

Research Article

A New QIM-Based Watermarking Method Robust to Gain Attack

Yevhen Zolotavkin and Martti Juhola

Research Center for Information and Systems, School of Information Sciences, University of Tampere, Kanslerinrinne 1, 33014 Tampere, Finland

Correspondence should be addressed to Yevhen Zolotavkin; zhzolat@suremail.us

Received 26 May 2014; Accepted 22 August 2014; Published 11 September 2014

Academic Editor: Harald Kosch

Copyright © 2014 Y. Zolotavkin and M. Juhola. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

We propose a new watermarking method based on quantization index modulation. A concept of initial data loss is introduced in order to increase capacity of the watermarking channel under high intensity additive white Gaussian noise. According to the concept some samples in predefined positions are ignored even though this produces errors in the initial stage of watermark embedding. The proposed method also exploits a new form of distribution of quantized samples where samples that interpret “0” and “1” have differently shaped probability density functions. Compared to well-known watermarking schemes, this provides an increase of capacity under noise attack and introduces a distinctive feature. Two criteria are proposed that express the feature numerically. The criteria are utilized by a procedure for estimation of a gain factor after possible gain attack. Several state-of-the-art quantization-based watermarking methods were used for comparison on a set of natural grayscale images. The superiority of the proposed method has been confirmed for different types of popular attacks.

1. Introduction

Digital media have a great impact on many aspects of modern society. Some aspects assume that we deal with audio-visual data that relates to a person or an organization. Information about the relation quite often should be preserved. Watermarking approach is to insert the information in the media itself [1]. However, in that case the watermark might be intentional or not altered by the third party. In order to avoid an alteration the watermark needs to be robust [2]. Other characteristics except robustness may also be important. Watermark invisibility and payload are among them. Invisibility is important to assure that the quality of the media does not degrade significantly as a result of watermarking [3]. High data payload might be needed in some applications in order to define many aspects of ownership.

In the field of digital image watermarking (DIW) digital images are used as a media (or host). DIW incorporates many different techniques and one of the most popular among them is quantization index modulation (QIM). Methods that belong to QIM are widely used in blind watermarking where neither original media nor watermark is known to the receiver [4]. For the purpose of evaluating robustness the watermarked image is being attacked and additive white

Gaussian noise (AWGN) is the most popular condition for that. Theoretical limit of the channel capacity which is achievable by QIM under AWGN was first derived in [5].

In most cases quantization is implemented to some coefficients rather than to signal samples. In order to obtain coefficients a transform is applied to a host signal. It has been shown that some transforms provide coefficients that are more robust to popular image processing algorithms like JPEG, geometric modifications, and so forth [6, 7].

It is assumed that during quantization each of the original coefficient values belongs to one of equally spaced intervals. Further, inside each interval coefficients to interpret “0” and “1” are selected. The task of quantization is to separate coefficients that represent different bits inside each interval. The separation efficiency influences robustness and invisibility. The result of the separation can be characterized by the size of original interval, distribution of separated samples, and the distortion incurred by the separation.

However, all the known implementations of QIM are far from achieving the capacity limit under AWGN. The simplest scalar realization of QIM is to replace all the coefficient values from a certain interval by a single value equal either to the left or right endpoint depending on a bit of a watermark [8].

Hence, the distribution of quantized samples that represent both “0” and “1” is degenerate (or Dirac). Nevertheless, the capacity of the simplest QIM (further referred to as QIM without “simplest”) is less than 10% of the limit value for the condition when noise and watermark energies are equal. More advanced realization of DC-QIM is to replace each coefficient value from an original interval by a corresponding value taken from one out of two disjoint intervals that are subsets of the original one [9]. A parameter $0.5(1 - \alpha)$ is to control the size of these intervals relatively to the original. The distribution for “0” and “1” in that case is uniform. Parameter α is being adjusted depending on noise level in order to maximize capacity. Method DC-QIM is widely used and provides the highest capacity under AWGN among known practical realizations. However, considering AWGN attack only, the most evident gap under high noise intensity is caused by low capacity in comparison with the theoretical limit.

Some other modifications of QIM have emerged over the past years. Forbidden zone data hiding (FZDH) modifies only a fraction (controlled by α) of coefficient values in each interval of original values [10]. Despite the fact that FZDH performs slightly worse than DC-QIM the paper represents a promising idea on how to reduce embedding distortions. Another idea was proposed by the authors of Thresholded Constellation Modulation (TCM) that use two different quantization rules to modify coefficients inside the original interval [11]. Each rule is applied only to samples from a particular subinterval and β defines their endpoints. The value of a shift is different for any value from a subinterval according to the first quantization rule. The second rule is to provide an equal shift to all the values from another subinterval. There are two shift directions in order to embed “0” and “1”.

The main advantage of the techniques based on QIM with different kinds of compensation [9–11] is a considerable robustness against AWGN. The limitation is that synchronization is required to extract a watermark. Even minor distortion of a different kind can make embedded information unreadable. The simplest realization of such kind of distortion is a gain attack (GA) which performs a constant scaling of the whole sequence of watermarked coefficients. 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. Usually GA is followed by AWGN that complicates retrieval of the watermark [12]. Vulnerability to GA causes one of the most critical gaps for practical implementation of QIM-based methods with compensation.

Many different approaches have been developed to improve robustness against GA of QIM related methods [13]. Most approaches can be classified into two groups where the main idea of the first group is to estimate the unknown factor while the idea of second is to quantize coefficients that are invariant to scaling of original signal.

Estimation of the scaling factor requires modelling. Some feature that is unique for the watermarked and attacked signal might be described by a model [14]. The scaling factor may be included in the model and to be a subject

to optimization. An obvious complication is that a process of feature selection is not straightforward. In some cases the feature is created instead of being selected and some permanent data agreed upon between the sender and the receiver is a suitable example. However, such compulsory agreement limits practical implementation of watermarking method. Other possible limitations are low model accuracy or computationally heavy optimization.

For instance, a kind of GA and a constant offset attack followed by AWGN are assumed in [12]. The solution proposed there is to embed a pilot signal and to use Fourier analysis to estimate the gain factor and the offset. However, an obvious disadvantage of the solution is that the precision of estimated parameters is low even for quite long pilot sequence.

The method of recovery after GA and AWGN is proposed in [15]. It uses information about dither sequence and applies maximum likelihood (ML) procedure to estimate the scaling factor. The estimation is based on a model of watermarked and attacked signal. Information about statistical characteristics of original host signal should be either known or guessed in order to define the model. Another limitation of the approach is that it requires exact information about embedding parameter α . Computational complexity of the approach is high.

As an opposite for estimation, invariance to GA, in general, requires more complex transform of original signal (e.g., nonlinear,) to obtain coefficients. It is necessary to modify coefficients to embed a watermark. However, a model to estimate distortions of the host is more complex in that case. Distortions should be controlled which limits the choice of the kind of QIM to one that adds less complexity to a model of distortion. This, for example, might result in reducing the number of adjustable parameters of QIM. This is one of the reasons why invariant to GA approaches are more vulnerable to AWGN compared to DC-QIM.

Rational dither modulation (RDM) is one of the most popular watermarking methods invariant to GA [16]. For a particular coefficient, a ratio that depends on a norm of other coefficients is being quantized instead of a coefficient itself. The simplest QIM scheme is utilized in order to quantize the ratio and the performance of RDM under AWGN (without GA) is close to the simplest QIM. Other recent blind watermarking methods robust to GA are proposed in [17–23]. Nevertheless, for GA invariant methods the gap is caused by the reduced capacity under AWGN.

In this paper, we propose our own scalar QIM-based watermarking approach that is beneficial in several aspects. The approach addresses the mentioned gaps in the literature: it both delivers higher capacity under AWGN and recovers after GA. In order to do this, host signal coefficients are separated in a way that the resulting distributions for coefficients that interpret “0” and “1” are different. This distinctive feature is used by a simple yet efficient procedure for estimation of a scaling factor under GA. A concept of initial data loss (IDL) is introduced in order to increase watermark channel capacity under low watermark to noise ratios (WNRs). According to IDL, some fraction of wrong watermark bits is accepted during embedding procedure.

The rest of the paper is organized as follows. In Section 2 we describe our quantization model using formal logic approach and derive some constraints on the parameters of the model. In Section 3 some important watermarking characteristics of the model are evaluated analytically while the following Section 4 contains description for the procedure of recovery after GA as well as experimental results obtained under popular attacks. In Section 5 we discuss in detail experimental conditions and compare the performance of the proposed method with the performance of well-known methods. Section 6 concludes the paper and outlines possible directions for improvement.

2. Quantization Model

In this section we define a new model of quantization. First, it is necessary to show that according to our model the separation of original coefficients is possible and we can embed information. Formal logic approach is used to define dependencies between several conditions that are important for the separation of original coefficients. Separation argument (SA) represents the model in a compact form yet has a clear structure which is sufficient to reason the intuition behind the dependencies. Second, it is necessary to assure conditions when SA is sound.

