two different quantization techniques are proposed. Since predicate logic is used to describe watermark embedding, a suitable logical construction should be able to distinguish between the techniques. According to our model, each kind of quantization can be represented by setting a corresponding logical value ("0" or "1") for zero-place predicate Ω. Hence, Ω is used to define one out of two possible quantization techniques. For each kind of quantization, $\mathbf{E}$ is split on two subsets $\mathbf{E}_0$ and $\mathbf{E}_1$. For two-place predicates E_0 and E_1 formulas $E_0 ix$ and $E_1 ix$ are defined in the following way:

$$\begin{aligned}
&\left(E_0 ix\right. \\
&\quad \left.\equiv \left(\mathrm{NIDL}_0 ix \vee \left(\mathrm{IDL}_1 ix \& \Omega\right) \vee \left(\mathrm{IDL}_0 ix \& \sim \Omega\right)\right)\right), \\
&\qquad (\forall i)(\forall x),
\end{aligned} \tag{10}$$

$$\left(E_1 ix \equiv \left(Eix \& \sim E_0 ix\right)\right), \quad (\forall i)(\forall x). \tag{11}$$

Using information about distribution inside $\mathbf{IDL}_0$, $\mathbf{IDL}_1$, $\mathbf{NIDL}_0$, and $\mathbf{NIDL}_1$ it is easy to derive distribution inside $\mathbf{E}_0$ and $\mathbf{E}_1$. Let us introduce variable $\omega \in \{0, 1\}$ of natural numbers domain $\mathbb{N}$ (not a logical variable) which satisfies $(\Omega \supset (\omega = 1)) \& (\sim \Omega \supset (\omega = 0))$. Common arithmetical operations can be performed with ω which makes it possible to express PDF $f_{\mathbf{E}_0}(x)$ in the following compact form:

$$f_{\mathbf{E}_0}(x) = \begin{cases} \dfrac{\left(\gamma_0 + \vartheta_0\right) f_{\mathbf{X}_0}(x) + \omega\left(\varphi_1 + \eta_1\right) f_{\mathbf{X}_1}(x)}{DN_0}, & \text{if } x \leq L_2, \\ \dfrac{\left(\gamma_0 + \vartheta_0\right) f_{\mathbf{X}_0}(x)}{DN_0}, & \text{if } L_2 < x \leq L_1, \\ \dfrac{(1 - \omega)\left(\gamma_0 + \vartheta_0\right) f_{\mathbf{X}_0}(x)}{DN_0}, & \text{otherwise,} \end{cases} \tag{12}$$

where $DN_0 = (\omega\eta_1 + \gamma_0 + (1 - \omega)\vartheta_0)$.

Therefore $f_{\mathbf{E}_1}(x)$ can be expressed as (Figures 3 and 4)

$$f_{\mathbf{E}_1}(x) = \frac{f_{\mathbf{E}}(x) - DN_0 f_{\mathbf{E}_0}(x)}{1 - DN_0}. \tag{13}$$

Elements of sets $\mathbf{E}_0$ and $\mathbf{E}_1$ are modified during quantization so that new sets $\mathbf{E}_0'$ and $\mathbf{E}_1'$ are obtained, respectively.

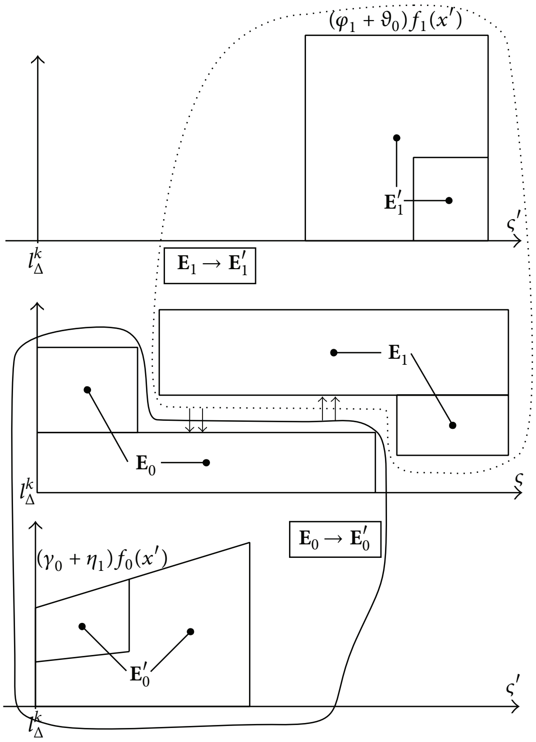

$(\varphi_1+\vartheta_0)f_1(x')$
$\mathbf{E}_1'$
ς'
l_Δ^k
$\mathbf{E}_1 \rightarrow \mathbf{E}_1'$
$\mathbf{E}_1$
$\mathbf{E}_0$
l_Δ^k
ς
$\mathbf{E}_0 \rightarrow \mathbf{E}_0'$
$(\gamma_0+\eta_1)f_0(x')$
$\mathbf{E}_0'$
ς'
l_Δ^k

Figure 3: Scheme of redistribution of original samples during quantization, Ω is "true."

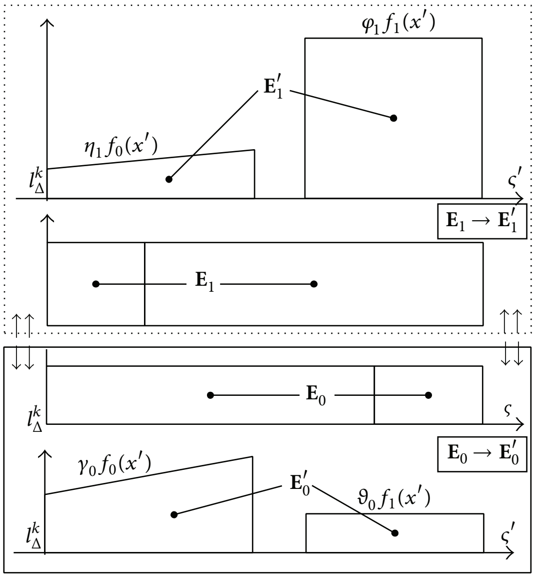


Figure 4: Scheme of redistribution of original samples during quantization, Ω is "false."

Therefore, for successful quantization, we require the following formula $F1$ to be true:

$$F1 \equiv \left(\left(E_0 ix \supset E_0' ix'\right) \& \left(E_1 ix \supset E_1' ix'\right)\right), \quad (\forall i)\,(\forall x)\,\left(\exists x'\right). \tag{14}$$

As a result of quantization, variables $X_{\mathbf{E}_0}$ and $X_{\mathbf{E}_1}$ are modified in a way that the resulting $X'_{\mathbf{E}_0'}$ and $X'_{\mathbf{E}_1'}$ are distributed according to some desired distributions. For each kind of quantization (depending on the value of Ω), the pair of desired distributions is different. We propose the following distributions that can be expressed as (Figures 3 and 4)

$$f_{\mathbf{E}_0'}\left(x'\right) = \omega f_0\left(x'\right) + (1-\omega)\frac{\gamma_0 f_0\left(x'\right) + \vartheta_0 f_1\left(x'\right)}{\gamma_0 + \vartheta_0},$$
$$f_{\mathbf{E}_1'}\left(x'\right) = \omega f_1\left(x'\right) + (1-\omega)\frac{\eta_1 f_0\left(x'\right) + \varphi_1 f_1\left(x'\right)}{\varphi_1 + \eta_1}. \tag{15}$$

It can be seen that, for any logical value of Ω, the distribution of X' inside $\{\mathbf{E}_0 \cup \mathbf{E}_1\}$ is the same and matches the distribution represented in Figure 1. It means that the efficiency of the procedure of GA recovery (proposed in the previous section) cannot be affected by the selection of Ω.

In addition to the necessity of providing desired distribution of the quantized samples, we need to minimize quantization distortions. Both requirements can be expressed by two two-place predicates U and V:

$$\left(E_0'ix' \equiv E_0ix\&Uxx'\right), \quad (\forall i)(\forall x)\left(\forall x'\right),$$
$$\left(E_1'ix' \equiv E_1ix\&Vxx'\right), \quad (\forall i)(\forall x)\left(\forall x'\right). \tag{16}$$

The idea of minimization of embedding distortions can be explained in the following example. Assuming two samples $x_i, x_j \in \mathbf{E}_0$, $x_i \le x_j$, we infer that quantization in a way in which $x_i' \le x_j'$ implies less distortion than in case when $x_i' > x_j'$. Let us sort elements in $\mathbf{E}_0$ and $\mathbf{E}_0'$ in the dimension of x and x', respectively. Then, for some x_i (index i is an order in a host sequence) the number of elements in $\mathbf{E}_0$ with x value less than x_i should be equal to the number of elements in $\mathbf{E}_0'$ that have x' value less than x_i'. Integration should be used in case we switch from discrete distribution of samples in $\mathbf{E}_0$ and $\mathbf{E}_0'$ to continuous one. Further, throughout the paper we assume that the constant of integration is zero for indefinite integrals. Hence, the truth values for both predicates U and V are defined as

$$\left(Uxx' \equiv \left(\int f_{\mathbf{E}_0}(x)\,dx = \int f_{\mathbf{E}_0'}\left(x'\right)dx'\right)\right),$$
$$(\forall x)\left(\forall x'\right), \tag{17}$$

$$\left(Vxx' \equiv \left(\int f_{\mathbf{E}_1}(x)\,dx = \int f_{\mathbf{E}_1'}\left(x'\right)dx'\right)\right),$$
$$(\forall x)\left(\forall x'\right). \tag{18}$$

Further, we introduce logical formula $F2$

$$F2 \equiv \left(\left(\exists x'\right)Uxx'\&\left(\exists x'\right)Vxx'\right), \quad (\forall x) \tag{19}$$

and state that argument

$$F2, (11), (16) \vDash F1 \tag{20}$$

is valid. The task of watermark embedding is to assure that the mentioned argument is sound. For that purpose, a procedure that makes $F2$ true should be proposed.

