Multiple Description Watermarking Based on Quantization Index Modulus Modulation*

MIIN-LUEN DAY+,1, SUH-YIN LEE+ AND I-CHANG JOU2

+*Department of Computer Science and Information Engineering*
National Chiao Tung University
Hsinchu, 300 Taiwan
E-mail: sylee@csie.nctu.edu.tw
1*Telecommunication Laboratory*
Chunghwa Telecom Co., Ltd.
Chungli, 320 Taiwan
E-mail: day@cht.com.tw
2*Department of Computer and Communication Engineering*
National Kaohsiung First University of Science and Technology
Kaohsiung, 811 Taiwan
E-mail: icjou@ccms.nkfust.edu.tw

In this paper, we study the problem of watermarking for error-prone transmission over unreliable network. We try to integrate an oblivious quantization index modulus modulation (QIMM) watermarking technique into the multiple description coding (MDC) framework and we call it multiple description watermarking technique (MDW). It is known that the balanced MDC encodes a signal source into multiple bitstreams (descriptions) of equal importance and equal data rate. Consider a traditional two-description case in a packet transmission network. The computation for watermark embedding is performed using either description. Once chosen, the corresponding values to be modulated for the other description are assigned with the same values as the just watermarked description. In the detection process, the embedded watermark could be extracted no matter either one or both descriptions are received. That is to say, the watermark is still detectable from MDW even with 50% packet loss. Furthermore, in the case of 50% packet loss, the resulting watermark from MDW is still robust to a variety of image processing attacks, including DCT based compression (JPEG), DWT based compression (JPEG-2000), Gaussian filtering, sharpening and median filtering. The experimental results confirmed the competitive performance and the effectiveness of the proposed scheme.

Keywords: error-prone, multiple description, watermarking, QIMM, MDW

1. INTRODUCTION

Watermarking is a technique to hide data or information imperceptibly within image, audio or video so that valuable contents can be protected. There are two commonly used categories of watermarking techniques in the literature: one is spread spectrum approach, and the other is quantization approach. Cox *et al.* [1] proposed an image watermarking method based on spread spectrum theory, which shows good performance in terms of invisibility and robustness to signal processing operations and common geometric trans-

Received September 22, 2005; revised January 9 & March 9, 2006; accepted April 10, 2006.
Communicated by Pau-Choo Chung.

[*] Part of the paper has been presented in the 14th CVGIP Conference on Computer Vision, Graphics and Image Processing.

formations. However, the main drawback of their approach is that both the original image and the watermark are needed in the detection process. On the other hand, the capacity of their watermark is low, since the detector can only tell whether the watermark exists or not. Therefore it is still not convincing enough for the third party to prove the rightful ownership.

Contrast to the low capacity problem inherent in the spread spectrum based watermarking techniques [1-3], the quantization based watermarking techniques [4, 5] normally have relatively high capacity. Chen and Wornell [4] presented a quantization index modulation (QIM) scheme based on the concept of dither modulation, which uses the watermark information as an index to select a dither signal. The dither signal is then added to the host signal, and a least distorted quantizer is then selected from a set of possible quantizers. The dithered host signal is quantized using this selected quantizer and finally the dither signal is subtracted from the quantized signal to form a watermarked value:

$$s(x; m) = Q(x + d(m)) - d(m), \tag{1}$$

where x is the host signal, $d(m)$ is the dither signal representing watermark message m (one bit of information), $Q(.)$ denotes the selected quantizer and $s(x; m)$ is corresponding to the host signal embedded with watermark message m. In the detection process, different dither signal representing watermark message is added to the received signal using Eq. (1), and the index (m = 0 or 1) of dither signal is the extracted watermark information. The detected index m^* is chosen so that it gives the minimum distance between the received signal (x') and its closest quantized signal.

$$m^* = \arg\min_{m} \|x' - s(x'; m)\| \tag{2}$$

In the literature, watermarking techniques have been extensively discussed, but few of them explored watermarking for wireless transmission. Hartung and Hamme [6] pointed out that as second-generation and third-generation (3G) mobile networks progress, digital media distribution for mobile E-commerce will eventually evolve into a huge business. The watermarking-related applications such as media identification and copy control are getting more and more feasible for mobile E-commerce. Knowing the error prone nature of wireless communications, Checcacci *et al.* [7] proposed a robust MPEG-4 watermarking technique for video sequences corrupted with errors. Chandramouli *et al.* [8] proposed a multiple description framework for oblivious watermarking. Among the multiple descriptions, one is used to embed watermark information and another for referential original image to assist detection. That is to say, the embedded watermark cannot be extracted without receiving both descriptions. Under these circumstances, it is not suitable for error-prone packet transmission network applications.

Multiple description coding (MDC) [9-13] is different from layered coding, simulcast coding, or even error resilient tools described in MPEG-4 [14]. On a wireless multihop network or a packet-switched network, several parallel channels do exist between the source and the destination and each channel may be temporarily down or suffering from long burst errors. The design philosophy of MDC scheme is that the quality of the decoded signal is acceptable when receiving only one description, and the signal can be further improved as more descriptions are received. In this paper, we propose a multiple description watermarking scheme based on oblivious quantization index modulus modulation (QIMM) watermarking technique together with the MDC framework. Consider a traditional two-description case here. The watermark is embedded in either description and can be extracted even when only one description is received. The reason of proposing the above approach is that we want to make sure a high enough watermark payload can be embedded into an images. In the meanwhile, the proposed MDW (multiple description watermarking) is robust to error-prone transmission and incidental data managing attacks. In the next section, the MDC and the proposed QIMM watermarking technique are introduced, while the proposed MDW technique is presented in section 3. In section 4 experimental results are presented. The concluding remarks are drawn in section 5.

2. MULTIPLE DESCRIPTION CODING (MDC) AND QUANTIZATION INDEX MODULUS MODULATION (QIMM)

In this section we describe the components of proposed multiple description watermarking technique. The MDC approach which was proposed in [12, 13] is described first. Then we shall present the proposed QIMM watermarking technique.