2.1. Formalization of SA. 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 by ς . We will further describe our model for values ς that are in some interval of size Δ . More specifically we will refer to an interval with integer index k whose left endpoint is l_{Δ}^k . Such an interval is referred to 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 length Δ is selected in a way that an appropriate document to watermark ratio (DWR) is guaranteed after the separation. We also assume that Δ is small enough to derive that the distribution of X is uniform. A random variable that represents separated coefficients inside k th interval is denoted by X' and its realization is denoted by x' . Correspondingly, a random variable that represents separated coefficients on the whole real number line is denoted by Σ' and its realization is denoted by ς' . Each pair of an original x and corresponding quantized x' belong to the same k th embedding interval so that an absolute shift is never larger than Δ .

Let us denote a watermark bit by b . Truncated pdfs $f_0(x')$ and $f_1(x')$ are used to describe the distribution of X' and should be defined prior to quantization. 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 the samples where original values x are to be modified by a quantizer for $b = 1$ and $b = 0$, respectively. It is therefore assumed that the fraction of zeros in a watermark data is $\gamma_0 + \vartheta_0$ and fraction of ones is $\varphi_1 + \eta_1$. Condition $\gamma_0 + \vartheta_0 + \varphi_1 + \eta_1 = 1$ always holds. The result of the separation in the k th embedding interval depends on $b, \eta_1, \vartheta_0, \varphi_1, \gamma_0, f_0(x')$, and $f_1(x')$. In other

words x' is defined by quantizer $Q_{\Delta}^k[\cdot]$ that has the mentioned parameters:

$$x' = Q_{\Delta}^k[x, b, \eta_1, \vartheta_0, \varphi_1, \gamma_0, f_0, f_1]. \quad (1)$$

We will use SA to describe the quantizer $Q_{\Delta}^k[\cdot]$. Each of logical atoms p, q, r, s, t, u , and v represents some condition which is either true or false:

$$p \mid x \leq \frac{\Delta\gamma_0}{\gamma_0 + \vartheta_0}, \quad (2)$$

$$q \mid x \geq \frac{\Delta\eta_1}{\varphi_1 + \eta_1}, \quad (3)$$

$$r \mid x' = x, \quad (4)$$

$$s \mid x' < x, \quad (5)$$

$$t \mid x' > x, \quad (6)$$

$$u \mid x \frac{\gamma_0 + \vartheta_0}{\Delta} = \gamma_0 \int_0^{x'} f_0(x') dx', \quad (7)$$

$$v \mid (\Delta - x) \frac{\varphi_1 + \eta_1}{\Delta} = -\varphi_1 \int_{\Delta}^{x'} f_1(x') dx'. \quad (8)$$

For example, $(\sim b \& p)$ is true if and only if “ $b = 0$ ” and x is not classified for IDL. We formalize SA in the following way:

$$\begin{aligned} & ((\sim b \& p) \supset (u \& (s \vee r))), \\ & ((b \& q) \supset (v \& (t \vee r))), \\ & (((\sim b \& \sim p) \vee (b \& \sim q)) \supset r) \\ & \models ((u \& (s \vee r)) \vee (v \& (t \vee r)) \vee r). \end{aligned} \quad (9)$$

It can be seen that SA is valid. The conclusion of SA states that the separation of coefficient values inside k th embedding interval is possible which means that the proposed model is suitable for information embedding. Furthermore, each premise represents an important dependency between input and output of the quantizer $Q_{\Delta}^k[\cdot]$ and we require that each premise is indeed true. Hence, it is necessary to enforce soundness for SA.

The intuition behind SA can be explained in the following way. Initially samples with labels “ $b = 0$ ” and “ $b = 1$ ” are not separated in the dimension of x inside the mentioned k th embedding interval. In order to separate them we shift those with “ $b = 0$ ” to the left and those with “ $b = 1$ ” to the right. If so, shift to the right for “ $b = 0$ ” or shift to the left for “ $b = 1$ ” is not acceptable because it would introduce distortion and on the other hand worsen separation between “0” and “1.” Therefore for $\sim b$ formula $(s \vee r)$ is true and for b formula $(t \vee r)$ is true.

Another consideration is that for any two $x_i \leq x_j$ with the same bit value we infer that quantization in a way that $x'_i \leq x'_j$ implies less distortion than if $x'_i > x'_j$. Saving the order we preserve cumulative distribution in respect to the order. Quantized samples x' that interpret “0” are distributed according to pdf $f_0(x')$; samples x' that interpret “1” are distributed according to pdf $f_1(x')$. Therefore u or v is true if $(\sim b \& p)$ or $(b \& q)$ is true, respectively.

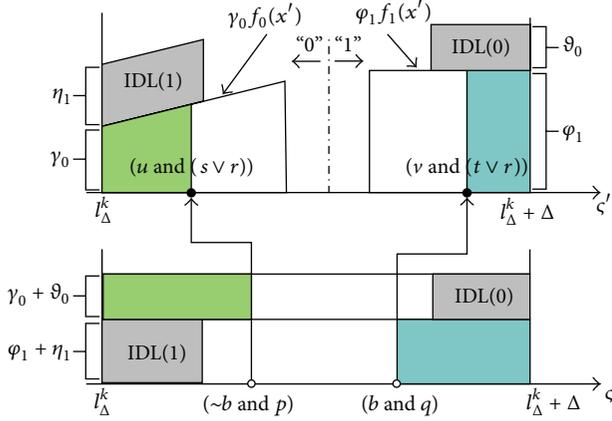


FIGURE 1: Illustration of the process of separation.

And, lastly, the condition for IDL is $((\sim b \& \sim p) \vee (b \& \sim q))$ and it is the case when x is not modified and therefore r .

An illustration of an example where SA is sound is given in Figure 1. Two positions of original values are shown on the lower part of Figure 1. Condition $(\sim b \& p)$ is satisfied for the first original value and condition $(b \& q)$ is satisfied for the second. Two positions of the modified values are shown on the upper part of Figure 1. After the separation the modified values satisfy conditions $(u \& (s \vee r))$ and $(v \& (t \vee r))$, respectively. The areas of green segments on the lower and the upper parts of Figure 1 are equal. The areas of blue segments are also equal. As it can be seen on the upper part of Figure 1, the distribution of separated coefficients in k th embedding interval depends on $\Delta, \eta_1, \vartheta_0, \varphi_1, \gamma_0, f_0(x')$, and $f_1(x')$.

Parameters of the pdfs $f_0(x')$ and $f_1(x')$ need to be specified in order to prove soundness for the whole range of x in the k th interval. In addition formulas (7) and (8) need to be rearranged in order to express x' in a suitable way for the quantization form.

We propose such $f_0(x')$ and $f_1(x')$ that in general there is no line of symmetry which can separate them inside embedding interval. This feature will provide easier recovery after GA. It is necessary to emphasize that the proposed functions $f_0(x')$ and $f_1(x')$ only describe distributions for fractions γ_0 and φ_1 , respectively (e.g., without taking into account fractions of IDL). We introduce parameters α, β , and τ to define both pdfs $f_0(x')$ and $f_1(x')$, where $0 \leq \alpha \leq \beta \leq 1$, as shown in Figure 2(a). As can be seen the density is zero in the subinterval $(\Delta(\beta - \alpha), \Delta\beta)$ which separates "0" from "1." In Figure 2(b) we can see the distribution of the quantized coefficients outside k th embedding interval as well.

Namely, the proposed truncated pdfs are a linear function and a constant:

$$f_0(x') = \begin{cases} cx' + \tau, & \text{if } x' \in [0, \Delta(\beta - \alpha)], \\ 0, & \text{otherwise;} \end{cases} \quad (10)$$

$$f_1(x') = \begin{cases} g, & \text{if } x' \in [\Delta\beta, \Delta], \\ 0, & \text{otherwise.} \end{cases} \quad (11)$$

The samples that belong to IDL fraction are distributed according to pdfs $IDL_0(x')$ and $IDL_1(x')$:

$$IDL_0(x') = \begin{cases} \frac{\gamma_0 + \vartheta_0}{\Delta\vartheta_0}, & \text{if } x' \in \left[\frac{\Delta\gamma_0}{\gamma_0 + \vartheta_0}, \Delta \right], \\ 0, & \text{otherwise;} \end{cases} \quad (12)$$

$$IDL_1(x') = \begin{cases} \frac{\varphi_1 + \eta_1}{\Delta\eta_1}, & \text{if } x' \in \left[0, \frac{\Delta\eta_1}{\varphi_1 + \eta_1} \right], \\ 0, & \text{otherwise.} \end{cases}$$

2.2. *Soundness Conditions for SA.* The soundness of SA is guaranteed if it is possible to satisfy $(u \& (s \vee r))$ or $(v \& (t \vee r))$ when $(\sim b \& p)$ or $(b \& q)$ is true, respectively. The requirement to satisfy $(u \& (s \vee r))$ or $(v \& (t \vee r))$ imposes some constraints on $\alpha, \beta, c, g, \tau, \gamma_0, \varphi_1, \eta_1, \vartheta_0$, and Δ . Let us find those constraints.