3.2. Quantization Equations. Quantization equations and their solutions are needed to satisfy formula $F2$ during embedding. For this purpose, we will analyze conditions that enforce qualities of predicates U and V. Due to the large number of variables in the text we recommend to refer to Nomenclature section for clarity. We can rewrite elements of (17) in the following way:

$$\int f_{\mathbf{E}_0}(x)\,dx = \begin{cases} \dfrac{\min\left(x, L_2\right)\omega\left(\varphi_1+\eta_1\right) + x\left(\gamma_0+\vartheta_0\right)}{\Delta DN_0}, & \text{if } x \le L_1; \\ \omega + \dfrac{(1-\omega)\,x\left(\gamma_0+\vartheta_0\right)}{\Delta DN_0}, & \text{otherwise,} \end{cases}$$
$$\int f_{\mathbf{E}_0'}\left(x'\right)dx' = \begin{cases} \left(\omega + \gamma_0\dfrac{1-\omega}{\gamma_0+\vartheta_0}\right)\displaystyle\int f_0\left(x'\right)dx', & \text{if } x' \le \Delta\beta; \\ \left(\omega + \gamma_0\dfrac{1-\omega}{\gamma_0+\vartheta_0}\right) + \vartheta_0\dfrac{1-\omega}{\gamma_0+\vartheta_0}\left(\displaystyle\int f_1\left(x'\right)dx' + \int_{\Delta\beta}^{0} f_1\left(x'\right)dx'\right), & \text{otherwise.} \end{cases} \tag{21}$$

From (21) it is clear that

$$\int_0^{L_1} f_{\mathbf{E}_0}(x)\,dx = \int_0^{\Delta(\beta-\alpha)} f_{\mathbf{E}_0'}\left(x'\right)dx'$$
$$= \omega + \gamma_0\frac{1-\omega}{\gamma_0+\vartheta_0}. \tag{22}$$

The equation above means that the following is true:

$$\left(Uxx' \supset \left(\left(\left(x \le L_1\right)\&\left(x' \le \Delta\beta\right)\right)\right.\right.$$
$$\left.\left.\vee\left(\left(x > L_1\right)\&\left(x' > \Delta\beta\right)\right)\right)\right), \quad (\forall x)\left(\forall x'\right). \tag{23}$$

We introduce two two-place predicates U^1 and U^2:

$$\left(\left(\left(Uxx'\&\left(x \le L_1\right)\&\left(x' \le \Delta\beta\right)\right) \equiv U^1xx'\right)\right.$$
$$\left.\&\left(\left(Uxx'\&\left(x > L_1\right)\&\left(x' > \Delta\beta\right)\right) \equiv U^2xx'\right)\right),$$
$$(\forall x)\left(\forall x'\right). \tag{24}$$

According to (21) and (24) the following can be derived:

$$\left(U^1xx' \equiv \left(\Upsilon_1\left(x, \omega, \gamma_0, \vartheta_0, \varphi_1, \eta_1\right) = 0.5cx'^2 + \tau x'\right)\right),$$

$$
\begin{aligned}
&(\forall x)\left(\forall x'\right),\\
&\left(U^2xx' \equiv \left(\Upsilon_2\left(x,\omega,\gamma_0,\vartheta_0,\varphi_1,\eta_1\right) = g\left(x'-\Delta\beta\right)\right)\right),\\
&(\forall x)\left(\forall x'\right),
\end{aligned}
\tag{25}
$$

where

$$
\begin{aligned}
&\Upsilon_1\left(x,\omega,\gamma_0,\vartheta_0,\varphi_1,\eta_1\right)\\
&= \left(\gamma_0+\vartheta_0\right)\frac{\min\left(x,L_2\right)\omega\left(\varphi_1+\eta_1\right)+x\left(\gamma_0+\vartheta_0\right)}{\Delta DN_0\left(\gamma_0+\omega\vartheta_0\right)},\\
&\Upsilon_2\left(x,\omega,\gamma_0,\vartheta_0,\varphi_1,\eta_1\right) = \frac{x\left(\gamma_0+\vartheta_0\right)^2-\gamma_0\Delta DN_0}{\vartheta_0\Delta DN_0}.
\end{aligned}
\tag{26}
$$

Now, let us analyze conditions that enforce quality of predicate V. Elements of (18) can be represented as

$$
\begin{aligned}
&\int f_{\mathbf{E}_1}(x)\,dx = \begin{cases} \dfrac{(1-\omega)x\left(\varphi_1+\eta_1\right)}{\Delta\left(1-DN_0\right)}, & \text{if } x \le L_2;\\ \dfrac{\max\left(x-L_1,0\right)\omega\left(\gamma_0+\vartheta_0\right)+\left(x-L_2\right)\left(\varphi_1+\eta_1\right)}{\Delta\left(1-DN_0\right)}, & \text{otherwise,}\end{cases}\\
&\int f_{\mathbf{E}_1'}\left(x'\right)dx' = \begin{cases} \dfrac{(1-\omega)\eta_1}{\varphi_1+\eta_1}\displaystyle\int f_0\left(x'\right)dx', & \text{if } x' \le \Delta\beta;\\ \dfrac{(1-\omega)\eta_1}{\varphi_1+\eta_1}+\left(\omega+\varphi_1\dfrac{1-\omega}{\varphi_1+\eta_1}\right)\left(\displaystyle\int f_1\left(x'\right)dx'+\int_{\Delta\beta}^{0} f_1\left(x'\right)dx'\right), & \text{otherwise.}\end{cases}
\end{aligned}
\tag{27}
$$

We can see that according to (25)

$$
\int_0^{L_2} f_{\mathbf{E}_1}(x)\,dx = \int_0^{\Delta(\beta-\alpha)} f_{\mathbf{E}_1'}\left(x'\right)dx' = \frac{(1-\omega)\eta_1}{\varphi_1+\eta_1}. \tag{28}
$$

This means that the following expression is true:

$$
\begin{aligned}
&\left(Vxx' \supset \left(\left(\left(x \le L_2\right)\&\left(x' \le \Delta\beta\right)\right)\right.\right.\\
&\quad\left.\left.\vee\left(\left(x > L_2\right)\&\left(x' > \Delta\beta\right)\right)\right)\right),\quad (\forall x)\left(\forall x'\right).
\end{aligned}
\tag{29}
$$

Next, two two-place predicates V^1 and V^2 are defined as

$$
\begin{aligned}
&\left(\left(\left(Vxx'\&\left(x \le L_2\right)\&\left(x' \le \Delta\beta\right)\right) \equiv V^1xx'\right)\right.\\
&\left.\&\left(\left(Vxx'\&\left(x > L_2\right)\&\left(x' > \Delta\beta\right)\right) \equiv V^2xx'\right)\right),\\
&(\forall x)\left(\forall x'\right).
\end{aligned}
\tag{30}
$$

According to (27) and (30) the following can be derived:

$$
\begin{aligned}
&\left(V^1xx' \equiv \left(\Upsilon_3\left(x,\omega,\gamma_0,\vartheta_0,\varphi_1,\eta_1\right) = 0.5cx'^2+\tau x'\right)\right),\\
&(\forall x)\left(\forall x'\right),\\
&\left(V^2xx' \equiv \left(\Upsilon_4\left(x,\omega,\gamma_0,\vartheta_0,\varphi_1,\eta_1\right) = g\left(x'-\Delta\beta\right)\right)\right),\\
&(\forall x)\left(\forall x'\right),
\end{aligned}
\tag{31}
$$

where

$$
\begin{aligned}
&\Upsilon_3\left(x,\omega,\gamma_0,\vartheta_0,\varphi_1,\eta_1\right) = \frac{x\left(\varphi_1+\eta_1\right)^2}{\eta_1\Delta\left(1-DN_0\right)},\\
&\Upsilon_4\left(x,\omega,\gamma_0,\vartheta_0,\varphi_1,\eta_1\right) = \frac{\left(\varphi_1+\eta_1\right)\left(\max\left(x-L_1,0\right)\omega\left(\gamma_0+\vartheta_0\right)+\left(x-L_2\right)\left(\varphi_1+\eta_1\right)\right)-\Delta\left(1-DN_0\right)(1-\omega)\eta_1}{\Delta\left(1-DN_0\right)\left(\varphi_1+\omega\eta_1\right)}.
\end{aligned}
\tag{32}
$$