2.1 The MDC Approach [12, 13]

The MDC-based wavelet based coding was proposed by Survetto *et al.* [12]. The two-description architecture of MDC [12, 13] is illustrated in Fig. 1. The major contribution of the MDC scheme is its capability on receiving satisfactory data quality even if part of the channels is broken. As shown in Fig. 1, the quality of a decoded signal is usually acceptable if either receiver 1 or receiver 2 receives the correct signal. Furthermore, the quality of a received signal can be better if both receivers function normally. The most crucial component of an MDC scheme is its multiple description scalar quantizer. It consists of a scalar quantizer, which quantizes continuous sample values to smaller countable integers, and an index assignment counter. The source input signal $x \in X$ is first scalar quantized to $x_Q \in X_Q$. The function of the index assignment component f: $x_Q \rightarrow (x_1, x_2)$ is to split a quantized coefficient x_Q into two complementary and possibly redundant smaller coefficients $x_1 \in X_1$ and $x_2 \in X_2$, so that each of these two small coefficients only needs lower bit rate to describe and both could be recombined later to recover the original quantized coefficient. That is, with the reception of two description values, a perfect reconstructed value $\hat{x}_0 = x_Q$ can be achieved by using $\hat{x}_0 = f^{-1}(x_1, x_2)$. When only one description value is received, an acceptable estimated value $\hat{x}_d$ ($|\hat{x}_d| \prec |x_Q|$) can be obtained through $\hat{x}_d = f^{-1}(x_d)$, where $d = 1, 2$.

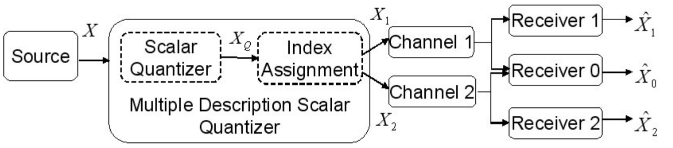


Fig. 1. The flowchart of multiple description coding scheme [12, 13].

To better explain the concept, we use an example to discuss the approach. A quantized coefficient x_Q valued 120 is split into the ordered pair $(x_1, x_2) = (39, 40)$, where 39 and 40 are the values assigned to description 1 and 2, respectively. On receiving two descriptions, a perfect recovered value $\hat{x} = \hat{x}_0 = x_Q = 120$ can be achieved by central decoder. When receiving only description 1 for the transmitted value 120, the estimated $\hat{x} = \hat{x}_1$ using $x_1 = 39$ will be 118, while receiving only description 2, the estimated $\hat{x} = \hat{x}_2$ using $x_2 = 40$ will be 121. As can be seen from this example, the central decoder should be more robust against various attacks than the side decoder since the reconstructed value received from central decoder is the same as the watermarked value before transmission. The detailed algorithm for index assignment can be found in [12, 13].

2.2 QIMM

In this section, we shall describe in detail how the proposed oblivious quantization index modulus modulation scheme functions. The proposed QIMM approach selects some of wavelet coefficients as the original host signal. Then the index of each quantized coefficient is modulated for embedding one bit of information. The embedding and detection processes are described as follows.

2.2.1 The embedding process of QIMM

The original host signal $X = \{x_1, x_2, \ldots, x_n\}$ is first divided by the quantization step size (δ), and a nearest integer index value is obtained by a round function. The quantized index value is then executed with modulo 2 to get the residue with value 0 or 1. If the residue is equal to the watermark message bit, then the watermarked value is the reconstruction point of quantized host signal. Otherwise, the biased (either + 1 or – 1) quantized index value is used to calculate the watermark value $X' = \{x_1', x_2', \ldots, x_n'\}$. To embed one bit of watermark message m, the embedding algorithm consists of the following steps:

Step 1: Take $Q(x_i) = Round(x_i/\delta)$.
Step 2: If $(Q(x_i) \bmod 2) = m$ then

$$x_i' = s(x_i; m) = Q(x_i) * \delta, \tag{3}$$

else

$$x_i' = s(x_i; m) = \arg\min_{P(x_i)}(P(x_i) - x_i), \tag{4}$$

where $P(x_i)$ in Eq. (4) is either $(Q(x_i) - 1) * \delta$ or $(Q(x_i) + 1) * \delta$, and $s(x_i; m)$ is the ith host signal embedded with watermark message m. The criterion of selecting either $(Q(x_i) - 1) * \delta$ or $(Q(x_i) + 1) * \delta$ depends on which one has less distortion with respect to x_i. The one with less distortion is used to reconstruct the watermarked signal x_i'. The difference between QIM and QIMM is compared and elaborated as follows.

We observe that low embedding distortion (q) leads to low degree of robustness. For QIM embedding with quantization step size δ_{QIM}, the embedding distortion (q) range is $\left[-\frac{\delta_{QIM}}{2}, \frac{\delta_{QIM}}{2}\right]$ and the detection robustness range is $\left[-\frac{\delta_{QIM}}{2}, \frac{\delta_{QIM}}{2}\right]$ too. If the host signal X is uniform, the mean squared error distortion (MSE) of embedding is the second moment of a random variable uniformly distributed in the interval $\left[-\frac{\delta_{QIM}}{2}, \frac{\delta_{QIM}}{2}\right]$:

$$MSE_{QIM} = \frac{1}{\delta_{QIM}} \int_{-\frac{\delta_{QIM}}{2}}^{\frac{\delta_{QIM}}{2}} q^2 dq = \frac{\delta_{QIM}^2}{12}. \tag{5}$$

As for QIMM embedding with quantization step size δ_{QIMM}, the embedding distortion (q) range is [$-\ \delta_{QIMM}$, δ_{QIMM}] and the detection robustness range is [$-\ \delta_{QIMM}$, δ_{QIMM}] too. The mean squared distortion (MSE) of embedding is:

$$MSE_{QIMM} = \frac{1}{2\delta_{QIMM}} \int_{-\delta_{QIMM}}^{\delta_{QIMM}} q^2 dq = \frac{\delta_{QIMM}^2}{3}. \tag{6}$$

It is expected that by setting $\delta_{QIM} = 2\delta_{QIMM}$, QIM and QIMM should obtain similar embedding distortion and detection robustness.