We start from defining parameters of $f_0(x')$ and $f_1(x')$ using property of pdf:

$$\int_0^{(\beta-\alpha)\Delta} f_0(x') dx' = c \frac{(\beta - \alpha)^2 \Delta^2}{2} + \tau \Delta (\beta - \alpha) = 1, \quad (13)$$

$$\int_{\beta\Delta}^{\Delta} f_1(x') dx' = g \Delta (1 - \beta) = 1. \quad (14)$$

It is easy to derive from (14) that

$$g = \frac{1}{\Delta(1 - \beta)}. \quad (15)$$

According to (4), (5), and (7) condition $(u \& (s \vee r))$ is satisfied if and only if for all x'

$$x' \frac{\gamma_0 + \vartheta_0}{\Delta} \leq \gamma_0 \int_0^{x'} f_0(x') dx'. \quad (16)$$

Using (10) and the fact $x' \geq 0$ we can derive

$$\tau \geq \frac{\gamma_0 + \vartheta_0}{\Delta\gamma_0} - c \frac{x'}{2}. \quad (17)$$

The latter inequality should be true for all $x' \in [0, \Delta(\beta - \alpha)]$ which means

$$\tau \geq \max_{x' \in [0, \Delta(\beta - \alpha)]} \left(\frac{\gamma_0 + \vartheta_0}{\Delta\gamma_0} - c \frac{x'}{2} \right). \quad (18)$$

For our particular application we chose $c \geq 0$; therefore

$$\tau \geq \frac{\gamma_0 + \vartheta_0}{\Delta\gamma_0}, \quad (19)$$

and we are using the value $\tau = (\gamma_0 + \vartheta_0)/(\Delta\gamma_0)$ in our method. Using (13) we can conclude that

$$c = 2 \frac{\gamma_0 - (\gamma_0 + \vartheta_0)(\beta - \alpha)}{\gamma_0(\beta - \alpha)^2 \Delta^2}. \quad (20)$$

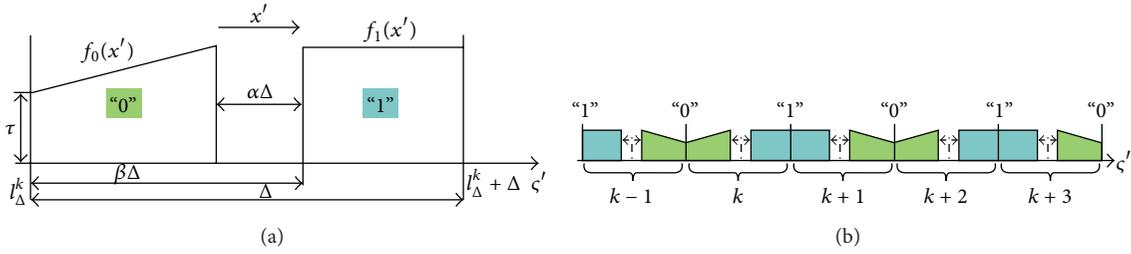


FIGURE 2: Distribution of the quantized coefficients: (a) inside k th embedding interval; (b) in five consecutive intervals.

Functions $f_0(x')$ and $f_1(x')$ can be fully defined now. Let us find dependencies that connect α and β with γ_0 , φ_1 , η_1 , and ϑ_0 . Taking into account that in our realization $c \geq 0$ we can derive from (20) that

$$\beta - \alpha \leq \frac{\gamma_0}{\gamma_0 + \vartheta_0}. \quad (21)$$

According to (4), (6), and (8) condition $(v \& (t \vee r))$ is satisfied if and only if

$$\frac{\varphi_1 + \eta_1}{\Delta} \leq g\varphi_1. \quad (22)$$

Using (15) we find that

$$\beta \geq \frac{\eta_1}{\varphi_1 + \eta_1}. \quad (23)$$

In the experiment section of the paper the goal is to find the highest capacity for a given WNR. Different values of the parameters need to be checked for that purpose. Preserving (15) and (19)–(21), (23) would guarantee soundness of SA and avoidance of using parameters' combinations that are not efficient for watermarking. This can reduce required computations.

2.3. Embedding Equations. For the proposed pdfs we can now define x' as a function of x , which is the main task of the quantizer $Q_{\Delta}^k[\cdot]$. Let us consider conditions $(\sim b \& p)$, $(b \& q)$ separately as it is never the case when both conditions are true. We will denote x' in case of $(\sim b \& p)$ by \dot{x}' , but in case of $(b \& q)$ the notation \ddot{x}' will be used.

From (7), (10), and $\tau = (\gamma_0 + \vartheta_0)/(\Delta\gamma_0)$ it is clear that

$$0.5c\dot{x}'^2 + \tau\dot{x}' = \tau x. \quad (24)$$

Taking into account that $\dot{x}' \geq 0$ we derive

$$\dot{x}' = \frac{\sqrt{\tau^2 + 2c\tau x}}{c} - \frac{\tau}{c}. \quad (25)$$

From (8), (11), and (15) we can find that

$$\ddot{x}' = Bx + \Delta(1 - B), \quad B = \frac{(1 - \beta)(\varphi_1 + \eta_1)}{\varphi_1}. \quad (26)$$

According to (26), the values of quantized coefficients are linearly dependent on original values while according

to (25) the dependency is nonlinear. Different character of dependency between quantized and original values for "0" and "1" is one of the key features of our approach. This differentiates the proposed watermarking method from the methods previously described in the literature [10–12].

3. Characteristics of Quantization Model

The model was proposed in the previous section. It was shown that it is suitable for coefficient separation and the conditions necessary for soundness of SA were defined. In this section we focus on efficiency of separation. The main characteristic that can be estimated analytically is the watermark channel capacity under AWGN. It is required to calculate such characteristic for different WNRs. First, we express WNR in terms of parameters of the quantization scheme. Second, we express error rates in terms of parameters of the quantization scheme. This makes it possible to include WNR in the expression for error rates (and capacity).

3.1. Estimation of Quantization Distortions. The variance σ_n^2 is the only parameter of AWGN attack and WNR is defined as

$$\text{WNR} = 10 \log_{10} \left(\frac{D}{\sigma_n^2} \right), \quad (27)$$

where D is a watermark energy. Alternatively, D can be seen as a distortion of a host signal, induced by the quantization. Let us define D .

For the matter of convenience of the experiment it is better to use a single parameter (control parameter) that can be adjusted in order to provide the desired value of D . While defining D we choose Δ to be the control parameter and collect it in the expression for D . The total distortion D is a sum of distortions D_0 and D_1 caused by two types of shifts that are $x \rightarrow \dot{x}'$ and $x \rightarrow \ddot{x}'$, respectively. The first distortion component D_0 is defined as

$$D_0 = \gamma_0 \int_0^{\Delta(\beta-\alpha)} f_0(x') \left(x' - \frac{1}{\tau} \int_0^{x'} f_0(x') dx' \right)^2 dx'. \quad (28)$$

Proceeding further and using (10) we can derive that

$$D_0 = \gamma_0 \int_0^{\Delta(\beta-\alpha)} (cx' + \tau) \frac{c^2 x'^4}{4\tau^2} dx'. \quad (29)$$

However, it is clear from (19)-(20) that both parameters c and τ depend on Δ . In order to collect Δ we introduce two independent of Δ parameters $\hat{c} = c\Delta^2$ and $\hat{\tau} = \tau\Delta$. This brings us to

$$D_0 = \Delta^2 Q_0, \quad (30)$$

$$Q_0 = \gamma_0 \left(\frac{\hat{c}^3}{24\hat{\tau}^2} (\beta - \alpha)^6 + \frac{\hat{c}^2}{20\hat{\tau}} (\beta - \alpha)^5 \right).$$

The second distortion component D_1 is defined as

$$D_1 = \varphi_1 \times \int_{\beta\Delta}^{\Delta} f_1(x') \times \left(x' - \left(\frac{\varphi_1 \Delta}{\eta_1 + \varphi_1} \int_{\beta\Delta}^{x'} f_1(x') dx' + \frac{\eta_1 \Delta}{\eta_1 + \varphi_1} \right) \right)^2 dx'. \quad (31)$$

Using (11), (15), and integrating in (31) we obtain

$$D_1 = \Delta^2 Q_1, \quad (32)$$

$$Q_1 = \varphi_1 \frac{((\eta_1 + \varphi_1)(1 - \beta) - \varphi_1)^2}{3(\eta_1 + \varphi_1)^2}.$$

The total quantization distortion D can be expressed in terms of Δ , Q_0 , and Q_1 :

$$D = \Delta^2 (Q_0 + Q_1). \quad (33)$$

For any combination of σ_n^2 , WNR, α , β , η_1 , ϑ_0 , γ_0 , and φ_1 the required value of Δ is defined using (27) and (33) as

$$\Delta = \sqrt{\frac{\sigma_n^2 10^{0.1 * \text{WNR}}}{Q_0 + Q_1}}. \quad (34)$$

3.2. Estimation of Error Rates. Bit error rate (BER) and channel capacity can be calculated without simulation of watermark embedding procedure. It is important that the kind of threshold used to distinguish between “0” and “1” is suitable for analytic estimations. Further we assume that the position of the threshold remains permanent after watermark is embedded and does not depend on attack parameters. In Figure 2(b) the position of the threshold is Th for intervals numbered $k + 2m$, $m \in \mathbb{Z}$. For the intervals numbered $k + 2m + 1$ the position of the threshold is $\Delta - \text{Th}$.