We can express U using U^1 and U^2 in the following way:

$$
\begin{aligned}
&\left(Uxx'\right.\\
&\quad\left.\equiv\left(\left(\left(x \le L_1\right)\supset U^1xx'\right)\&\left(\left(x > L_1\right)\supset U^2xx'\right)\right)\right),\\
&\quad(\forall x)\left(\forall x'\right).
\end{aligned}
\tag{33}
$$

Also, we can express V using V^1 and V^2:

$$
\begin{aligned}
&\left(Vxx'\right.\\
&\quad\left.\equiv\left(\left(\left(x \le L_2\right)\supset V^1xx'\right)\&\left(\left(x > L_2\right)\supset V^2xx'\right)\right)\right),\\
&\quad(\forall x)\left(\forall x'\right).
\end{aligned}
\tag{34}
$$

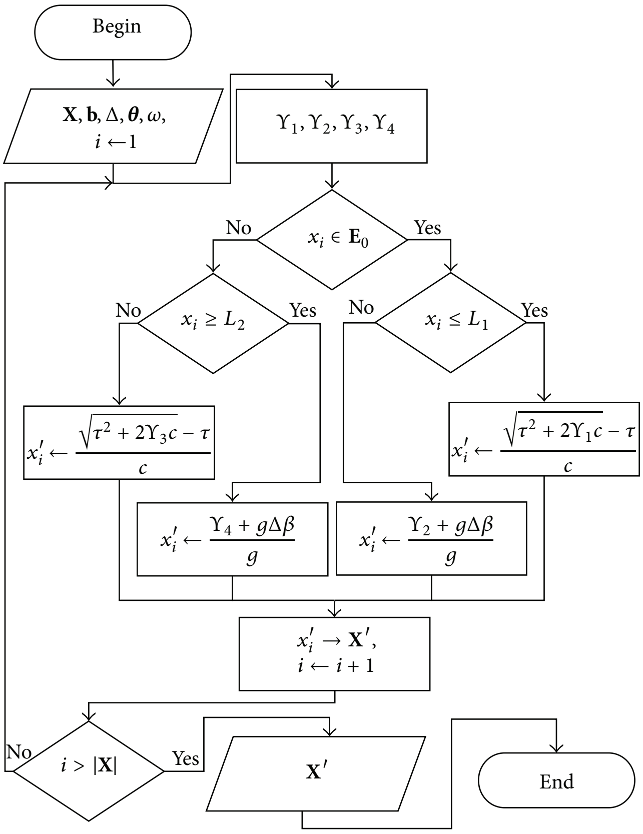

Begin
$\mathbf{X}, \mathbf{b}, \Delta, \boldsymbol{\theta}, \omega,$
$i \leftarrow 1$
$\Upsilon_1, \Upsilon_2, \Upsilon_3, \Upsilon_4$
No
$x_i \in \mathbf{E}_0$
Yes
No
$x_i \ge L_2$
Yes
No
$x_i \le L_1$
Yes
$x_i' \leftarrow \frac{\sqrt{\tau^2 + 2\Upsilon_3 c} - \tau}{c}$
$x_i' \leftarrow \frac{\sqrt{\tau^2 + 2\Upsilon_1 c} - \tau}{c}$
$x_i' \leftarrow \frac{\Upsilon_4 + g\Delta\beta}{g}$
$x_i' \leftarrow \frac{\Upsilon_2 + g\Delta\beta}{g}$
$x_i' \to \mathbf{X}',$
$i \leftarrow i + 1$
No
$i > |\mathbf{X}|$
Yes
$\mathbf{X}'$
End

Figure 5: Quantization diagram for the kth embedding interval.

Further, utilizing property $L_2 \le L_1$ we can obtain

$$
\begin{gathered}
((x \le L_2) \supset ((\exists x')(U^1 xx') \& (\exists x')(V^1 xx'))), \\
(\forall x), \\
((L_2 < x \le L_1) \\
\supset ((\exists x')(U^1 xx') \& (\exists x')(V^2 xx'))), (\forall x), \\
((L_1 < x) \supset ((\exists x')(U^2 xx') \& (\exists x')(V^2 xx'))) \\
\vDash F2, \quad (\forall x).
\end{gathered}
\tag{35}
$$

Here, each premise should be true. With the aim to provide this, equations in (25) and (31) should be solvable. It can be seen that the solutions are straightforward:

$$x'_{U^1,V^1} = \frac{\sqrt{\tau^2 + 2\Upsilon_{1,3} c} - \tau}{c}, \tag{36}$$

$$x'_{U^2,V^2} = \frac{\Upsilon_{2,4} + g\Delta\beta}{g}, \tag{37}$$

where, for example, in (36), x'_{U^1,V^1} denotes the values of x' that turn either $U^1 xx'$ or $V^1 xx'$ true for $\Upsilon_1(\cdot)$ or $\Upsilon_3(\cdot)$, respectively. The diagram of quantization is represented in Figure 5. Each ith original sample is chosen from array $\mathbf{X}$ on ith iteration. The corresponding bit of a watermark is chosen from array $\mathbf{b}$. Vector $\boldsymbol{\theta}$ contains parameters of the quantization. At the end of each iteration, quantized value of ith sample is written to array $\mathbf{X}'$.

4. Robustness under AWGN

In this section, we will analytically estimate the robustness of the proposed watermarking scheme under AWGN. Robustness is reflected by the term "extracted information" which denotes mutual information between embedded and detected messages. In contrast to channel capacity, the index of extracted information is practical but depends on the algorithm of detection. Also, throughout this section we assume that the original samples are distributed uniformly inside the quantization interval.

The derivations for extracted information are less involved when Ω is "false." Therefore, only that condition is considered here. In order to estimate extracted information we first find error rates. The rates depend on the attack severity (represented by σ), Δ, and parameter set $\boldsymbol{\theta} = \{\gamma_0, \varphi_1, \eta_1, \vartheta_0, \alpha, \beta\}$. Moreover, we derive a stronger statement that information about Δ/σ and $\boldsymbol{\theta}$ is sufficient to perform analytic estimation of error rates for our watermarking scheme. Finally, we will demonstrate how error rates can be expressed using WNR and $\boldsymbol{\theta}$.

4.1. Estimation of Error Rates. For our estimation, it is considered that, during watermark extraction, in each embedding interval samples that interpret “0” are separated from samples that interpret “1” using a threshold (e.g., hard decision region detector). The position of the threshold in ith embedding interval is $\mathrm{Th} + [\Delta - 2\mathrm{Th}] \bmod (i-k, 2)$ (dashed vertical lines in Figure 1(b)). Therefore, the whole real number line can be seen as a union of two domains:

$$\mathbf{Z} = \bigcup_{m=-\infty}^{\infty} \left[2\Delta m + l_{\Delta}^{k} - \mathrm{Th}, 2\Delta m + l_{\Delta}^{k} + \mathrm{Th}\right), \tag{38}$$

$$\mathbf{O} = \bigcup_{m=-\infty}^{\infty} \left[2\Delta m + l_{\Delta}^{k} + \mathrm{Th}, 2\Delta (m+1) + l_{\Delta}^{k} - \mathrm{Th}\right). \tag{39}$$

During extraction, all the elements in $\mathbf{Z}$ will be labeled “0” and all the elements in $\mathbf{O}$ will be labeled “1.”

After noise is added, elements quantized in kth embedding interval might spread over its limits and other notations should be used. We notate sample values that are affected by noise as ς_n'. Also, ς_n' belongs to some embedding interval and inside this interval we use $x_n' = \varsigma_n' - \Delta\lfloor \varsigma_n'/\Delta \rfloor$. Random variables Σ_n' and X_n' represent ς_n' and x_n', respectively (alternatively we use $\dot{\Sigma}'$ and $\dot{X}'$ to save space in lower subscript part). Therefore, two modified sets are obtained: $\mathbf{E}_0' \xrightarrow{\text{AWGN}} \dot{\mathbf{\Sigma}}_0'$; $\mathbf{E}_1' \xrightarrow{\text{AWGN}} \dot{\mathbf{\Sigma}}_1'$. For noise variance σ^2 we might, for instance, estimate the expected fraction for each of the noisy sets $\dot{\mathbf{\Sigma}}_0'$ and $\dot{\mathbf{\Sigma}}_1'$ in $\mathbf{Z}$. Fractions of $\dot{\mathbf{\Sigma}}_0'$ and $\dot{\mathbf{\Sigma}}_1'$ that belong to $\mathbf{O}$ can be found in a trivial manner. In that way we obtain error rates for “0” and “1.”