To better illustrate the Delta-Distortion relationship of QIM and QIMM, we performed Monte Carlo simulations with host signal X drawn from 1,000 samples of a Gaussian zero-mean random variable with variance σ_X^2 ranging from 2500 to 14400. Figs. 2 (a) and (c) both show the MSE distortion under various embedding quantization step sizes ranging from 5 to 50 for QIM and QIMM, while Figs. 2 (b) and (d) show the MSE distortion under various embedding quantization step sizes ranging from 5 to 50 for QIMM and 10 to 100 for QIM, respectively. As we can see from Figs. 2 (b) and (d), to get the same distortion for QIM and QIMM, the embedding quantization step size δ_{QIM} of QIM is almost equal to two times of δ_{QIMM} of QIMM.

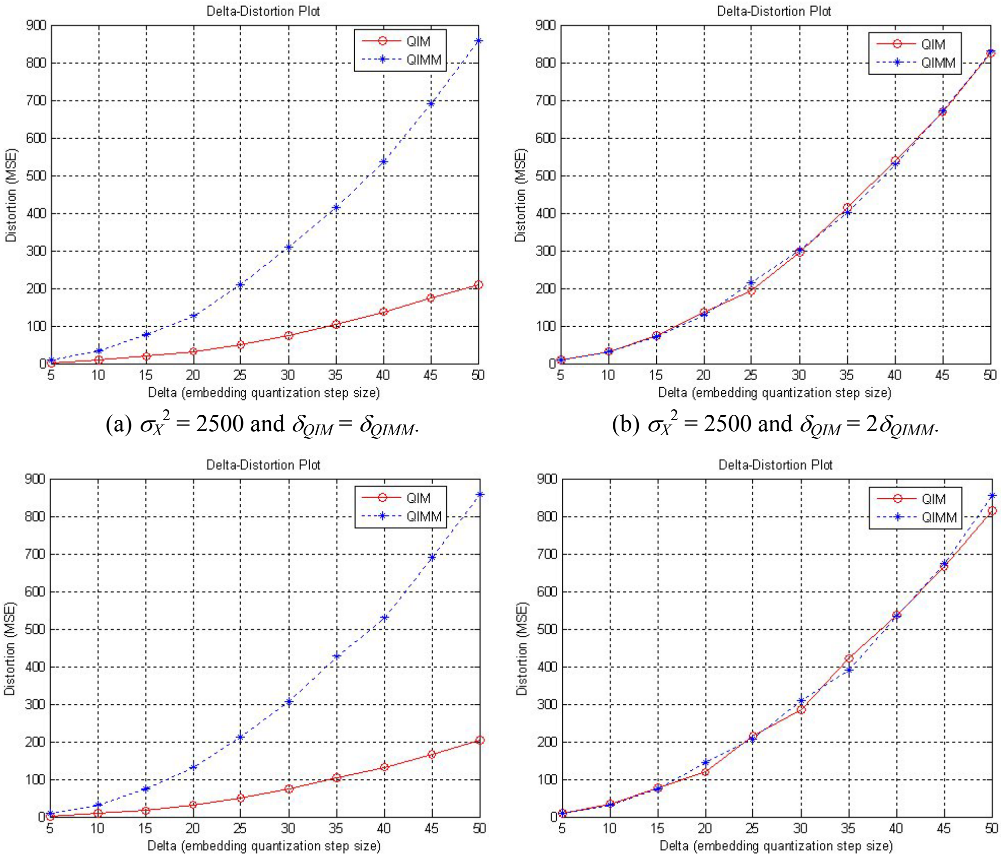
2.2.2 The detection process of QIMM

After receiving the watermarked signal X', the attacked watermarked signal X'' is also divided by the quantization step size, so that a nearest integer index value is obtained by a round function. The quantized index value is then taken modulo 2 to get the extracted watermark message bit m^*. The detection algorithm consists of the following steps:

Step 1: $Q(x_i'') = \text{Round}(x_i''/\delta)$.
Step 2: $m^* = Q(x_i'') \bmod 2$.

In section 2.2.1, we have shown that by setting $\delta_{QIM} = 2\delta_{QIMM}$, QIM and QIMM have obtained similar embedding distortion. In this section, we demonstrate that by setting $\delta_{QIM} = 2\delta_{QIMM}$, QIM and QIMM obtain the similar detection robustness as follows. To evaluate the reliability (robustness) of watermark detection, the correlation ratio ρ was defined as:

$$\rho = \frac{\text{Total number of correctly detected bits}}{\text{Total number of embedded bits}}. \tag{7}$$



(a) $\sigma_X^2 = 2500$ and $\delta_{QIM} = \delta_{QIMM}$. (b) $\sigma_X^2 = 2500$ and $\delta_{QIM} = 2\delta_{QIMM}$.

(c) $\sigma_X^2 = 14400$ and $\delta_{QIM} = \delta_{QIMM}$. (d) $\sigma_X^2 = 14400$ and $\delta_{QIM} = 2\delta_{QIMM}$.