The absolute value of quantized sample in any interval is ζ' . We use ζ'_n for a sample that is distorted by noise. Hence, ζ'_n interprets “0” or “1” depending on belonging to \mathbf{Z} or \mathbf{O} , respectively:

$$\mathbf{Z} = \bigcup_{m=-\infty}^{\infty} [2\Delta m + l_{\Delta}^k - \text{Th}, 2\Delta m + l_{\Delta}^k + \text{Th}), \quad (35)$$

$$\mathbf{O} = \bigcup_{m=-\infty}^{\infty} [2\Delta m + l_{\Delta}^k + \text{Th}, 2\Delta(m + 1) + l_{\Delta}^k - \text{Th}). \quad (36)$$

There are two cases when errors occur in non-IDL samples. An error in “0” is incurred by a noise if and only if the both following conditions are true:

$$(\zeta' \in \mathbf{Z}), \quad (\zeta'_n \in \mathbf{O}). \quad (37)$$

An error in “1” occurs if and only if the following is true:

$$(\zeta' \in \mathbf{O}), \quad (\zeta'_n \in \mathbf{Z}). \quad (38)$$

Two cases when errors occur in IDL samples can be presented with the following conditions for “0” and “1” respectively:

$$(\zeta' \in \mathbf{O}), \quad (\zeta'_n \in \mathbf{O}), \quad (39)$$

$$(\zeta' \in \mathbf{Z}), \quad (\zeta'_n \in \mathbf{Z}). \quad (40)$$

The pdf of AWGN with variance σ_n^2 can be represented in terms of ζ' and ζ'_n as $f_{\mathcal{N}}[\zeta'_n - \zeta', 0, \sigma_n]$. In general we can estimate error rates for an interval with any integer index $k + m$. For that purpose we use generalized notations $\dot{f}_0(\zeta')$, $\dot{f}_1(\zeta')$, $\text{IDL}_0(\zeta')$, and $\text{IDL}_1(\zeta')$ for pdfs of quantized samples in any interval. For example, for even m pdf $\dot{f}_0(\zeta') = f_0[\zeta' - (l_{\Delta}^k + \Delta m)]$; for odd m pdf $\dot{f}_0(\zeta') = f_0[l_{\Delta}^k + \Delta(m + 1) - \zeta']$. We denote $k + m$ interval by $I_{k+m} = [l_{\Delta}^k + \Delta m, l_{\Delta}^k + \Delta(m + 1)]$. Then, the error rates for quantized samples in I_{k+m} can be defined as

$$\text{BER}_0 = \frac{\gamma_0}{\gamma_0 + \vartheta_0} \int_{\mathbf{O}} \int_{I_{k+m}} \dot{f}_0(\zeta') f_{\mathcal{N}}[\zeta'_n - \zeta', 0, \sigma_n] d\zeta' d\zeta'_n + \frac{\vartheta_0}{\gamma_0 + \vartheta_0} \int_{\mathbf{O}} \int_{I_{k+m}} \text{IDL}_0(\zeta') \times f_{\mathcal{N}}[\zeta'_n - \zeta', 0, \sigma_n] d\zeta' d\zeta'_n, \quad (41)$$

$$\text{BER}_1 = \frac{\varphi_1}{\varphi_1 + \eta_1} \int_{\mathbf{Z}} \int_{I_{k+m}} \dot{f}_1(\zeta') f_{\mathcal{N}}[\zeta'_n - \zeta', 0, \sigma_n] d\zeta' d\zeta'_n + \frac{\eta_1}{\varphi_1 + \eta_1} \int_{\mathbf{Z}} \int_{I_{k+m}} \text{IDL}_1(\zeta') \times f_{\mathcal{N}}[\zeta'_n - \zeta', 0, \sigma_n] d\zeta' d\zeta'_n.$$

Now we can show that BER_0 and BER_1 can be calculated according to (41) for any chosen interval. For that purpose it is enough to demonstrate that any component in (41) remains the same for every interval. For example, we state that

$$\int_{\mathbf{O}} \int_{I_{k+m}} \dot{f}_0(\zeta') f_{\mathcal{N}}[\zeta'_n - \zeta', 0, \sigma_n] d\zeta' d\zeta'_n = \int_{\mathbf{O}} \int_0^{\Delta} f_0(x') f_{\mathcal{N}}[\zeta'_n - (l_{\Delta}^k + x'), 0, \sigma_n] dx' d\zeta'_n, \quad (42)$$

for any m .

Let us first assume $m = 2n$, $n \in \mathbb{Z}$. Then, $\zeta' = x' + l_{\Delta}^k + 2\Delta n$, $\dot{f}_0(\zeta') = f_0(x')$. However, it is also clear from (36) that $\mathbf{O} + 2\Delta n = \mathbf{O}$. Hence,

$$\begin{aligned} & \int_{\mathbf{O}} \int_{l_{k+2n}} \dot{f}_0(\zeta') f_{\mathcal{N}}[\zeta'_n - \zeta', 0, \sigma_n] d\zeta' d\zeta'_n \\ &= \int_{\mathbf{O}+2n\Delta} \int_0^{\Delta} f_0(x') \\ & \quad \times f_{\mathcal{N}}[(\zeta'_n - 2n\Delta) \\ & \quad - (l_{\Delta}^k + x'), 0, \sigma_n] dx' d\{\zeta'_n - 2n\Delta\}, \end{aligned} \quad (43)$$

and we prove the statement.

Now let us assume $m = 2n + 1$, $n \in \mathbb{Z}$. Then, $\zeta' = (x' - \Delta) + l_{\Delta}^k + 2\Delta(n + 1)$, $\dot{f}_0(\zeta') = f_0(\Delta - x')$. For the matter of convenience we accept that $l_{\Delta}^k + j\Delta = 0$ for some $j \in \mathbb{Z}$. Therefore $f_{\mathcal{N}}[\zeta'_n - \zeta', 0, \sigma_n] = f_{\mathcal{N}}[(\zeta'_n - 2\Delta(n + 1 - j)) - (-l_{\Delta}^k + (x' - \Delta)), 0, \sigma_n]$. Also $-(\mathbf{O} + 2\Delta(n + 1 - j)) = \mathbf{O}$. The property of pdf of AWGN provides that $f_{\mathcal{N}}[y, 0, \sigma_n] = f_{\mathcal{N}}[-y, 0, \sigma_n]$ and, consequently,

$$\begin{aligned} & f_{\mathcal{N}}[(\zeta'_n - 2\Delta(n + 1 - j)) \\ & \quad - (-l_{\Delta}^k + (x' - \Delta)), 0, \sigma_n] \\ &= f_{\mathcal{N}}[-(\zeta'_n - 2\Delta(n + 1 - j)) \\ & \quad - (l_{\Delta}^k + (\Delta - x')), 0, \sigma_n]. \end{aligned} \quad (44)$$

Using the latest equation we derive that

$$\begin{aligned} & \int_{\mathbf{O}} \int_{l_{k+2n+1}} \dot{f}_0(\zeta') f_{\mathcal{N}}[\zeta'_n - \zeta', 0, \sigma_n] d\zeta' d\zeta'_n \\ &= \int_{-(\mathbf{O}+2\Delta(n+1-j))} \int_0^{\Delta} f_0(\Delta - x') \\ & \quad \times f_{\mathcal{N}}[-(\zeta'_n - 2\Delta(n + 1 - j)) \\ & \quad - (l_{\Delta}^k + (\Delta - x')), 0, \sigma_n] \\ & \quad \times d\{\Delta - x'\} \\ & \quad \times d\{-(\zeta'_n - 2\Delta(n + 1 - j))\}, \end{aligned} \quad (45)$$

and we prove the statement.

4. Experimental Results

In this section we describe conditions, procedure, and results of two different kinds of experiments based on analytic estimation of capacity as well as simulations. The preferred index of attack severity is WNR (indexes σ_n and quality of JPEG compression are also used). For a given set of embedding parameters, the error rates and capacity are

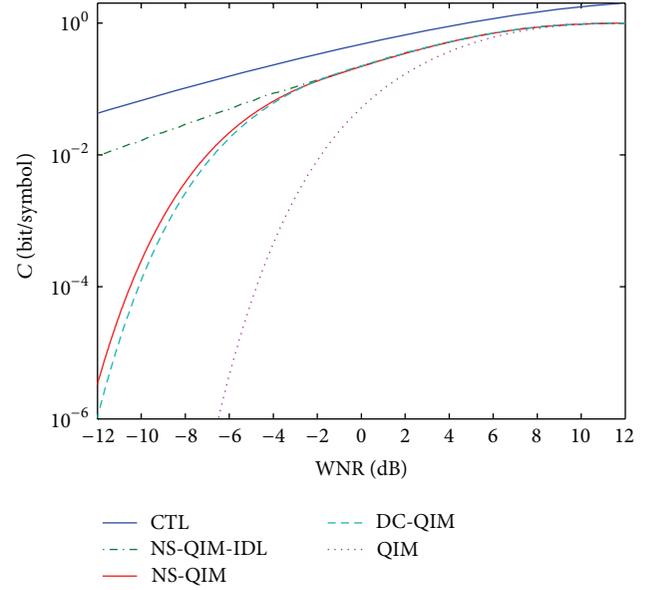


FIGURE 3: Analytic-based estimation of capacity under AWGN.

estimated differently using different models suitable for each kind of experiment. However, for both kinds of experiment, the maximum capacity for a given level of attack severity is found by using brute force search in the space of all adjustable parameters.