However, instead of appealing directly to sets $\dot{\mathbf{\Sigma}}_0'$ and $\dot{\mathbf{\Sigma}}_1'$, we use an indirect but computationally lighter approach. In case Ω is “false” we can conclude for the following distributions of quantized samples (not affected by AWGN yet) that

$$f_{\check{\mathbf{E}}_0'}\left(x'\right) = f_{\check{\mathbf{E}}_1'}\left(x'\right) = f_0\left(x'\right), \tag{40}$$

where

$$\begin{aligned} &\left(\check{E}_0' i x' \equiv \left(E_0' i x' \,\&\, \left(x' \le \Delta(\beta - \alpha)\right)\right)\right), \quad (\forall i)\left(\forall x'\right), \\ &\left(\check{E}_1' i x' \equiv \left(E_1' i x' \,\&\, \left(x' \le \Delta(\beta - \alpha)\right)\right)\right), \quad (\forall i)\left(\forall x'\right). \end{aligned} \tag{41}$$

Also, we can conclude that the following distributions are also identical:

$$f_{\hat{\mathbf{E}}_0'}\left(x'\right) = f_{\hat{\mathbf{E}}_1'}\left(x'\right) = f_1\left(x'\right), \tag{42}$$

where

$$\begin{aligned} &\left(\hat{E}_0' i x' \equiv \left(E_0' i x' \,\&\, \left(x' \ge \Delta\beta\right)\right)\right), \quad (\forall i)\left(\forall x'\right), \\ &\left(\hat{E}_1' i x' \equiv \left(E_1' i x' \,\&\, \left(x' \ge \Delta\beta\right)\right)\right), \quad (\forall i)\left(\forall x'\right). \end{aligned} \tag{43}$$

For any σ, (40) means that, for example, the fraction of elements from $\check{\mathbf{E}}_0'$ that after AWGN appear in $\mathbf{Z}$ is equal to that of $\check{\mathbf{E}}_1'$ and can be calculated using $f_0(x')$. This fraction will be denoted as $\check{F}_{\mathbf{Z}}$. The PDF of AWGN with variance σ_n^2 is denoted as $f_{\mathcal{N}}[\varsigma_n' - \varsigma', 0, \sigma_n]$ using parameters $\varsigma' = x' + l_{\Delta}^{k}$ and ς_n'. Therefore

$$\begin{aligned} &\check{F}_{\mathbf{Z}} \\ &\quad = \int_{\mathbf{Z}} \int_{0}^{\Delta(\beta-\alpha)} f_0\left(x'\right) f_{\mathcal{N}}\left[\varsigma_n' - x' - l_{\Delta}^{k}, 0, \sigma_n\right] dx' d\varsigma_n'. \end{aligned} \tag{44}$$

Fraction of elements from $\hat{\mathbf{E}}_0'$ that after AWGN appear in $\mathbf{Z}$ will be denoted as $\hat{F}_{\mathbf{Z}}$:

$$\hat{F}_{\mathbf{Z}} = \int_{\mathbf{Z}} \int_{\Delta\beta}^{\Delta} f_1\left(x'\right) f_{\mathcal{N}}\left[\varsigma_n' - x' - l_{\Delta}^{k}, 0, \sigma_n\right] dx' d\varsigma_n'. \tag{45}$$

Error rates are calculated using $\check{F}_{\mathbf{Z}}$ and $\hat{F}_{\mathbf{Z}}$:

$$\begin{aligned} \mathrm{BER}_0 &= \left(1 - \check{F}_{\mathbf{Z}}\right) \frac{\gamma_0}{\gamma_0 + \vartheta_0} + \left(1 - \hat{F}_{\mathbf{Z}}\right) \frac{\vartheta_0}{\gamma_0 + \vartheta_0}, \\ \mathrm{BER}_1 &= \check{F}_{\mathbf{Z}} \frac{\eta_1}{\varphi_1 + \eta_1} + \hat{F}_{\mathbf{Z}} \frac{\varphi_1}{\varphi_1 + \eta_1}. \end{aligned} \tag{46}$$

In order to demonstrate that error rates can be calculated based on Δ/σ, $\boldsymbol{\theta}$ we analyze expression for $\check{F}_{\mathbf{Z}}$ (expression for $\hat{F}_{\mathbf{Z}}$ can be analyzed in a similar way). Function $f_0(x')$ is present in (44). According to (2) it is defined using parameters c, τ. Parameters α, β are also present in (2) as well as in (44). Parameters α, β have clear constraints (the same is true about $\gamma_0, \vartheta_0, \varphi_1, \eta_1$). It is possible to express c, τ using α, $\beta, \gamma_0, \vartheta_0, \varphi_1, \eta_1$. In the realization of our method parameter τ is set as

$$\tau = \frac{\gamma_0 + \vartheta_0}{\Delta\gamma_0}. \tag{47}$$

Defining new parameter $\acute{\tau}$ as

$$\acute{\tau} = \tau\Delta, \tag{48}$$

it can be seen that $\acute{\tau} = (\gamma_0 + \vartheta_0)/\gamma_0$ does not depend on the choice of Δ.

Using property of PDF, the following is obtained from (2):

$$\begin{aligned} \int_0^{(\beta-\alpha)\Delta} f_0\left(x'\right) dx' &= c \frac{(\beta - \alpha)^2 \Delta^2}{2} + \tau\Delta(\beta - \alpha) \\ &= 1. \end{aligned} \tag{49}$$

It is easy to derive from (48) and (49) that

$$c\Delta^2 = 2 \frac{1 - \acute{\tau}(\beta - \alpha)}{(\beta - \alpha)^2}. \tag{50}$$

According to (50), it is also obvious that parameter

$$\acute{c} = c\Delta^2 \tag{51}$$

is independent of Δ.

One of the properties of PDF of AWGN is

$$f_{\mathcal{N}}\left[x,0,\sigma_n\right]=\frac{1}{\sigma_n}f_{\mathcal{N}}\left[\frac{x}{\sigma_n},0,1\right]. \tag{52}$$

Therefore, we can rewrite (44) in the following manner:

$$\begin{aligned}\check{F}_{\mathbf{Z}}={}&\int_{\mathbf{Z}}\int_{0}^{\Delta(\beta-\alpha)}f_0\left(x'\right)f_{\mathcal{N}}\left[\varsigma_n'-x'-l_{\Delta}^{k},0,\right.\\&\left.\sigma_n\right]dx'd\varsigma_n'=\frac{\Delta^2}{\sigma_n}\int_{(\mathbf{Z}-l_{\Delta}^{k})/\Delta}\int_{0}^{(\beta-\alpha)}f_0\left(x'\right)\\&\cdot f_{\mathcal{N}}\left[\Delta\frac{\left(\varsigma_n'-l_{\Delta}^{k}\right)-x'}{\Delta\sigma_n},\right.\\&\left.0,1\right]d\left\{\frac{x'}{\Delta}\right\}d\left\{\frac{\left(\varsigma_n'-l_{\Delta}^{k}\right)}{\Delta}\right\}.\end{aligned} \tag{53}$$

Now, it can be demonstrated that domain

$$\acute{\mathbf{Z}}=\frac{\left(\mathbf{Z}-l_{\Delta}^{k}\right)}{\Delta}=\bigcup_{m=-\infty}^{\infty}\left[2m-\frac{\mathrm{Th}}{\Delta},2m+\frac{\mathrm{Th}}{\Delta}\right) \tag{54}$$

is independent of Δ if during extraction parameter

$$\acute{\mathrm{Th}}=\frac{\mathrm{Th}}{\Delta} \tag{55}$$

can be set without information about Δ (e.g., $\acute{\mathrm{Th}}$ may be set as $\acute{\mathrm{Th}}=\beta-0.5\alpha$). Hence, (53) can be represented in the following way:

$$\begin{aligned}\check{F}_{\mathbf{Z}}={}&\int_{\acute{\mathbf{Z}}}\int_{0}^{(\beta-\alpha)}\frac{\Delta}{\sigma_n}\left(\acute{c}\frac{x'}{\Delta}+\acute{\tau}\right)f_{\mathcal{N}}\left[\frac{\Delta}{\sigma_n}\frac{\left(\varsigma_n'-l_{\Delta}^{k}\right)-x'}{\Delta},\right.\\&\left.0,1\right]d\left\{\frac{x'}{\Delta}\right\}d\left\{\frac{\left(\varsigma_n'-l_{\Delta}^{k}\right)}{\Delta}\right\}.\end{aligned} \tag{56}$$

Here, for integration we consider $(\varsigma_n'-l_{\Delta}^{k})/\Delta\in\acute{\mathbf{Z}}$ and $x'/\Delta\in[0,(\beta-\alpha)]$, where both domains $\acute{\mathbf{Z}}$ and $[0,(\beta-\alpha)]$ depend only on β,α. Except the terms $(\varsigma_n'-l_{\Delta}^{k})/\Delta$ and x'/Δ, only Δ/σ_n, $\acute{c},\acute{\tau}$ appear under the integrals. Therefore, the result of integration, $\check{F}_{\mathbf{Z}}$, depends only on Δ/σ_n, $\boldsymbol{\theta}$.

Further we will express Δ/σ_n in terms of WNR and $\boldsymbol{\theta}$ which confirms that BER_0 and BER_1 can be defined using only WNR and $\boldsymbol{\theta}$.

4.2. Estimation of Δ/σ_n. Measure WNR is widely used in watermarking. It expresses relation between watermark and noise energies and in AWGN case is

$$\mathrm{WNR}=10\log_{10}\left(\frac{D}{\sigma^2}\right), \tag{57}$$

where D is the energy of the watermark. Plot of robustness index in respect to WNR is one of the characteristics that are the most meaningful for practical implementation [4, 11]. Therefore it is important to be able to express error rates using WNR and the set of embedding parameters $\boldsymbol{\theta}$. For this purpose, we first express Δ/σ_n using WNR and $\boldsymbol{\theta}$.