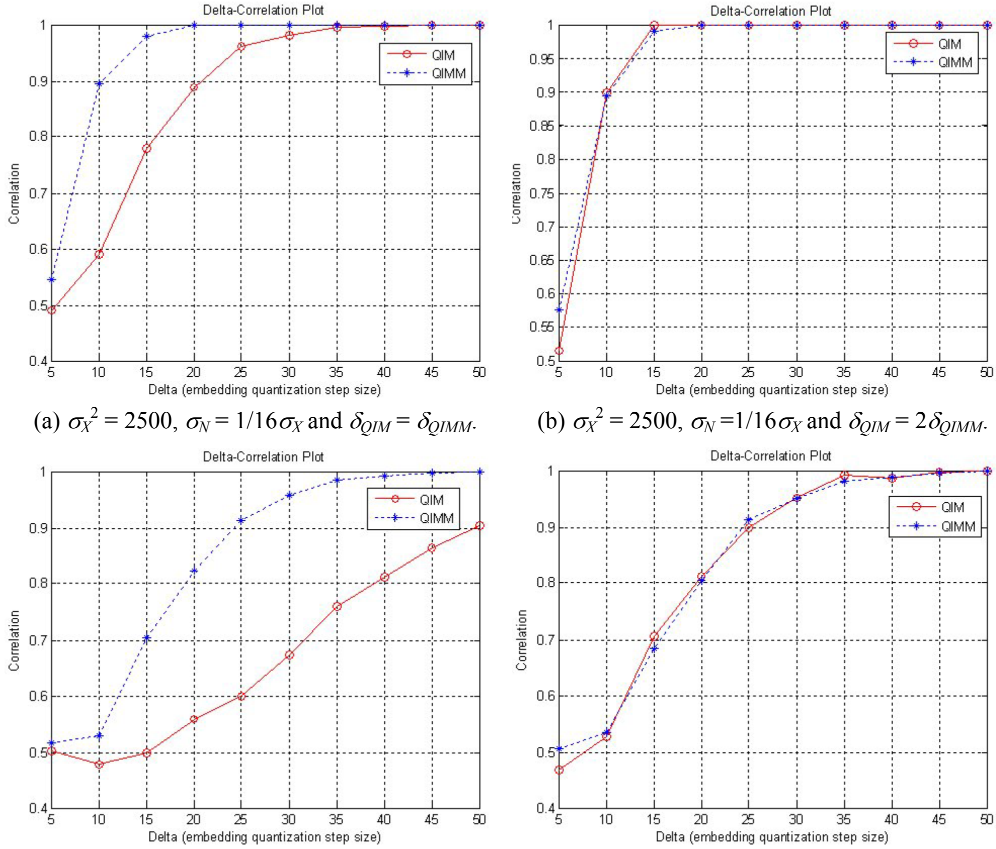
Fig. 2. The delta-distortion curve of QIM and QIMM.

A higher value of ρ indicated a more reliable detection. The perfect recognition rate can be achieved when the value of ρ equals 1.

Following the same scenario as in section 2.2.1, we performed Monte Carlo simulations with host signal X drawn from 1,000 samples of a Gaussian zero-mean random variable with variance σ_X^2 ranging from 2500 to 14400. Moreover, a noise signal N drawn from 1,000 samples of a Gaussian zero-mean random variable with standard deviation $\sigma_N = \frac{1}{16}\sigma_X$ is employed to simulate the various attacks.

Each sample of signal X was used to embed one bit of watermark information under various embedding quantization step sizes, where totally 1,000 bits were embedded for each specific quantization step size. The watermarked signal X' is attacked with noise signal N via $X'' = X' + N$ (a similar results can be obtained via $X'' = X' - N$) before detection.

As can be seen from Figs. 3 (a-d), smaller embedding quantization step sizes leads to lower degree of robustness for both QIM and QIMM. Figs. 3 (a) and (c) both show the correlation ratio under various embedding quantization step sizes ranging from 5 to 50



(a) $\sigma_X^2 = 2500$, $\sigma_N = 1/16\sigma_X$ and $\delta_{QIM} = \delta_{QIMM}$.

(b) $\sigma_X^2 = 2500$, $\sigma_N = 1/16\sigma_X$ and $\delta_{QIM} = 2\delta_{QIMM}$.

(c) $\sigma_X^2 = 14400$, $\sigma_N = 1/16\sigma_X$ and $\delta_{QIM} = \delta_{QIMM}$.

(d) $\sigma_X^2 = 14400$, $\sigma_N = 1/16\sigma_X$ and $\delta_{QIM} = 2\delta_{QIMM}$.

Fig. 3. The delta-correlation curve of QIM and QIMM.

for QIM and QIMM, while Figs. 3 (b) and (d) show the correlation ratio under various embedding quantization step sizes ranging from 5 to 50 for QIMM and 10 to 100 for QIM, respectively. As we can see from Figs. 2 (a, c) and Figs. 3 (a, c), though the MSE of QIM is lower than that of QIMM, the robustness of QIM is inferior to that of QIMM. In contrast, as seen from Figs. 2 (b, d) and Figs. 3 (b, d), under the same MSE condition, the robustness of QIM is almost equal to that of QIMM.

As the QIM scheme [4] has been proven to be nearly optimal with respect to the tradeoff among embedding distortion, detection robustness and hiding capacity, we do not expect that QIMM can outperform QIM in the scalar-based case. Rather, we intend to explore this topic from different perspective. Since for watermark embedding based on scalar quantization, focus can not be put solely on distortion introduced by embedding, as the accompanied robustness should also be taken into consideration. Robustness should be compared on the ground of the same distortion. Furthermore, by understanding QIMM as generalized LSB with delta value larger than 2, the concept is better grasped and more accessible to most readers, and leads to less implementation effort than that of the dithering concept of QIM.

3. THE PROPOSED MULTIPLE DESCRIPTION WATERMARKING (MDW) SCHEME

In this section, a multiple description watermarking technique using both MDC and QIMM is described. The design goal of the MDW scheme is to embed in one description a watermark, which can be detected from either one of the multiple descriptions. The advantage of the proposed scheme is two-fold. First, it can increase the detection robustness for error-prone transmission over unreliable network. Second, it is able to increase the capacity while preserving the transparency. This is achieved by modulating the selected coefficients of either description appropriately so that one bit of information can be embedded.