4.1. Analytic Estimation of Watermarking Performance under AWGN. In this subsection of our experiment we use $\sigma_n = 1$. Parameters $\alpha, \beta, \eta_1, \gamma_0, \vartheta_0$, and φ_1 are subjects to constraints (21), (23), $\eta_1 + \gamma_0 = 0.5$, and $\vartheta_0 + \varphi_1 = 0.5$ and the simulations are repeated for each new value of WNR. Then, the length of embedding interval Δ is calculated according to (34). Error rates are calculated according to (41).

We use two variants of the proposed quantization scheme with adjustable parameters: nonsymmetric QIM (NS-QIM) and nonsymmetric QIM with IDL (NS-QIM-IDL). Such a decision can be explained by a consideration that IDL is acceptable for some application, but other applications may require all the watermark data to be embedded correctly.

In Figure 3 the plots for channel capacity toward WNR are shown for two variants of the proposed method as well as DC-QIM and QIM [9]. The permanent thresholding $\text{Th} = \Delta(\beta - 0.5\alpha)$ is applied to NS-QIM and NS-QIM-IDL. As a reference, Costa theoretical limit (CTL) [5] is plotted in Figure 3:

$$\text{CTL} = \frac{1}{2} \log_2 (1 + 10^{0.1 * \text{WNR}}). \quad (46)$$

Capacity is calculated analytically according to the description provided in the literature for DC-QIM and QIM.

During the estimation, the subsets $\tilde{\mathbf{Z}} \subset \mathbf{Z}$ and $\tilde{\mathbf{O}} \subset \mathbf{O}$ were used instead of \mathbf{Z} and \mathbf{O} :

$$\begin{aligned}\tilde{\mathbf{Z}} &= \bigcup_{m=-100}^{100} \left[2\Delta m + l_{\Delta}^k - \text{Th}, 2\Delta m + l_{\Delta}^k + \text{Th} \right), \\ \tilde{\mathbf{O}} &= \bigcup_{m=-100}^{100} \left[2\Delta m + l_{\Delta}^k + \text{Th}, 2\Delta(m+1) \right. \\ &\quad \left. + l_{\Delta}^k - \text{Th} \right).\end{aligned}\quad (47)$$

Therefore, for such estimation we assume that quantized coefficients from the k th interval after AWGN are distributed only inside $[-200\Delta + l_{\Delta}^k - \text{Th}, 202\Delta + l_{\Delta}^k - \text{Th})$. The assumption is a compromise between computational complexity and the fidelity of the result.

As can be seen from Figure 3 both variants of the proposed method perform better than DC-QIM for WNR values less than -2 dB and, obviously, much higher capacity provided by DC-QIM-IDL is compared to the other methods in that range. Taking into account that DC-QIM provides the highest capacity under AWGN compared to the other known in the literature methods [12, 19], newly proposed method DC-QIM-IDL fills an important gap. Reasonably, the demonstrated superiority is mostly due to IDL.

4.2. Watermarking Performance in Simulation Based Experiments without GA. The advantage of analytic estimation of error rates according to (41) is that the stage of watermark embedding can be omitted and host signal is not required. The practical limitation of the approach is that $\tilde{\mathbf{Z}}$ and $\tilde{\mathbf{O}}$ are just subsets of \mathbf{Z} and \mathbf{O} , respectively. Other disadvantages are that estimation might become even more complex in case the threshold position is optimized depending on the level of noise; only rates for AWGN can be estimated, but there are other kinds of popular attacks [24]. Therefore in this subsection we will also simulate watermarking experiments using real host signals.

4.2.1. Conditions for Watermark Embedding and Extraction. In case of experiments with real signals the parameters of the proposed watermarking scheme must satisfy some other constraints instead of (34). However, constraints (21), (23), $\eta_1 + \gamma_0 = 0.5$, and $\vartheta_0 + \varphi_1 = 0.5$ remain the same as in the analytic based experiment.

Some lower limit of DWR has to be satisfied for watermarked host, which assures acceptable visual quality. DWR is calculated according to

$$\text{DWR} = 10 \log_{10} \left(\frac{\sigma_H^2}{D} \right), \quad (48)$$

where σ_H^2 is the variance of the host.

Therefore, using (33) the equation for Δ in that case is

$$\Delta = \frac{\sigma_H}{\sqrt{(Q_0 + Q_1) 10^{0.1\text{DWR}}}}. \quad (49)$$

In contrast to analytic based experiment, σ_n should be adjusted for different severity of the attack and is defined as

$$\sigma_n^2 = \frac{\sigma_H^2}{10^{0.1(\text{DWR} + \text{WNR})}}. \quad (50)$$

After watermark is embedded and AWGN with σ_n^2 is introduced we perform extraction and calculate channel capacity.

A variant NSC-QIM with constant (nonadjustable) parameters is also used in some experiments. The intention to adjust the parameters in order to maximize capacity is natural. However, maximization requires information about WNR to be known before watermark embedding and transmission. In some application areas level of noise (or severity of an attack) might change over time or remain unknown. Therefore watermark should be embedded with some constant set of parameters depending on expected WNR.

Different positions of the threshold can be used to extract a watermark. An optimal position of the threshold is not obvious. Placing the threshold in the middle of the interval might be inefficient because the distribution of quantized samples inside embedding interval is nonsymmetric. Two kinds of thresholding are proposed: permanent and nonpermanent. The permanent position is $\text{Th} = \Delta(\beta - 0.5\alpha)$ for the intervals with numbers $k + 2m$, $m \in \mathbb{Z}$. The name ‘‘permanent’’ is because Th cannot be changed after embedding. Its position depends only on α , β , and Δ and does not depend on the parameters of attack.

The nonpermanent position of Th is the median of the distribution inside each interval. Nonpermanent position may depend on the type and severity of a noise. The advantage of nonpermanent Th is that extraction of a watermark can be done without information about α and β .

4.2.2. Watermarking Performance for AWGN and JPEG Attacks without GA. The performance of the proposed method was evaluated using real host signals. For that purpose we used 87 natural grayscale images with resolution 512×512 . Each bit of a watermark was embedded by quantizing the first singular value of SVD of 4×4 block. This kind of transform is quite popular in digital image watermarking and the chosen block size provides a good tradeoff between watermark data payload and robustness [7, 25]. The value of DWR was 28 dB. An attack of AWGN was then applied to each watermarked image. The resulting capacity toward noise variance is plotted for different methods in Figure 4.

It can be seen that the resulting capacity after AWGN attack is the highest for NS-QIM. The other two methods whose performance is quite close to NS-QIM are DC-QIM and FZDH. Compared to DC-QIM the advantage is more obvious for higher variance. However, for moderate variance the advantage is more obvious compared to FZDH.

Methods QIM and RDM do not have parameters that can be adjusted to different variance. Under some circumstances adjustment is not feasible for NS-QIM as well. We have chosen constant parameters $\alpha = 0.05$ and $\beta = 0.35$ for NSC-QIM in order to provide a fair comparison with QIM and RDM. The plots for NSC-QIM, QIM and RDM are marked

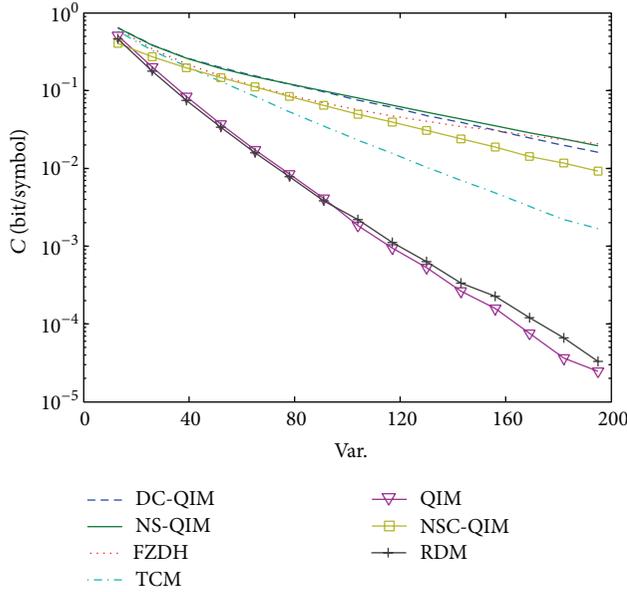


FIGURE 4: Capacity under AWGN for natural grayscale images.

by squares, triangles, and crosses, respectively, in Figure 4. As can be seen, NSC-QIM performs considerably better than QIM and RDM and the advantage is especially noticeable for higher noise variance.