Parameter D in (57) can be seen as a distortion of a host signal, caused by the quantization. There are many different approaches that adequately assess quality degradation for digital images [19, 20]. Nevertheless, in this paper we are using simple and well-known distortion measure based on MSE between original and quantized samples [21]. We will define D and factor it in a form $\Delta^2 Q$, where Q depends only on $\boldsymbol{\theta}$. It is assumed that original samples are distributed uniformly inside embedding interval. Distortion D is needed to obtain quantized sets $\check{\mathbf{E}}_0'$, $\check{\mathbf{E}}_1'$, $\widehat{\mathbf{E}}_0'$, and $\widehat{\mathbf{E}}_1'$. Therefore, further we will consider D as a sum of four kinds of distortion: $D=\check{D}_0+\check{D}_1+\widehat{D}_0+\widehat{D}_1$. Each of the distortion components is defined as follows:

$$\begin{aligned}\check{D}_0={}&\gamma_0\int_{0}^{\Delta(\beta-\alpha)}f_0\left(x'\right)\left(x'-\frac{\Delta\gamma_0}{\gamma_0+\vartheta_0}\right.\\&\left.\cdot\int_{0}^{x'}f_0\left(x'\right)dx'\right)^2dx',\\\check{D}_1={}&\eta_1\int_{0}^{\Delta(\beta-\alpha)}f_0\left(x'\right)\left(x'-\frac{\Delta\eta_1}{\eta_1+\varphi_1}\right.\\&\left.\cdot\int_{0}^{x'}f_0\left(x'\right)dx'\right)^2dx',\\\widehat{D}_0={}&\vartheta_0\int_{\beta\Delta}^{\Delta}f_1\left(x'\right)\left(x'-\left(\frac{\Delta\vartheta_0}{\gamma_0+\vartheta_0}\int_{\beta\Delta}^{x'}f_1\left(x'\right)dx'\right.\right.\\&\left.\left.+\frac{\Delta\gamma_0}{\gamma_0+\vartheta_0}\right)\right)^2dx',\\\widehat{D}_1={}&\varphi_1\int_{\beta\Delta}^{\Delta}f_1\left(x'\right)\left(x'-\left(\frac{\Delta\varphi_1}{\eta_1+\varphi_1}\int_{\beta\Delta}^{x'}f_1\left(x'\right)dx'\right.\right.\\&\left.\left.+\frac{\Delta\eta_1}{\eta_1+\varphi_1}\right)\right)^2dx'.\end{aligned} \tag{58}$$

It can be demonstrated that each of the distortion components can be factored using Δ^2. For instance, considering $\check{D}_0$ the next result can be obtained:

$$\begin{aligned}\check{D}_0={}&\Delta^2\gamma_0\int_{0}^{(\beta-\alpha)}\left(\acute{c}\frac{x'}{\Delta}+\acute{\tau}\right)\left(\frac{x'}{\Delta}\right.\\&\left.-\check{\rho}_0\int_{0}^{x'/\Delta}\left(\acute{c}\frac{x'}{\Delta}+\acute{\tau}\right)d\left\{\frac{x'}{\Delta}\right\}\right)^2d\left\{\frac{x'}{\Delta}\right\}\\&=\Delta^2\check{Q}_0,\end{aligned} \tag{59}$$

where

$$\check{Q}_0 = \gamma_0 (\beta - \alpha)^3 \left(\frac{\acute{c}^3 \check{\rho}_0^2}{24} (\beta - \alpha)^3 + \acute{c}^2 \check{\rho}_0 \frac{5\acute{\tau}\check{\rho}_0 - 4}{20} (\beta - \alpha)^2 + \frac{\acute{c}(1 - \acute{\tau}\check{\rho}_0)(1 - 2\acute{\tau}\check{\rho}_0)}{4} (\beta - \alpha) + \frac{\acute{\tau}(1 - \acute{\tau}\check{\rho}_0)^2}{3} \right). \tag{60}$$

Here

$$\check{\rho}_0 = \frac{\gamma_0}{\gamma_0 + \vartheta_0}. \tag{61}$$

The rest of the distortion components can also be factored in a similar way, where

$$\begin{aligned}
\check{Q}_1 &= \eta_1 (\beta - \alpha)^3 \left(\frac{\acute{c}^3 \check{\rho}_1^2}{24} (\beta - \alpha)^3 + \acute{c}^2 \check{\rho}_1 \frac{5\acute{\tau}\check{\rho}_1 - 4}{20} (\beta - \alpha)^2 + \frac{\acute{c}(1 - \acute{\tau}\check{\rho}_1)(1 - 2\acute{\tau}\check{\rho}_1)}{4} (\beta - \alpha) + \frac{\acute{\tau}(1 - \acute{\tau}\check{\rho}_1)^2}{3} \right), \\
\widehat{Q}_0 &= \vartheta_0 \acute{g} (1 - \beta) \left(\frac{(1 - \widehat{\rho}_0 \acute{g})^2}{3} (1 + \beta + \beta^2) + (1 - \widehat{\rho}_0 \acute{g})(\widehat{\rho}_0 \acute{g}\beta - \check{\rho}_0)(1 + \beta) + (\widehat{\rho}_0 \acute{g}\beta - \check{\rho}_0)^2 \right), \\
\widehat{Q}_1 &= \varphi_1 \acute{g} (1 - \beta) \left(\frac{(1 - \widehat{\rho}_1 \acute{g})^2}{3} (1 + \beta + \beta^2) + (1 - \widehat{\rho}_1 \acute{g})(\widehat{\rho}_1 \acute{g}\beta - \check{\rho}_1)(1 + \beta) + (\widehat{\rho}_1 \acute{g}\beta - \check{\rho}_1)^2 \right), \\
\check{\rho}_1 &= \frac{\eta_1}{\eta_1 + \varphi_1}, \\
\widehat{\rho}_0 &= 1 - \check{\rho}_0 = \frac{\vartheta_0}{\gamma_0 + \vartheta_0}, \\
\widehat{\rho}_1 &= 1 - \check{\rho}_1 = \frac{\varphi_1}{\eta_1 + \varphi_1}.
\end{aligned} \tag{62}$$

Factorization in the form $D = \Delta^2 Q$ can be done based on $Q = \check{Q}_0 + \check{Q}_1 + \widehat{Q}_0 + \widehat{Q}_1$. Therefore, according to (57) Δ/σ can be expressed in the following way:

$$\frac{\Delta}{\sigma} = \sqrt{\frac{10^{0.1 * \mathrm{WNR}}}{\check{Q}_0 + \check{Q}_1 + \widehat{Q}_0 + \widehat{Q}_1}}. \tag{63}$$

5. Experimental Results

In this section, two different settings are considered for experiments. AWGN attack is investigated assuming the first kind of settings and GA attack is investigated assuming the second kind of settings. For the first type, the obtained results are compared with the results of QIM and DC-QIM. For the second type, the performance is compared with the results of RDM (DC-QIM was not considered here as it is vulnerable to GA). Here, in each type of experiment, the goal is to estimate the highest possible amount of extracted information of the method for a given intensity of attack. We explore optimization of embedding parameters. During watermark embedding, parameters $\gamma_0, \vartheta_0, \varphi_1, \eta_1$, and Ω define sets $\mathbf{E}_0$ and $\mathbf{E}_1$. In addition to the mentioned parameters, c, τ, and g are needed to define $\mathbf{E}_0'$ and $\mathbf{E}_1'$. Extracted information is maximized over $\gamma_0, \vartheta_0, \varphi_1, \eta_1, \Omega, c, \tau$, and g by brute force approach. With the aim to reduce computations, parameters $\eta_1, \vartheta_0, \varphi_1$, and γ_0 are constrained according to our considerations.

5.1. Information Extracted under AWGN.

During the experiment, parameters $\eta_1, \gamma_0, \vartheta_0$, and φ_1 were constrained as $\eta_1 + \gamma_0 = 0.5$, $\vartheta_0 + \varphi_1 = 0.5$. It can be explained by our intention to use a detector based on median thresholding inside embedding interval. Therefore, if one detects the watermark message right after embedding, the IDL fraction for "0" and "1" will be ϑ_0 and η_1, respectively. One of the advantages of median thresholding is that no additional information is needed for detection even though the distribution of quantized samples is asymmetric and controlled by many parameters. The parameter Th for median-based (hard decision) detector is calculated using two steps: (a) for all ς_n' find x_n' according to (5); (b) calculate $\mathrm{Th} = \mathrm{median}(X_n')$.

For other methods that were used for comparisons, the standard hard decision detector was used (with equal length of decision intervals for "0" and "1").

For the proposed watermarking method IDL occurs only if the condition $\gamma_0 + \varphi_1 < 1$ holds. In that case, different values of ω cause different robustness characteristics. However, IDL might not be suitable for some application in Digital Watermarking. For instance, in semifragile watermarking a fraction of lost data can be interpreted as the presence of an attack (which increases false positive rate). Therefore, condition $\gamma_0 + \varphi_1 = 1$ has been investigated first.