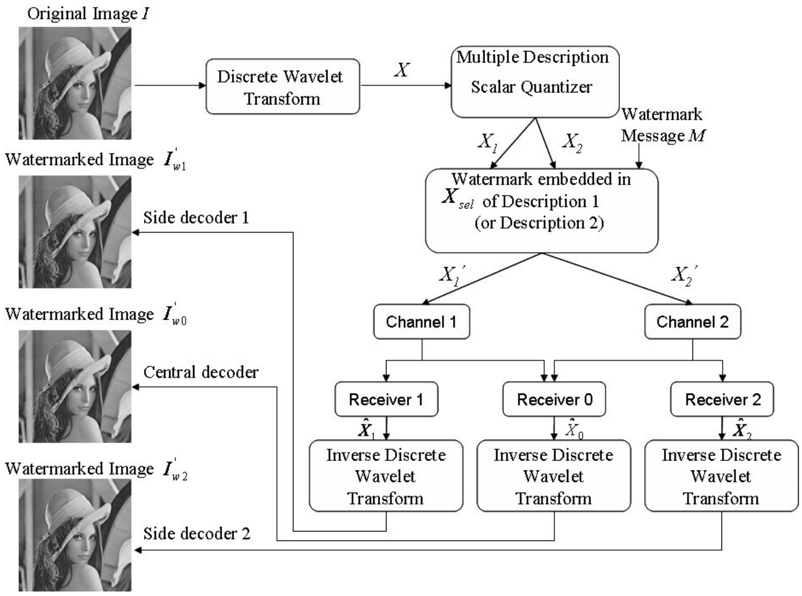

Original Image I
Discrete Wavelet Transform
X
Multiple Description Scalar Quantizer
Watermark Message M
X_1
X_2
Watermarked Image I'_{w1}
Watermark embedded in X_{sel} of Description 1 (or Description 2)
Side decoder 1
X_1'
X_2'
Watermarked Image I'_{w0}
Channel 1
Channel 2
Central decoder
Receiver 1
Receiver 0
Receiver 2
$\hat{X}_1$
$\hat{X}_0$
$\hat{X}_2$
Watermarked Image I'_{w2}
Inverse Discrete Wavelet Transform
Inverse Discrete Wavelet Transform
Inverse Discrete Wavelet Transform
Side decoder 2

Fig. 4. The flow of proposed multiple description watermark embedding scheme for error-prone transmission over unreliable network.

Fig. 4 shows the flow of MDW, which is composed of a watermark embedding process and a transmission process. The original image is first transformed into the discrete wavelet domain. The transformed coefficients are then processed by multiple description scalar quantizer (MDSQ) to generate two independent descriptions, X_1 and X_2. Next, a bit (m) of the watermark message M is embedded in some of the selected coefficients from one of the descriptions using QIMM. During the watermark embedding process, whenever each of the selected coefficients is modulated by the watermarking embedding rule, the corresponding coefficient of the other un-watermarked description (say description 2) is also replaced with the same value. Each of the watermarked bitstream is then sent through one independent channel. The watermarked images (I'_{w1} from side decoder 1, I'_{w2} from side decoder 2 or I'_{w0} from central decoder) could then be obtained by receiving either one description (receiver 1 $(\widehat{X}_1)$ or receiver 2 $(\widehat{X}_2)$) or two

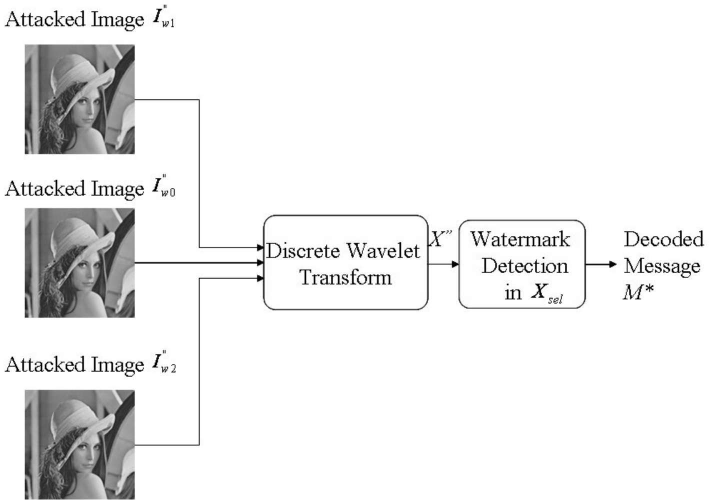

Attacked Image I^{*}_{w1}
Attacked Image I^{*}_{w0}
Attacked Image I^{*}_{w2}
Discrete Wavelet Transform
X''
Watermark Detection in X_{sel}
Decoded Message M^{*}

Fig. 5. The flow of proposed multiple description watermark detection scheme.

descriptions (receiver $0\,(\hat{X}_0)$) and inversing the Discrete Wavelet transforms. In the detection process in Fig. 5, the attacked image I''_{wr} (r = 0, 1 or 2) first goes through Discrete Wavelet transform, and some of the selected coefficients are then used to extract the embedded watermark message M^{*}.

The proposed scheme is completely different from that of [8], where two-description design is adopted as well. In contrast to [8], the value pairs of these two descriptions in our scheme are almost with the same value. When the watermark embedding process is executed, one only needs to consider one description. Whenever a coefficient of one description is modulated using watermark embedding rules, the corresponding coefficient of the other description is set to the same value. The time complexity is reduced because watermarking one description implies watermarking another description at the same time. The good characteristics of our proposed MDW results from the design nature of the index assignment function. Moreover, the MDW can detect watermark no matter either one or two descriptions are received. This means in an error-prone packet transmission network, the watermark can still be detected even with 50% packet loss rate.

3.1 Embedding and Transmission Process of MDW

To embed n bits of watermark message M into image I, the algorithm is described as follows:

(1) The original image I is decomposed into 13-subbands using the 4-level octave band wavelet transform.
(2) Each of the subband coefficients are quantized by a uniform scalar quantizer.
(3) Two descriptions (X_1, X_2) of the quantized coefficient are created by mapping each quantized coefficient to a pair of numbers by the index assignment component.
(4) Select the coefficients on LL band of description 1 (or 2) for watermark embedding, namely $X_{sel} = \{x_1, x_2, \ldots, x_n\}$.

(5) Apply embedding process of QIMM on X_{sel} to embed watermark message M.
(6) Replace the corresponding coefficients of un-watermarked description 2 (or 1) with the same values as those embedded in description 1 (or 2).
(7) Transmit these two watermarked descriptions over network via two different channels.
(8) Apply inverse transform to obtain watermarked image I'_{wr} (r = 0, 1 or 2) depending on received descriptions $\widehat{X}_r$ (r = 0, 1 or 2).