Other image processing techniques except additive noise are able to destroy a watermark and one of them is JPEG compression which is quite popular. The capacity of the proposed watermarking method was also compared with other methods and the procedure of embedding was the same as in AWGN case. However, this time JPEG compression with different levels of quality was considered as an attack. The results are plotted in Figure 5.

According to the plots in Figure 5, the performance of NS-QIM in general is very close to that of DC-QIM but is slightly worse for low Q factor. The methods FZDH and TCM provide lower capacity than NS-QIM and DC-QIM but in general are quite close to them. The worst performance is demonstrated by QIM and RDM and the disadvantage is especially noticeable for low Q. For NSC-QIM with $\alpha = 0.05$ and $\beta = 0.35$ the performance is considerably better than that for QIM and RDM under low Q but is worse for higher quality of JPEG compression.

4.3. Procedure for GA Recovery. It has been demonstrated that for some popular types of attack the performance of NS-QIM is comparable or better than that of DC-QIM. The mentioned DC-QIM is considered to be one of the best quantization methods for watermarking, but it is extremely vulnerable to GA. On the other hand the performance of RDM is not as good under AWGN and JPEG attacks and is comparable to that of QIM. In this subsection, we propose a procedure for GA recovery in order to fill an important gap in the literature and introduce a watermarking method that provides high efficiency under AWGN as well as GA. The procedure utilizes

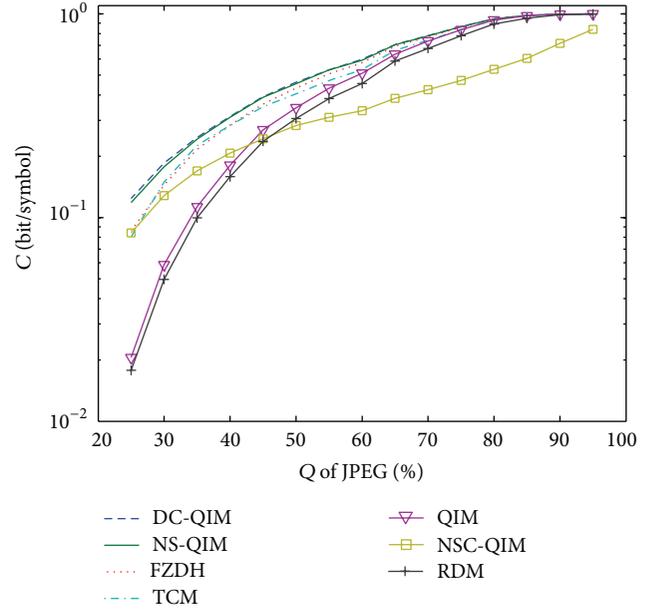


FIGURE 5: Capacity under JPEG for natural grayscale images.

features that are unique for the proposed approach and have not been discussed in the field of watermarking before.

We are proposing several criteria that will be used by the procedure to provide robustness against GA for NS-QIM. The criteria exploit nonsymmetric distribution inside embedding interval and help to recover a watermarked signal after the attack. It is presumed that a constant gain factor is applied to the watermarked signal (followed by AWGN) and the task is either to estimate the factor or the resulting length of embedding interval.

Let us denote the actual gain factor by λ and our guess about it by λ' . The length of the embedding interval (which is optimal for watermark extraction) is modified as a result of GA and is denoted by $\tilde{\Delta} = \lambda\Delta$. Our guess about $\tilde{\Delta}$ is $\tilde{\Delta}' = \lambda'\Delta$.

The core of the procedure of recovery after GA is the following. For each particular value $\tilde{\Delta}'$, noisy quantized samples c'_n are being projected on a single embedding interval:

$$x'_n = \begin{cases} c'_n \bmod \tilde{\Delta}', & \text{if } \left\lfloor \frac{c'_n - l^k}{\tilde{\Delta}'} \right\rfloor \bmod 2 = 0, \\ \tilde{\Delta}' - (c'_n \bmod \tilde{\Delta}'), & \text{otherwise.} \end{cases} \quad (51)$$

One of the following criteria is being applied to the random variable $X'_n \in [0, \tilde{\Delta}']$:

$$C_1(\tilde{\Delta}') = \left| \frac{\text{median}(X'_n)}{\tilde{\Delta}'} - 0.5 \right|, \quad (52)$$

$$C_2(\tilde{\Delta}') = \left| \frac{E([X'_n]^w)}{[\tilde{\Delta}']^w} \right|, \quad w = 2m + 1, \quad m \in \mathbb{N}.$$

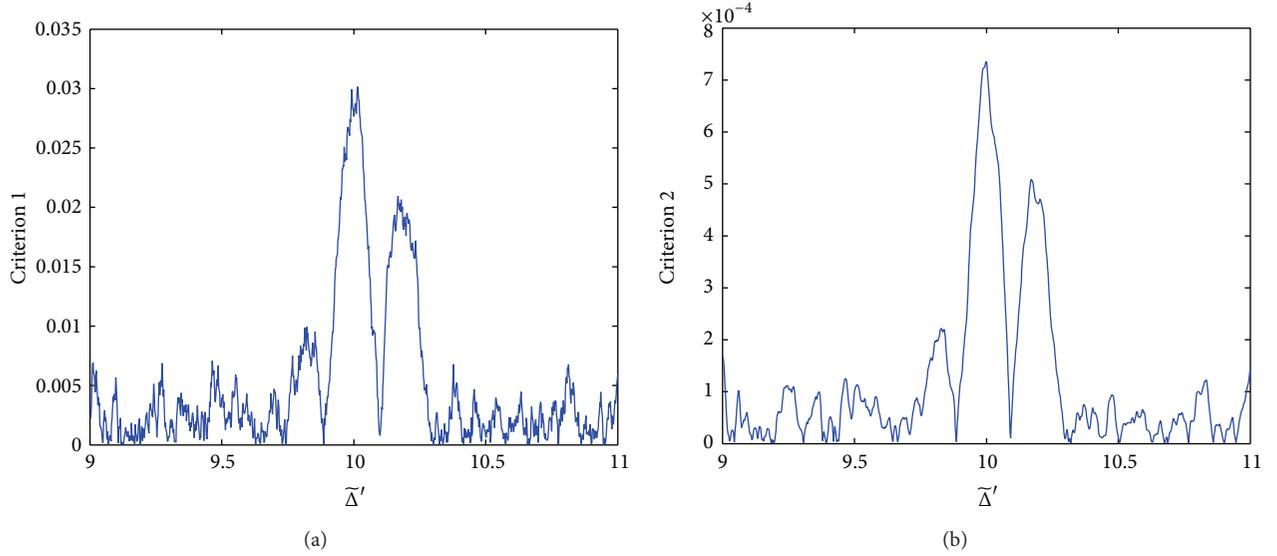


FIGURE 6: Plots of criteria values toward guessed length of embedding interval: (a) criterion C_1 ; (b) criterion C_2 .

The value of $\tilde{\Delta}''$ that maximizes one of the proposed criteria should be chosen as the best estimate of $\tilde{\Delta}$:

$$\tilde{\Delta}'' = \arg \max_{\tilde{\Delta}'} C_{1,2}(\tilde{\Delta}'). \quad (53)$$

The intuition behind the proposed procedure of recovery from GA is the following. The variance of the coefficients of the host signal is much larger than the length of embedding interval. Embedding intervals are placed next to each other without gaps and even small error in estimation of $\tilde{\Delta}$ results in considerable mismatch between positions of samples inside corresponding embedding intervals. In other words, wrong assumption about $\tilde{\Delta}$ makes distribution of X'_n very close to uniform. However, in case $\tilde{\Delta}'$ is close to $\tilde{\Delta}$ the distribution of X'_n demonstrates asymmetry because the distribution of quantized samples inside embedding interval (before GA is introduced) is indeed asymmetric. Hence, criteria C_1 and C_2 are just measures of asymmetry. The main advantage of the procedure is simplicity and low computational demand.

Experimental results demonstrate high level of accuracy of the proposed procedure of recovery after GA. Grayscale image Lena.tif with dimension 512×512 was used as a host signal for that purpose. A random watermark sequence was embedded into the largest singular values of SVD of 4×4 blocks using NS-QIM with $\alpha = 0.05$ and $\beta = 0.35$. The AWGN attack was applied after the embedding so that $\text{WNR} = -5$ dB. The length of embedding interval was 10. However we use notation $\tilde{\Delta} = 10$ because the value is not known to the receiver and during watermark extraction the proposed recovery procedure was used. The interval of initial guess was $\tilde{\Delta} \pm 10\%$ so that $\tilde{\Delta}' \in [9, 11]$. Such an initial guess reflects real needs for recovery after GA because a gain factor that is outside the range $0.9 \sim 1.1$ causes considerable visual distortions in most cases. The initial guess interval was split by equally spaced 1000 steps and for each step the recovery procedure was applied. The plots for values of C_1 and C_2 ,

$w = 5$, toward guessed values of $\tilde{\Delta}$, are shown in Figures 6(a) and 6(b), respectively.