In Figure 6, amount of extracted information toward WNR is plotted for the proposed method, DC-QIM and QIM [8]. During watermark extraction, the value of the normalized threshold was set to $\acute{\mathrm{Th}} = \beta - 0.5\alpha$.

Error rates were calculated according to (46). However, only the integers from $[-100, 100]$ were used as a set for m in (38) instead of the whole set $\mathbb{Z}$. The purpose of the limitation is to reduce computational complexity while still maintaining high fidelity of the result. Then, the maximized amount of extracted information C was calculated according to

$$C = \max_{p_{\mathrm{em}}(\sim b)} \left[p(\sim b, b) \log_2 \left(\frac{p(\sim b, b)}{p_{\mathrm{em}}(\sim b)\, p_{\mathrm{ex}}(b)} \right) + p(b, \sim b) \log_2 \left(\frac{p(b, \sim b)}{p_{\mathrm{em}}(b)\, p_{\mathrm{ex}}(\sim b)} \right) \right.$$

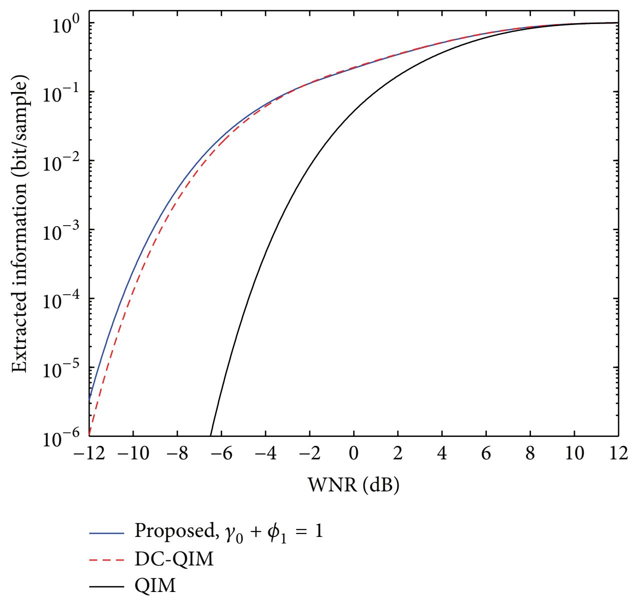


Figure 6: Analytic-based estimation of information extracted under AWGN without IDL.

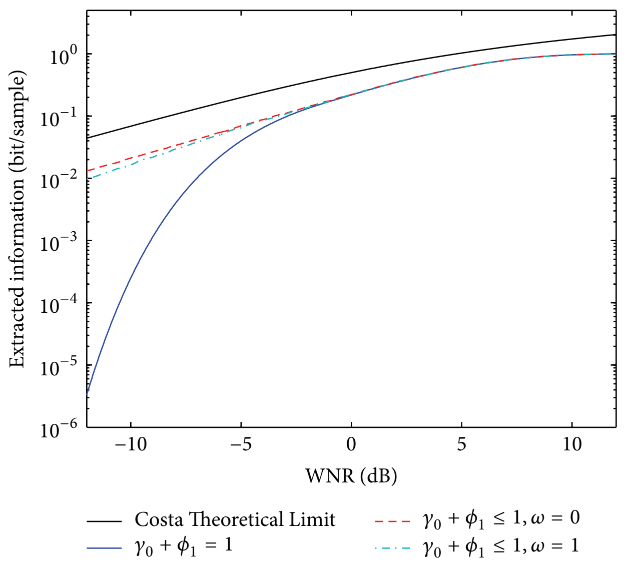


Figure 7: Analytic-based estimation of information extracted under AWGN with IDL.

$$+ p(\sim b, \sim b)\log_2\left(\frac{p(\sim b, \sim b)}{p_{\mathrm{em}}(\sim b)\, p_{\mathrm{ex}}(\sim b)}\right) + p(b, b)\log_2\left(\frac{p(b, b)}{p_{\mathrm{em}}(b)\, p_{\mathrm{ex}}(b)}\right)\Bigg]. \tag{64}$$

Here, $p(\sim b, b)$ denotes joint probability of embedding symbol $\sim b$ and extracting symbol b; $p_{\mathrm{em}}(b)$ and $p_{\mathrm{ex}}(b)$ denote probabilities of symbol b to be embedded and extracted, respectively. Using joint probabilities, we calculate probabilities of extracting a particular bit:

$$\begin{aligned} p_{\mathrm{ex}}(b) &= p(\sim b, b) + p(b, b), \\ p_{\mathrm{ex}}(\sim b) &= p(b, \sim b) + p(\sim b, \sim b). \end{aligned} \tag{65}$$

Joint probabilities can be expressed using $p_{\mathrm{em}}(\cdot)$ and error rates:

$$\begin{aligned} p(\sim b, b) &= p_{\mathrm{em}}(\sim b)\,\mathrm{BER}_0, \\ p(b, \sim b) &= p_{\mathrm{em}}(b)\,\mathrm{BER}_1, \\ p(\sim b, \sim b) &= p_{\mathrm{em}}(\sim b)\left(1 - \mathrm{BER}_0\right), \\ p(b, b) &= p_{\mathrm{em}}(b)\left(1 - \mathrm{BER}_1\right). \end{aligned} \tag{66}$$

As it was mentioned earlier, embedding probabilities are

$$\begin{aligned} p_{\mathrm{em}}(\sim b) &= \gamma_0 + \vartheta_0, \\ p_{\mathrm{em}}(b) &= \eta_1 + \varphi_1. \end{aligned} \tag{67}$$

From Figure 6 it can be seen that with no IDL the proposed method performs better than QIM for WNR ≤ 9 dB and better than DC-QIM for WNR values less than −2 dB.

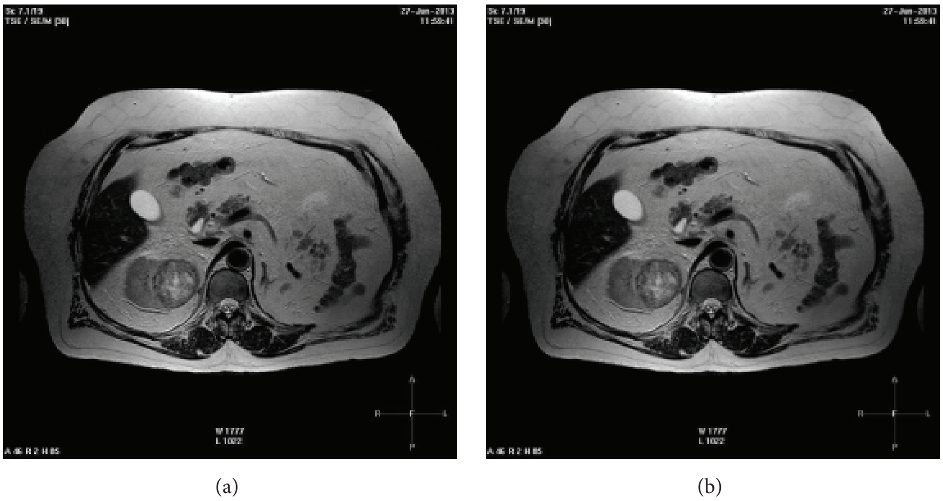
While comparing the designed method with DC-QIM, explanation of a slightly better performance should be found in the new distribution of quantized samples and thresholding technique. Optimal solution for the problem of informed data hiding has been theorized by Costa [6], and every known practical answer, including DC-QIM, uses structured codebook which lacks certain desirable characteristics [11]. We believe that the minor advantage of the presented method is due to larger number of variables that were adjusted for embedding.

In case IDL is acceptable (for a particular watermarking application), much better results are achievable for both "true" and "false" Ω under low WNRs (Figure 7). Obviously, the demonstrated superiority is due to IDL only. Additionally, it can be seen that "false" logical value of Ω provides slightly more beneficial outcome under AWGN compared to when Ω is "true." As a reference, Costa Theoretical Limit (CTL) [6] is plotted in Figure 7:

$$\mathrm{CTL} = \frac{1}{2}\log_2\left(1 + 10^{0.1*\mathrm{WNR}}\right). \tag{68}$$

5.2. Information Extracted under GA. In this subsection, we explore performance of the proposed quantization approach under GA. For comparison, RDM is chosen instead of DC-QIM as it is known to be vulnerable to GA. We describe conditions and the results of the simulations based on real images and assuming watermark embedding followed by GA.

For the experimental evaluation, we used 92 natural grayscale images with resolution 512 × 512. Each image was split on 4 × 4 blocks and first singular values of Singular Value Decomposition (SVD) were quantized to embed a watermark [22]. The watermarking was arranged without IDL and



(a)

(b)

Figure 8: Common MRI imaging of a patient's kidney: (a) original diagnostic image; (b) watermarked image.

$\gamma_0 = \varphi_1 = 0.5$. Document to Watermark Ratio (DWR) was set to 28 dB, where

$$\mathrm{DWR} = 10\log_{10}\left(\frac{\sigma_H^2}{D}\right) \quad (69)$$

and σ_H^2 is the variance of the original coefficients. An example of original and watermarked diagnostic images is given in Figure 8.