3.2 Detection Process of MDW

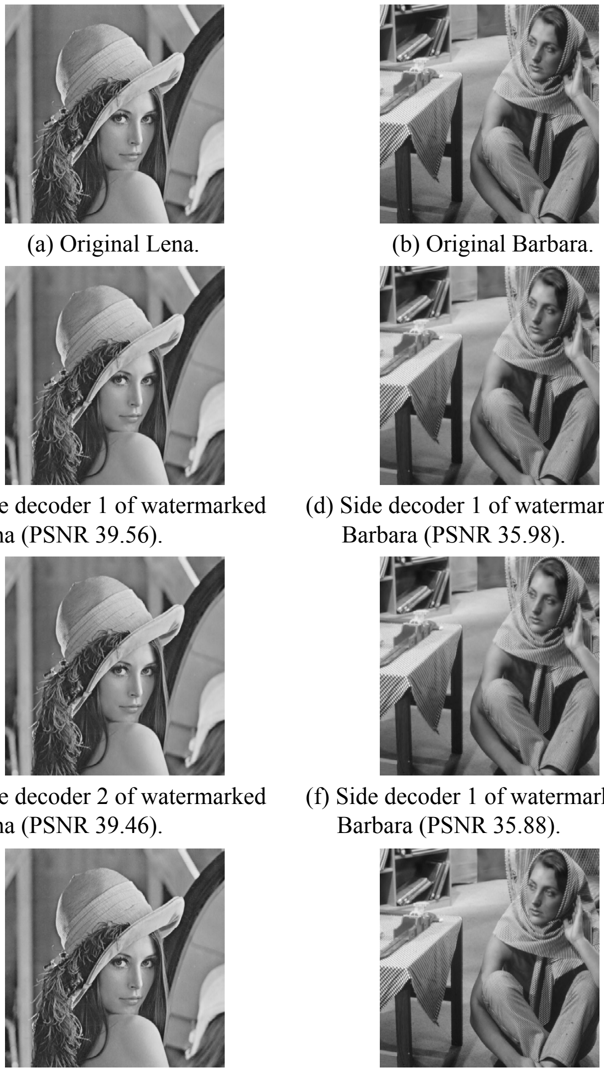
The received watermarked image I'_{wr} (r = 0, 1 or 2) could be attacked by intentional or unintentional modifications, leading to attacked image I''_{wr} (r = 0, 1 or 2). To extract n bits of watermark message M^* from an attacked image, the algorithm is described as follows:

(1) The attacked image I''_{wr} is decomposed into 13-subbands using the 4-level octave band wavelet transform.
(2) Each of the subband coefficients are quantized by a uniform scalar quantizer.
(3) Select the coefficients on LL band of the attacked image for watermark extraction, namely $X''_{sel} = \{x''_1, x''_2, ..., x''_n\}$.
(4) Apply detection process of QIMM on X''_{sel} to obtain the extracted watermark message M^*.

4. EXPERIMENTAL RESULTS

To evaluate the effectiveness of the proposed method, one transformed coefficient was used to embed one bit of watermark information, and totally 128 coefficients were used to embed 128 bits of watermark information. Several standard images including “Lena”, “Barbara”, “House” and “Boat” were tested and demonstrated similar performance. To save space, only “Lena” (Fig. 6 (a)) and “Barbara” (Fig. 6 (b)) are given here. In order to show the flexibility of our proposed MDW framework and to make comparison with our proposed watermarking technique (QIMM), another state-of-the-art watermark technique QIM [4] detailed in section 1 was integrated into the MDW framework with QIMM replaced.

When talking about compression, larger quantization step size will lead to larger distortion MSE (mean square error), meaning smaller PSNR, and hence smaller bit rates is needed. However, when comparing two watermark algorithms, we follow the common practice by fixing two requirements, namely watermark capacity and the transparency (distortion) of watermarked image, and then comparing the robustness. For a fair comparison, the parameter that defined the quantization step was adjusted so that similar PSNR values (in other words, similar distortion) and bit rates could be obtained. The PSNRs of watermarked and un-watermarked “Lena” and “Barbara” for side decoder 1, side decoder 2 and central decoder are illustrated, respectively, in Table 1. From our experiments, the degree of PSNR dropped when the quantization step size was increased. A larger quantization step size brought more robustness, but it also introduced more distortion. According to the theoretical and experimental analysis on both QIMM and QIM as



(a) Original Lena.

(b) Original Barbara.

(c) Side decoder 1 of watermarked Lena (PSNR 39.56).

(d) Side decoder 1 of watermarked Barbara (PSNR 35.98).

(e) Side decoder 2 of watermarked Lena (PSNR 39.46).

(f) Side decoder 1 of watermarked Barbara (PSNR 35.88).

(g) Central decoder of watermarked Lena (PSNR 43.62).

(h) Central decoder of watermarked Barbara (PSNR 40.04).

Fig. 6. Original and watermarked Lenas and Barbaras.

Table 1. The PSNRs of un-watermarked and watermarked "Lena" and "Barbara" for proposed QIMM and Chen's QIM.

Method	PSNR(dB)					
	Lena			Barbara		
	Side 1	Side 2	Central	Side 1	Side 2	Central
Un-watermark	40.94	40.96	49.46	37.53	37.55	47.11
Our QIMM	39.56	39.46	43.62	35.98	35.88	40.04
Chen's QIM	39.71	39.61	44.05	36.09	35.99	40.31

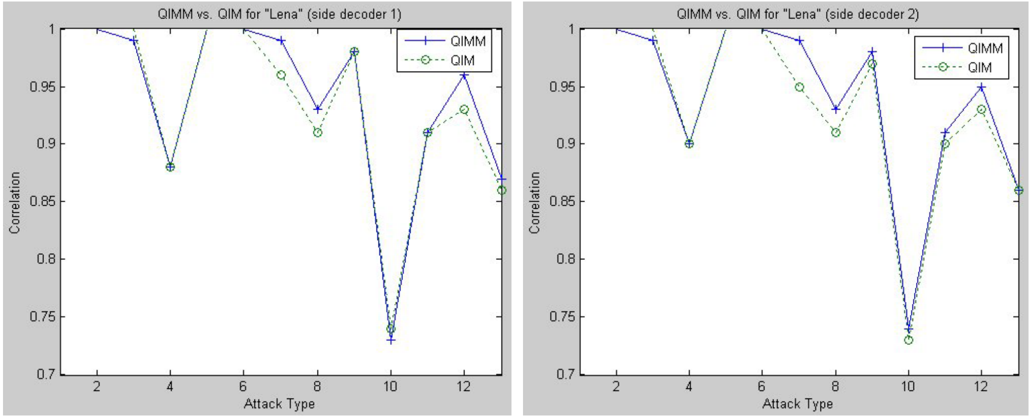
well as comparison of their properties in the aspect of embedding distortion and detection robustness as described in section 2.2, δ_{QIM} was set to 64 and δ_{QIMM} was set to 32 in our setting. The recovered watermarked images by side decoder 1, side decoder 2 and central decoder for QIMM are shown in Figs. 6 (c), (e) and (g) for Lena, respectively, and similarly, in Figs. 6 (d), (f) and (h) for Barbara, respectively. The quality of the pictures recovered from the side decoders was inferior to that recovered from the central decoder, yet still acceptable.