Despite the fact that for the same Δ the difference between values of C_1 and C_2 is huge, the shapes of the plots are similar. The criteria reach their maximum at 10.042 and 9.998 for C_1 and C_2 , respectively, which are quite precise estimates of the actual Δ used during watermark embedding.

4.4. Performance for AWGN and JPEG Attacks with GA. The embedding constraints for the current experiment are the same as described in Section 4.2.1. Among the quantization methods used for comparison the only method robust to GA is RDM. Therefore, only RDM was used as a reference to NS-QIM and NSC-QIM under GA followed by AWGN and JPEG attacks, respectively. The exact information about Δ was not used for extraction in NS-QIM and NSC-QIM cases which is equivalent to GA with unknown scaling factor.

The watermark embedding domain was the same as in previous tests: first singular values of SVD of 4×4 blocks from 512×512 grayscale images were quantized, $\text{DWR} = 28$ dB. In case of RDM, the quantized value of a particular coefficient is based on the information about the last 100 previous coefficients. For NSC-QIM the parameters of embedding were $\alpha = 0.05$ and $\beta = 0.35$. For both AWGN and JPEG attacks the same as previously ranges of parameters were used.

However, during watermark extraction no information except initial guess interval $\Delta \pm 10\%$ was used in NS-QIM and NSC-QIM cases. Criterion C_1 was used for the estimation of actual Δ . Nonpermanent thresholding was applied to both modifications of the proposed watermarking method. In contrast to that RDM does use the exact information about quantization step. The resulting capacity toward AWGN variance is plotted for each method in Figure 7.

It can be seen from Figure 7 that both NS-QIM and NSC-QIM outperform RDM. The advantage of the proposed method is more evident for larger variance of the noise.

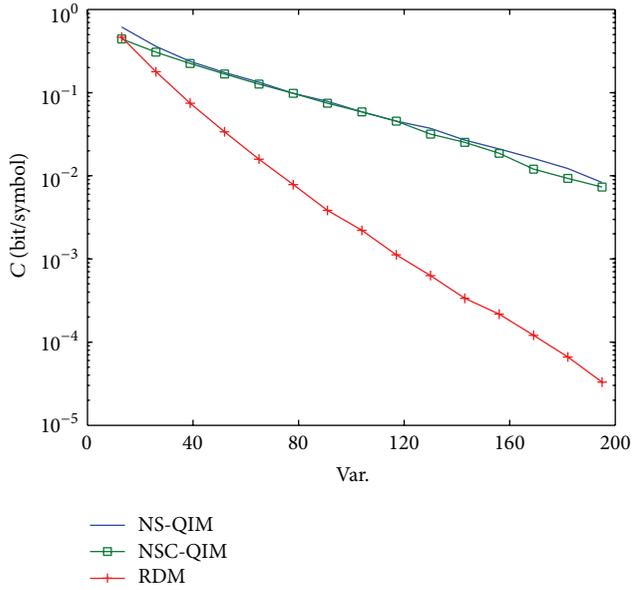


FIGURE 7: Capacity under GA followed by AWGN.

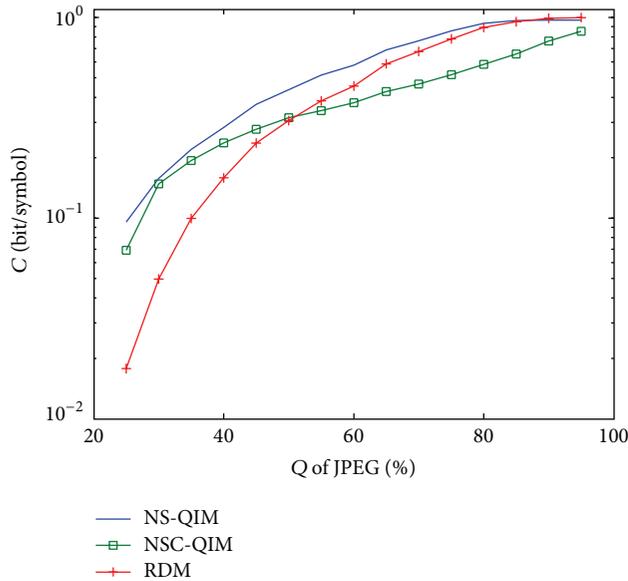


FIGURE 8: Capacity under GA followed by JPEG compression.

The capacity plots for NS-QIM, NSC-QIM, and RDM in case of JPEG attack are shown in Figure 8.

From Figure 8 we can conclude that both modifications of the proposed watermarking method supply higher capacity than RDM when $Q < 50\%$. However, only NS-QIM outperforms RDM in case $Q > 50\%$ and NSC-QIM performs worse than RDM for that range.

5. Discussion

In the experiment section we have estimated the capacity of the proposed method in both analytical and empirical

ways. Following both ways we can witness that the proposed method provides higher capacity compared to the other reference methods. In this section we are to discuss in more detail measures of watermarking efficiency, conditions of the experiments, and the reasons of superiority of NS-QIM-IDL.

Channel capacity C is one of the most important measures for watermarking as it indicates the maximum amount of the information that can be transmitted by a single embedded symbol [1, 12]. However, some authors in their original papers refer to error rates instead [13, 16, 19–21]. It can be demonstrated that calculations of C using error rates are straightforward [26]. Capacity can be calculated according to the following expression:

$$C = \max_{p_{em}(\sim b)} \left[p(\sim b, b) \log_2 \left(\frac{p(\sim b, b)}{p_{em}(\sim b) p_{ex}(b)} \right) + p(b, \sim b) \log_2 \left(\frac{p(b, \sim b)}{p_{em}(b) p_{ex}(\sim b)} \right) + p(\sim b, \sim b) \log_2 \left(\frac{p(\sim b, \sim b)}{p_{em}(\sim b) p_{ex}(\sim b)} \right) + p(b, b) \log_2 \left(\frac{p(b, b)}{p_{em}(b) p_{ex}(b)} \right) \right], \quad (54)$$

where, for instance, $p(\sim b, b)$ denotes joint probability of embedding symbol $\sim b$ and extracting symbol b ; $p_{em}(b)$ and $p_{ex}(b)$ denote probabilities of embedding and extracting of symbol b . Probabilities of extracting a particular symbol can be calculated using joint probabilities:

$$p_{ex}(b) = p(\sim b, b) + p(b, b), \quad (55)$$

$$p_{ex}(\sim b) = p(b, \sim b) + p(\sim b, \sim b).$$

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

$$p(\sim b, b) = p_{em}(\sim b) \text{BER}_{\sim b},$$

$$p(b, \sim b) = p_{em}(b) \text{BER}_b,$$

$$p(\sim b, \sim b) = p_{em}(\sim b) (1 - \text{BER}_{\sim b}),$$

$$p(b, b) = p_{em}(b) (1 - \text{BER}_b).$$

Embedding probabilities for the methods proposed in this paper are

$$p_{em}(\sim b) = \gamma_0 + \vartheta_0, \quad (57)$$

$$p_{em}(b) = \eta_1 + \varphi_1.$$

As a contrast to the watermarking approach proposed in this paper, the QIM-based methods known in the literature assume equal embedding probabilities and provide equal error rates for “0” and “1” [12, 19]. For all the mentioned in the experimental section methods (QIM, DC-QIM, RDA, FZDH, TCM, and the proposed methods) the results were collected under equal conditions of each kind of attack. In

order to compare efficiency of the proposed methods with some other state-of-the-art papers in watermarking [13, 21], their channel capacity can be calculated based on the data provided in those papers. From (54)–(56) we derive that QIM-based watermarking which has been presented in the literature capacity is

$$C = 1 + \text{BER} \log_2(\text{BER}) + (1 - \text{BER}) \log_2(1 - \text{BER}). \quad (58)$$

The largest singular values of SVD of 4×4 blocks were used by all the methods for watermark embedding in the empirical estimations of capacity. Such a domain is a natural choice for many watermarking applications because it provides a good tradeoff between robustness, invisibility, and data payload [7, 27, 28]. Commonly, the largest singular values are being quantized [25]. The robustness of a watermark embedded in the domain can be explained by a consideration that the largest singular values have a great importance. For example, compared to a set of the coefficients of discrete cosine transform (DCT) the set of singular values has more compact representation for the same size of a segment of an image [29]. At the same time the block size of 4×4 is enough to avoid some visible artefacts and this guarantees invisibility under DWR = 28 dB. The data payload of 1 bit per 16 pixels is sufficient for inclusion of important copyright information and for image size 512×512 provides capacity of 2 kB.

Among the reference (and state of the art) methods used for comparison no one performs better than the proposed watermarking methods simultaneously under both AWGN and GA. Hence, the proposed methods fill the gap existing in watermarking literature. This is thanks to several new advancements used for embedding and extraction of a watermark.