For some healthcare organizations, protection of personal data is a high priority task. On the other hand, diagnostic data might need to be shared between experts from other organizations. For that purpose, DIW is a suitable tool [23]. However, an important additional constraint is imposed in that case: an expert conclusion (diagnosis) should not be affected by watermarking. According to the judgements of collaborating group of medical imaging experts, the diagnostic statement for the watermarked image in Figure 8(b) is identical to the statement for the original one in Figure 8(a).

For watermark embedding (encoding), a brute force optimization over α and β was repeated for each new value of σ. Obviously, this needs to be done only once as the optimal parameters can be stored. In addition to the concept of optimal parameters, we investigated efficiency of a constrained version of the proposed quantization approach, where α and β were constant and equal to 0.05 and 0.35, respectively. The common sense behind such a modification is that actual σ of AWGN might not be known on practice during watermark embedding (because the attack happens after embedding).

For watermark extraction (hard decision decoding), these two steps are required: (1) apply GA recovery procedure; (2) define threshold. In accordance with the proposed procedure for GA recovery, criterion C_1 was used for the estimation of actual Δ during the experiment. The condition of GA was simulated by ignoring information about Δ value that was used for embedding. Hence, the value was estimated by the procedure of GA recovery. No information except initial guess interval with $\widetilde{\Delta}'_{\min} = 0.9\Delta$, $\widetilde{\Delta}'_{\max} = 1.1\Delta$ was used for watermark extraction. In contrast to that, RDM does use the information about the exact value of quantization step. For RDM, the value of a given quantized coefficient was calculated using the information about the previous 100 coefficients.

Two types of thresholding are possible and two types of extraction conditions exist. Under condition when α and β are constants, no additional information needs to be transferred to the decoder. However, if α and β are optimized on encoder's side, information about them might need to be sent. This is necessary if thresholding is established in the way that $\acute{\mathrm{Th}} = \beta - 0.5\alpha$ (e.g., the threshold is in the middle of separating zone in quantization interval). Since the requirement for additional information seems impractical, we proposed median thresholding $\mathrm{Th} = \mathrm{median}(X'_n)$ as well.

For each method that took part in the experiment, the resulting amount of extracted information is plotted toward AWGN variance (Figure 9).

As it can be seen from Figure 9, under both mentioned conditions of embedding, the proposed approach outperforms RDM. The advantage is more evident for larger AWGN variance.

6. Discussion

In the experimental section, robustness of the proposed quantization method was estimated under AWGN and GA. The proposed approach provides higher amount of extracted information compared to the other state-of-the-art reference methods, like DC-QIM and RDM. The reasons of its superiority will be discussed in more detail in this section.

Asymmetric distribution of quantized samples and the proposed procedure for GA recovery is a successful combination that provides robustness under GA. Compared to other estimations of the scaling factor from the literature, the proposed estimation approach is light. For instance, in order to estimate the scaling factor, a model of a host is used in [14] which complicates estimation and reduces

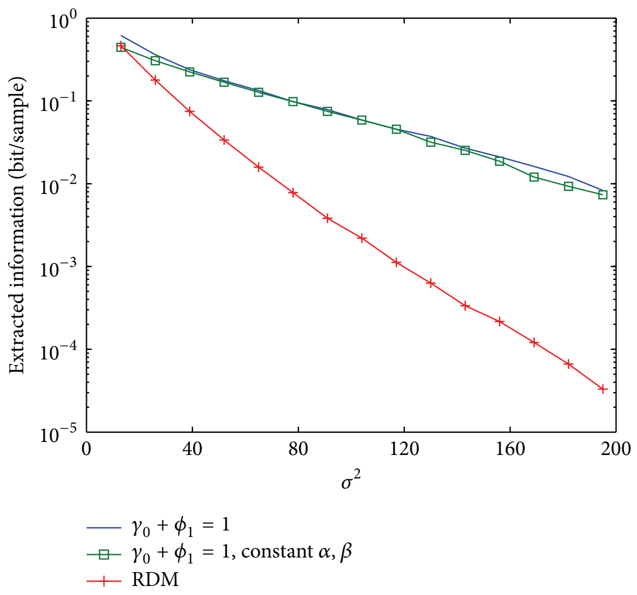


FIGURE 9: Information extracted under GA followed by AWGN.

its precision. On the other hand, an approach different to estimation is exploited by RDM [15]. However, Distortion Compensation is not present in RDM. In contrast to that, the proposed quantization method has Distortion Compensation and outperforms RDM because AWGN is introduced (as a second stage of GA).

The proposed quantization approach demonstrates higher robustness under AWGN compared to well-known DC-QIM. The advancement that causes such superiority is IDL. Parameter Ω was introduced in order to distinguish between two different ways of realization for IDL. Target distribution for all the samples in quantization interval remains the same for any logical value of Ω (which guarantees equally successful recovery from GA). Distributions are different if "ones" and "zeros" are considered separately. This influences the resulting performance. As it has been demonstrated by the experiment, modification of the quantization approach with "false" Ω performs slightly better. In general, usage of IDL is beneficial under low WNRs. The common sense here is that predicting the loss of some information (as a result of an attack) we might accept the scenario when a part of information is lost initially. Compared to DC-QIM, such quantization behavior enables redistribution of embedding distortion from samples that are likely to be misinterpreted to the other (non-IDL) samples that can be more robust.

Unlike DC-QIM, the proposed quantization method has many parameters that need to be set up for watermark embedding. Some additional parameters might be needed depending on the technique for watermark extraction. For instance, the thresholding that depends on $\acute{\mathrm{Th}} = \beta - 0.5\alpha$ may be applied, which requires parameters α, β to be communicated to the receiver.

On the other hand, no parameters are needed for extraction if the proposed median thresholding is used (absolutely blind extraction). Parameter Δ can be estimated using procedure for GA recovery taking as input only rough interval $[\widetilde{\Delta}'_{\min}, \widetilde{\Delta}'_{\max}]$. This is an advantage compared to DC-QIM that always requires Δ to be known to the decoder.

We do not consider any case with malicious attacks (that analyze and deliberately change the watermarked signal) as they are not the objectives of our paper. However in case a key is used to protect a watermark, it will also be needed for decoding.

Lastly, we need to emphasize that the computational cost of our scheme is low. Optimization of embedding parameters conducted in Section 5 is computationally heavy, but it needs to be done only once. The optimized parameters can be used for embedding then. The computational cost of embedding is comparable with that of DC-QIM (please, refer to the quantization diagram). For extraction, complexity of the proposed procedure of GA recovery is $O(n)$.

7. Conclusions

A new scalar QIM-based watermarking method has been proposed in this paper. It provides higher robustness under AWGN and GA compared to other quantization methods. The benefits of the method are due to the introduced procedure of recovery after GA as well as new distribution of quantized samples with IDL.

For the new distribution of quantized samples there is no symmetry inside embedding interval. The nonsymmetric distribution of quantized samples is exploited by the introduced procedure of recovery after GA. Two different criteria are proposed to be used within the procedure. During experiment it has been confirmed that the procedure is computationally light and efficient.

In addition to the new kind of distribution of quantized samples, the proposed QIM-based method benefits from IDL. Utilization of IDL can reduce embedding distortions introduced to a host signal. This is done by letting some watermark bits to be interpreted incorrectly during embedding and before any attack occurs. A model that describes quantization process assumes that IDL can be implemented in two different ways depending on the logical value of parameter Ω. The proposed realization of IDL is beneficial for any Ω under highly intensive AWGN attack. However, "false" value of Ω provides slightly higher robustness compared to "true."

Considerable performance improvements are due to the abovementioned advancements. The amount of information extracted (using hard decision decoder) under AWGN is at the same or of a higher level compared to DC-QIM. Usage of IDL is the most advantageous under AWGN for WNRs close to −12 dB, where it performs up to 10^4 times better than DC-QIM. Under GA, the performance of the proposed method is up to 10^3 times higher than that of RDM. Finally, visual quality degradation caused by the proposed quantization method was also estimated in a subjective way by a group of medical imaging experts. It was confirmed that as a result of watermarking, important diagnostic characteristics did not change.