In addition to the degree of robustness against packet loss, a desirable and fundamental property for a watermarking algorithm is to survive compression attack. In the real-world applications, compression is frequently used to facilitate efficient storage and transmission. Here, we used images compressed by JPEG (low quality factor ranging from 10 to 25) and JPEG-2000 (low bit-rates ranging from 0.125 bpp to 1.0 bpp) to test our algorithm. Moreover, a variety of signal manipulation attacks such as Gaussian filtering, sharpening and median filtering were also introduced to check the feasibility of our approach. Among these attacks, we used JPEG-2000 VM8.0 to compress target images and adopted Stirmark3.1 [15] to manipulate the other attacks. Totally 13 attack types as listed in Table 2 were used in these experiments. Under One description loss com- bined with each of the 13 attack types, these two methods still have good performance in the MDW framework.

Table 2. The tested attack types.

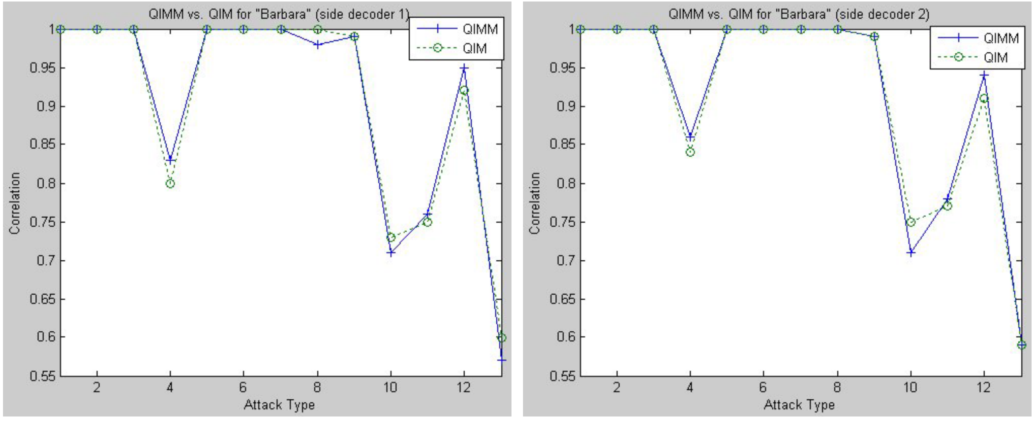
Attack Types	
1	JPEG-2000 1.000 bpp
2	JPEG-2000 0.500 bpp
3	JPEG-2000 0.250 bpp
4	JPEG-2000 0.125 bpp
5	JPEG Quality factor Q(%) = 25
6	JPEG Quality factor Q(%) = 20
7	JPEG Quality factor Q(%) = 15
8	JPEG Quality factor Q(%) = 10
9	Gaussian filtering 3 × 3
10	Sharpening 3 × 3
11	2 × 2 Median filtering
12	3 × 3 Median filtering
13	4 × 4 Median filtering

The detected correlations ratio from the "Lena" and "Barbara" images against the combined attacks are summarized in Figs. 7 and 8, respectively. For some types the detection rate maintains 100% and for other types it degrades. For the "Lena" image, except for the number 10 attack (sharpening 3 × 3), the correlation ratio ρ were all above 0.85. As to the "Barbara" image, except for the number 13 attack (4 × 4 median filtering), the correlation ratio ρ were all above 0.7. It is noted that the primary aim of this paper was to propose a watermarking scheme resilient to packet loss over unreliable network. Therefore, by embedding one bit of information, our scheme uses only one coefficient,



(a) QIMM vs. QIM for "Lena" (side decoder 1). (b) QIMM vs. QIM for "Lena" (side decoder 2).

Fig. 7. The comparison between QIMM and QIM in terms of correlation ratio.



(a) QIMM vs. QIM for "Barbara" (side decoder 1). (b) QIMM vs. QIM for "Barbara" (side decoder 2).

Fig. 8. The comparison between QIMM and QIM in terms of correlation ratio.

and the robustness to these further attacks even with one description loss is an added bonus. It goes without saying, more elaborated schemes which use more coefficients (say one 8 × 8 block) to embed one bit of information should further improve the detector's performance. Though this issue is not treated here, it is obvious that our scheme applies in this extension as well.

5. CONCLUSION

In this paper, the theoretical and experimental analysis on both QIMM and QIM are demonstrated. The comparison of their properties in the aspects of embedding distortion and detection robustness is explored. It is verified that by setting $\delta_{QIM} = 2\delta_{QIMM}$, QIM and QIMM obtained similar embedding distortion, as shown by Delta-Distortion curve, and they are competitive in detection robustness, as shown by Delta-Correlation curve. Furthermore, we propose a multiple description watermarking technique which integrates an oblivious QIMM with the MDC framework. The watermark embedding is computed in either description and could be extracted with the reception of either one or two descriptions. Another advantage of our scheme worth mentioning here is the flexibility of the MDW framework. It can be integrated easily with most current watermarking schemes. This flexibility property is demonstrated in our experiments (see Figs. 7 and 8), where MDW is integrated with QIM and QIMM, respectively. It is evident that, both of these two methods performed well in our MDW framework. In addition to resilience to packet loss, the performance tradeoff between invisibility and robustness to various attacks shows the usefulness of this proposed approach. In the future, we expect that other MDC approach [9-11] or some error resilient algorithms [14] could be integrated with the more elaborated watermarking schemes. Moreover, as the distortion introduced by losing some of the transmitted descriptions of MD transmission can be viewed as a non-linear value-metric attack [16-19], research of an adaptive hexagonal lattice-based QIM which is more robust to value-metric attack is worth further investigation. We believe that the results of these works will make it possible the watermarking of multimedia content for mobile E-commerce applications.