In the case when AWGN is applied at the absence of GA the benefit is caused mostly by IDL and the kind of thresholding during watermark extraction. From Figure 3 it can be noticed that even without IDL variant NS-QIM delivers slightly higher capacity under low WNRs compared to DC-QIM. However, the capacity rises dramatically for low WNRs if we switch to NS-QIM-IDL. It is remarkable that the form of capacity plot in the latter case does not inherit the steepness demonstrated by the other methods. Instead, the plot shape is similar to CTL but is placed at a lower position. The explanation of such phenomena is in the quantization process. According to IDL we refuse to modify samples whose quantization brings the highest embedding distortion. In case these samples are quantized they are placed closer to the threshold which separates “0” and “1.” Therefore the information interpreted by these samples is the most likely to be lost under low WNRs. Predicting the loss of information we might accept that fact and introduce IDL instead. It is a kind of “accumulation” of embedding distortion which can be “spent” on making the rest of embedded information more robust. Another unique feature is the proposed way of nonpermanent thresholding. In contrast to the permanent thresholding the information about α, β is not required for watermark extraction. Hence, during embedding these parameters can be adjusted to deliver higher capacity even in case there is no way to communicate new parameters to the receiver.

The proposed method is in advantageous position compared to RDM in the case when GA is used to attack the watermarked image. As one of its stages, GA assumes AWGN and this explains superiority of NS-QIM over RDM in general. The success of recovery is due to easy and efficient procedure that utilizes a unique feature introduced by the proposed methods. The feature is created during quantization and is a result of different quantization rules for “0” and “1.”

The proposed estimation of scaling factor in this paper has some advantages compared to other known retrieving procedures. For instance, a model of a host is used in [15] to estimate the scaling factor. In contrast to that we exploit the unique asymmetric feature of the proposed quantization approach and this feature is not dependent on a host. The only important assumption about the host is that its variance is much larger than the size of embedding interval. As soon as this holds the estimation is not dependent on the model of the host which is a contrast to [15]. Also, our recovery procedure does not use any additional information except interval guess for $\tilde{\Delta}$, which can be given roughly. These improvements imply more efficient retrieval after GA which in addition requires fewer samples.

The nonpermanent thresholding was proposed with the aim to avoid transmitting any additional information to the receiver. For example, different size of embedding interval Δ and different parameters α, β can be used to watermark different images. Nevertheless, a watermark can be extracted in case the recovery procedure and nonpermanent thresholding are used. Such feature might be beneficial in adaptation to the conditions that change.

In the paper we do not consider a constant offset attack. In some other papers like [12, 14, 19] it is assumed to be applied in conjunction with GA. Further modifications of the proposed recovery procedure are needed to cope with it. Also, another criterion that exploits different features compared C_1 and C_2 might be useful for that task. Apart from this goal we would like to experiment with other concepts of IDL. For example, it might be reasonable to allow for those samples to be shifted during quantization procedure. Such shifts may increase chances for those samples to be interpreted correctly after an attack is applied.

6. Conclusions

The new watermarking method based on scalar QIM has been proposed. It provides higher capacity under different kinds of attacks compared to other existing methods. The proposed NS-QIM-IDL method is the most beneficial in case of GA and AWGN. The advantages of the method are due to its unique approach to watermark embedding as well as a new procedure of recovery and extraction.

The main features of the unique approach to watermark embedding are a new kind of distribution of quantized samples and IDL. In general there is no line of symmetry inside embedding interval for the new distribution of quantized samples. This feature is used to recover a watermark after GA. The feature of IDL can reduce distortions introduced to a host signal which are caused by watermarking. This is done by letting some watermark bits to be interpreted

incorrectly at the initial phase of embedding and before any attack occurs. The proposed IDL is extremely beneficial for low WNRs under AWGN attack.

The new procedure of recovery after GA exploits the nonsymmetric distribution of quantized samples. One out of two different criteria might be chosen to serve as a goal function for the procedure. The criteria behave in a similar way despite the differences in realization. It has been demonstrated experimentally that the proposed recovery procedure estimates the original length of embedding interval with deviation of 0.02% even in case when WNR is quite low. Nonpermanent thresholding was proposed in order to avoid transmitting additional information to the site where watermark extraction is done. The technique is simple and establishes the threshold in the position of the median of the distribution inside embedding interval.

The mentioned advancements implied considerable performance improvement. Under conditions of AWGN and JPEG attacks (at the absence of GA) the capacity of the proposed method is at the same or higher level compared to DC-QIM. The most advantageous application of NS-QIM-IDL is under AWGN for WNRs around -12 dB where it performs up to 10^4 times better than DC-QIM. Under the condition of GA followed by high level of AWGN the performance of the proposed method is up to 10^3 times higher than that of RDM. For the case when GA is followed by JPEG with $Q = 25\%$ the capacity of the proposed method is up to 10 times higher than that of RDM. Superiority of the proposed methods under AWGN as well as GA allows narrowing the gap between watermarking performances achievable in theory and in practice.

Conflict of Interests

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

References

- [1] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, *Digital Watermarking and Steganography*, Morgan Kaufmann, San Francisco, Calif, USA, 2nd edition, 2007.
- [2] M. Barni, F. Bartolini, V. Cappellini, and A. Piva, "Robust watermarking of still images for copyright protection," in *Proceedings of the 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] T. Chen, "A framework for optimal blind watermark detection," in *Proceedings of the 2001 Workshop on Multimedia and Security: New Challenges*, pp. 11–14, Ottawa, Canada, 2001.
- [5] M. H. M. Costa, "Writing on dirty paper," *IEEE Transactions on Information Theory*, vol. 29, no. 3, pp. 439–441, 1983.
- [6] E. Ganic and A. M. Eskicioglu, "Robust DWT-SVD domain image watermarking: embedding data in all frequencies," in *Proceedings of the Multimedia and Security Workshop (MM & Sec '04)*, pp. 166–174, September 2004.
- [7] K. Loukhaoukha, "Image watermarking algorithm based on multiobjective ant colony optimization and singular value decomposition in wavelet domain," *Journal of Optimization*, vol. 2013, Article ID 921270, 10 pages, 2013.
- [8] B. Chen and G. 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, April 1999.
- [9] 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.
- [10] E. Esen and A. Alatan, "Forbidden zone data hiding," in *Proceedings of the IEEE International Conference on Image Processing*, pp. 1393–1396, October 2006.
- [11] M. Ramkumar and A. N. Akansu, "Signalling methods for multimedia steganography," *IEEE Transactions on Signal Processing*, vol. 52, no. 4, pp. 1100–1111, 2004.
- [12] 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.
- [13] J. Oostveen, T. Kalker, and M. Staring, "Adaptive quantization watermarking," in *Security, Steganography, and Watermarking of Multimedia*, Proceedings of SPIE, pp. 296–303, San Jose, Calif, USA, January 2004.
- [14] 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.
- [15] 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.
- [16] 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.
- [17] 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)*, pp. 797–800, March 2005.
- [18] M. Zareian and H. Tohidypour, "Robust quantisation index modulation-based approach for image watermarking," *IET Image Processing*, vol. 7, no. 5, pp. 432–441, 2013.
- [19] 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.
- [20] M. A. Akhaee, S. M. E. Sahraeian, and C. Jin, "Blind image watermarking using a sample projection approach," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 883–893, 2011.
- [21] N. K. Kalantari and S. M. Ahadi, "A logarithmic quantization index modulation for perceptually better data hiding," *IEEE Transactions on Image Processing*, vol. 19, no. 6, pp. 1504–1517, 2010.
- [22] E. Nezhadarya, J. Wang, and R. K. Ward, "A new data hiding method using angle quantization index modulation in gradient domain," in *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '11)*, pp. 2440–2443, Prague, Czech Republic, May 2011.

- [23] M. Zareian and A. Daneshkhah, "Adaptive angle quantization index modulation for robust image watermarking," in *Proceedings of the IEEE Global Communications Conference (GLOBECOM '12)*, pp. 881–884, Anaheim, Calif, USA, December 2012.
- [24] C. Song, S. Sudirman, M. Merabti, and D. Llewellyn-Jones, "Analysis of digital image watermark attacks," in *Proceeding of the 7th IEEE Consumer Communications and Networking Conference (CCNC '10)*, pp. 1–5, Las Vegas, Nev, USA, January 2010.
- [25] V. Gorodetski, L. Popyack, V. Samoilov, and V. Skormin, "SVD-based approach to transparent embedding data into digital images," in *Proceedings of the International Workshop on Information Assurance in Computer Networks: Methods, Models, and Architectures for Network Security (MMM-ACNS '01)*, pp. 263–274, 2001.
- [26] R. Gallager, *Information Theory and Reliable Communication*, John Wiley & Sons, New York, NY, USA, 1968.
- [27] 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 and PCS '13)*, pp. 184–192, Nangang, China, March 2013.
- [28] Y. Zolotavkin and M. Juhola, "SVD-based digital image watermarking on approximated orthogonal matrix," in *Proceedings of the 10th International Conference on Security and Cryptography (SECRYPT '13)*, pp. 321–330, July 2013.
- [29] X. Jun and W. Ying, "Toward a better understanding of DCT coefficients in watermarking," in *Proceedings of The Pacific-Asia Workshop on Computational Intelligence and Industrial Application (PACIIA '08)*, vol. 2, pp. 206–209, Wuhan, China, December 2008.



Hindawi

Submit your manuscripts at
<http://www.hindawi.com>