Nomenclature

i:	Unique integer index for each particular sample
Σ:	Random variable for the domain of original samples
ς:	Particular realization of Σ
Δ:	The length of embedding interval
l_{Δ}^{k}:	The left endpoint of kth embedding interval
X:	Random variable for the domain of original samples inside embedding interval
x:	Particular realization of X
X':	Random variable for the domain of quantized samples inside embedding interval
x':	Particular realization of X'
Σ':	Random variable for the domain of quantized samples
ς':	Particular realization of Σ'
$f_0(x')$, $f_1(x')$:	Truncated distributions for quantized samples inside embedding interval
α, β,τ, c, g:	Parameters of $f_0(x')$, $f_1(x')$
γ_0, ϑ_0, φ_1, η_1:	Fractions of samples that are labeled as non-IDL$_0$, IDL$_0$, non-IDL$_1$, and IDL$_1$, respectively
$\widetilde{\Delta}$:	The length of embedding interval that is required for watermark extraction after GA
$\widetilde{\Delta}'$:	Uniformly sampled guessed values of $\widetilde{\Delta}$
$\widetilde{\Delta}''$:	Best-fit value from $\{\widetilde{\Delta}'\}$ according to the estimator
Σ_n' (or $\dot{\Sigma}'$):	Random variable for the domain of quantized samples affected by attack/noise
ς_n':	Particular realization of Σ_n'
X_n' (or $\dot{X}'$):	Random variable for the domain of noisy quantized samples inside embedding interval
x_n':	Particular realization of X_n'
ω:	Parameter of quantization model
$\mathbf{E}$:	The set of X
$\mathbf{E}_0$, $\mathbf{E}_1$:	Two disjoint subsets of $\mathbf{E}$ defined by $\gamma_0 + \vartheta_0$ and $\varphi_1 + \eta_1$, respectively
$\mathbf{E}'$:	The set of X'
$\mathbf{E}_0'$, $\mathbf{E}_1'$:	Two disjoint subsets of $\mathbf{E}'$
$X_{\mathbf{E}_0}$:	Random variable from $\mathbf{E}_0$
$X_{\mathbf{E}_1}$:	Random variable from $\mathbf{E}_1$
$X_{\mathbf{E}_0'}'$:	Random variable from $\mathbf{E}_0'$
$X_{\mathbf{E}_1'}'$:	Random variable from $\mathbf{E}_1'$
$f_{\mathbf{E}_0}(x)$:	PDF of $X_{\mathbf{E}_0}$
$f_{\mathbf{E}_1}(x)$:	PDF of $X_{\mathbf{E}_1}$
$f_{\mathbf{E}_0'}(x')$:	PDF of $X_{\mathbf{E}_0'}'$
$f_{\mathbf{E}_1'}(x')$:	PDF of $X_{\mathbf{E}_1'}'$
Th:	The threshold used by the detector
$\acute{\mathrm{T}}\mathrm{h}$:	The normalized threshold used by the detector, for example, $\acute{\mathrm{T}}\mathrm{h} = \mathrm{Th}/\Delta$
$\mathbf{Z}$:	Decision region "0" for the detector
$\mathbf{O}$:	Decision region "1" for the detector
$\dot{\boldsymbol{\Sigma}}_0'$:	The set of all the elements of $\mathbf{E}_0'$ influenced by an attack
$\dot{\boldsymbol{\Sigma}}_1'$:	The set of all the elements of $\mathbf{E}_1'$ influenced by an attack
$\mathbf{IDL}_0$, $\mathbf{NIDL}_0$:	Two disjoint subsets of $\mathbf{E}_0$, defined by ϑ_0 and γ_0, respectively
$\mathbf{IDL}_1$, $\mathbf{NIDL}_1$:	Two disjoint subsets of $\mathbf{E}_1$, defined by η_1 and φ_1, respectively
$\check{\mathbf{E}}_0'$, $\widehat{\mathbf{E}}_0'$:	Two disjoint subsets of $\mathbf{E}_0'$, defined by γ_0 and ϑ_0, respectively
$\check{\mathbf{E}}_1'$, $\widehat{\mathbf{E}}_1'$:	Two disjoint subsets of $\mathbf{E}_1'$, defined by η_1 and φ_1, respectively
$\check{D}_0$:	Embedding distortion necessary to transform $\mathbf{NIDL}_0$ to $\check{\mathbf{E}}_0'$
$\check{D}_1$:	Embedding distortion necessary to transform $\mathbf{IDL}_1$ to $\check{\mathbf{E}}_1'$
$\widehat{D}_0$:	Embedding distortion necessary to transform $\mathbf{IDL}_0$ to $\widehat{\mathbf{E}}_0'$
$\widehat{D}_1$:	Embedding distortion necessary to transform $\mathbf{NIDL}_1$ to $\widehat{\mathbf{E}}_1'$
BER$_0$:	Bit Error Rate for $\mathbf{E}_0'$
BER$_1$:	Bit Error Rate for $\mathbf{E}_1'$
C:	Maximized mutual information between embedded and detected messages.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

The paper was supported by University of Tampere. Additional gratitude for provided diagnostic images and postwatermarking quality assessment is to Dr. Oleksandr Iatsyna and other members of collaborating oncological expert group from National Cancer Institute, Kiev, Ukraine.

References

[1] J. Fridrich, *Steganography in Digital Media: Principles, Algorithms, and Applications*, Cambridge University Press, New York, NY, USA, 2009.

[2] M. Barni, F. Bartolini, V. Cappellini, and A. Piva, "Robust watermarking of still images for copyright protection," in *Proceedings of 13th International Conference on Digital Signal Processing (DSP '97)*, vol. 2, pp. 499–502, Santorini, Greece, July 1997.

[3] H. R. Sheikh and A. C. Bovik, "Image information and visual quality," *IEEE Transactions on Image Processing*, vol. 15, no. 2, pp. 430–444, 2006.

[4] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, *Digital Watermarking and Steganography*, Morgan Kaufmann Publishers, San Francisco, Calif, USA, 2nd edition, 2007.

[5] T. Bianchi and A. Piva, "Secure watermarking for multimedia content protection: a review of its benefits and open issues," *IEEE Signal Processing Magazine*, vol. 30, no. 2, pp. 87–96, 2013.

[6] M. H. Costa, "Writing on dirty paper," *IEEE Transactions on Information Theory*, vol. 29, no. 3, pp. 439–441, 1983.

[7] B. Chen and G. W. Wornell, "Dither modulation: a new approach to digital watermarking and information embedding," in *Security and Watermarking of Multimedia Contents*, vol. 3657 of *Proceedings of SPIE*, pp. 342–353, San Jose, Calif, USA, April 1999.

[8] B. Chen and G. W. Wornell, "Quantization index modulation: a class of provably good methods for digital watermarking and information embedding," *IEEE Transactions on Information Theory*, vol. 47, no. 4, pp. 1423–1443, 2001.

[9] E. Esen and A. Alatan, "Forbidden zone data hiding," in *Proceedings of the IEEE International Conference on Image Processing*, pp. 1393–1396, Atlanta, Ga, USA, October 2006.

[10] M. Ramkumar and A. N. Akansu, "Signalling methods for multimedia steganography," *IEEE Transactions on Signal Processing*, vol. 52, no. 4, pp. 1100–1111, 2004.

[11] J. J. Eggers, R. Bäuml, R. Tzschoppe, and B. Girod, "Scalar Costa scheme for information embedding," *IEEE Transactions on Signal Processing*, vol. 51, no. 4, pp. 1003–1019, 2003.

[12] J. Oostveen, T. Kalker, and M. Staring, "Adaptive quantization watermarking," in *Security, Steganography, and Watermarking of Multimedia Contents VI*, Proceedings of SPIE, pp. 296–303, San Jose, Calif, USA, January 2004.

[13] X. Kang, J. Huang, and W. Zeng, "Improving robustness of quantization-based image watermarking via adaptive receiver," *IEEE Transactions on Multimedia*, vol. 10, no. 6, pp. 953–959, 2008.

[14] I. D. Shterev and R. L. Lagendijk, "Amplitude scale estimation for quantization-based watermarking," *IEEE Transactions on Signal Processing*, vol. 54, no. 11, pp. 4146–4155, 2006.

[15] F. Pérez-González, C. Mosquera, M. Barni, and A. Abrardo, "Rational dither modulation: a high-rate data-hiding method invariant to gain attacks," *IEEE Transactions on Signal Processing*, vol. 53, no. 10, pp. 3960–3975, 2005.

[16] F. Ourique, V. Licks, R. Jordan, and F. Pérez-González, "Angle QIM: a novel watermark embedding scheme robust against amplitude scaling distortions," in *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '05)*, vol. 2, pp. ii/797–ii/800, IEEE, Philadelphia, Pa, USA, March 2005.

[17] M. Zareian and H. R. Tohidypour, "Robust quantisation index modulation-based approach for image watermarking," *IET Image Processing*, vol. 7, no. 5, pp. 432–441, 2013.

[18] X. Zhu and J. Ding, "Performance analysis and improvement of dither modulation under the composite attacks," *EURASIP Journal on Advances in Signal Processing*, vol. 2012, no. 1, article 53, 2012.

[19] Q. Sang, X. Wu, C. Li, and Y. Lu, "Universal blind image quality assessment using contourlet transform and singular-value decomposition," *Journal of Electronic Imaging*, vol. 23, no. 6, Article ID 061104, 2014.

[20] S. Chikkerur, V. Sundaram, M. Reisslein, and L. J. Karam, "Objective video quality assessment methods: a classification, review, and performance comparison," *IEEE Transactions on Broadcasting*, vol. 57, no. 2, pp. 165–182, 2011.

[21] M. Petrou and C. Petrou, *Image Processing: The Fundamentals*, John Wiley & Sons, 2010.

[22] Y. Zolotavkin and M. Juhola, "A new blind adaptive watermarking method based on singular value decomposition," in *Proceedings of the International Conference on Sensor Network Security Technology and Privacy Communication System (SNS & PCS '13)*, pp. 184–192, Taipei, Taiwan, March 2013.

[23] W. Pan, G. Coatrieux, N. Cuppens-Boulahia, F. Cuppens, and C. Roux, "Watermarking to enforce medical image access and usage control policy," in *Proceedings of the 6th International Conference on Signal-Image Technology and Internet-Based Systems (SITIS '10)*, pp. 251–260, IEEE, Kuala Lumpur, Malaysia, December 2010.