REFERENCES

1. I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Transactions on Image Processing*, Vol. 6, 1997, pp. 1673-1687.
2. C. S. Lu, S. K. Huang, C. J. Sze, and H. Y. M. Liao, "Cocktail watermarking for digital image protection," *IEEE Transactions on Multimedia*, Vol. 2, 2000, pp. 209-224.
3. H. S. Malvar and D. A. F. Florêncio, "Improved spread spectrum: a new modulation technique for robust watermarking," *IEEE Transactions on Signal Processing*, Vol. 51, 2003, pp. 898-905.
4. 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, 2001, pp. 1423-1443.
5. J. J. Eggers, R. Bäuml, R. Tzschoppe, and B. Girod, "Scalar Costa scheme for information embedding," *IEEE Transactions on Image Processing*, Vol. 51, 2003, pp. 1003-1019.
6. F. Hartung and F. Ramme, "Digital rights management and watermarking of multimedia content for M-commerce applications," *IEEE Communications Magazine*, Vol. 38, 2000, pp. 78-84.
7. N. Checcacci, M. Barni, F. Bartolini, and S. Basagni, "Robust video watermarking for wireless multimedia communications," in *Proceedings of IEEE Wireless Communications and Networking Conference*, Vol. 3, 2000, pp. 1530-1535.
8. R. Chandramouli, B. M. Graubard, and C. R. Richmond, "A multiple description framework for oblivious watermarking," in *Proceeding of SPIE: Security and Watermarking of Multimedia Contents III*, Vol. 4314S, 2001, pp. 585-593.

9. Y. Wang, M. T. Orchard, V. A. Vaishampayan, and A. R. Reibman, "Multiple description coding using pairwise correlating transforms," *IEEE Transactions on Image Processing*, Vol. 10, 2001, pp. 351-366.
10. V. K. Goyal, "Multiple description coding: compression meets the network," *IEEE Signal Processing Magazine*, Vol. 18, 2001, pp. 74-93.
11. Y. Wang, A. R. Reibman, and S. Lin, "Multiple description coding for video delivery," in *Proceedings of the IEEE*, Vol. 93, 2005, pp. 57-70.
12. S. D. Servetto, K. Ramchandran, V. A. Vaishampayan, and K. Nahrstedt, "Multiple description wavelet based image coding," *IEEE Transactions on Image Processing*, Vol. 9, 2000, pp. 813-826.
13. V. A. Vaishampayan, "Design of multiple description scalar quantizers," *IEEE Transactions on Information Theory*, Vol. 39, 1993, pp. 821-834.
14. Y. Wang, S. Wenger, J. Wen, and A. K. Katsaggelos, "Error resilient video coding techniques," *IEEE Signal Processing Magazine*, Vol. 17, 2000, pp. 61-82.
15. M. Kutter and F. A. P. Petitcolas, "Fair evaluation methods for image watermarking systems," *Journal of Electronic Imaging*, Vol. 9, 2000, pp. 445-455.
16. F. Pérez-González, C. Mosquera, M. Barni, and A. Abrardo, "Rational dither modulation: a high-rate data-hiding method robust to gain attacks," *IEEE Transactions on Signal Processing*, Vol. 53, 2005, pp. 3960-3975.
17. P. Bas, "A quantization watermarking technique robust to linear and non-linear valumetric distortion using a fractal set of floating quantizers," in *Proceedings of Information Hiding Workshop*, 2005, pp. 106-117.
18. M. L. Miller, G. J. Doerr, and I. J. Cox, "Applying informed coding and informed embedding to design a robust, high capacity watermark," *IEEE Transactions on Image Processing*, Vol. 13, 2004, pp. 792-807.
19. A. Abrardo and M. Barni, "Informed watermarking by means of orthogonal and quasi-orthogonal dirty paper coding," *IEEE Transactions on Signal Processing*, Vol. 53, 2005, pp. 824-833.

Miin-Luen Day (戴敏倫) received his M.S. degree in Electronic Engineering from Chung Yuan Christian University, Taiwan, in 1990, and the Ph.D. degree in Computer Science from Chiao Tung University, Taiwan, in 2007. Since joining the Telecommunication Laboratories of Chunghwa Telecom Co., Ltd. in 1990, he has been doing research and development works in several areas of information and communication. His current research interests include multimedia security, multimedia communication, image processing, and pattern recognition.

Suh-Yin Lee (李素瑛) received her B.S.E.E. degree from the National Chiao Tung University, Taiwan, in 1972, and her M.S. degree in Computer Science from the University of Washington, Seattle, in 1975. She joined the faculty of the Department of Computer Engineering at Chiao Tung University in 1976 and received the Ph.D. degree in Electronic Engineering there in 1982. Dr. Lee is now a professor in the Department of Computer Science and Information Engineering at Chiao Tung University. Her current research interests include multimedia information systems, mobile computing, and data mining. Dr. Lee is a member of Phi Tau Phi, the ACM, and the IEEE Computer Society.

I-Chang Jou (周義昌) received the B.S. degree in Electrical Engineering from National Taiwan University, Taiwan, in 1969; the M.S. degree in Geophysics and in Computer Science from National Central University, Taiwan, in 1972 and 1983, respectively, and the Ph.D. degree in Electrical Engineering from National Taiwan University, Taiwan, in 1986. He was with Telecommunication Laboratories Ministry of Communications, Taiwan from 1972 to 1997. Currently, he is the President of National Kaohsiung First University of Science and Technology. His major research fields are VLSI for DSP, digital signal processing, image processing, speech processing and neural networks. He has published over 131 papers in the areas of parallel computing, image processing, speech processing and neural networks. He is the senior member of IEEE.