Transform-Based Hybrid Data Hiding for Improved Robustness in the Presence of Perceptual Coding

Chuhong Fei, Deepa Kundur and Raymond Kwong

Edward S. Rogers Sr. Department of Electrical and Computer Engineering
University of Toronto, Toronto, Ontario, Canada M5S 3G4

ABSTRACT

This paper addresses the issue of robust data hiding in the presence of perceptual coding. Two common classes of data hiding schemes are considered: spread spectrum and quantization-based techniques. We identify analytically the advantages of both approaches under the lossy compression class of "attacks." Based on our mathematical model, a novel hybrid data hiding algorithm which exploits the "best of both worlds" is presented. Theoretical and simulation results demonstrate the superior robustness of the resulting hybrid scheme.

Keywords: perceptual coding, hybrid data hiding, DCT watermarking

1. INTRODUCTION

Watermarking is emerging as a technology useful not only for copy protection and tamper assessment applications, but also for broadcast monitoring and signal tagging. For the two latter applications, sophisticated attacks are not necessarily the leading threat. Instead, practical compression is the most common form of incidental distortion that limits the robustness or capacity of a data hiding scheme. In this work we address the problem of robust data hiding in the presence of perceptual coding, where robustness and invisibility are two basic requirements. *Perceptual coding* refers to the lossy compression of multimedia signal data using human perceptual models. The compression mechanism is based on the premise that minor modifications of the signal representation will not be noticeable in the displayed signal content. These modifications are imposed on the signal in such a way as to reduce the number of information bits required for storage of the content. Currently, the most common lossy still image compression standard is JPEG.

Many robust data hiding algorithms have been proposed. Many of them are based on spread spectrum principles.[1–5] Spread spectrum data hiding schemes borrow ideas from spread spectrum communications. In these schemes, a watermark is embedded into the host signal by adding a low energy pseudo-randomly generated white noise sequence. This specific pseudonoise sequence is detected by correlating the original watermark sequence with either the extracted watermark or the watermarked signal itself (if the host image is not available for extraction). Spread spectrum data hiding has been demonstrated with excellent robustness and invisibility when the original host signal is available for detection.[1] However, in blind detection, the watermark experiences interference from the host data even when there is no noise from processing and intentional attack.

Another typical class of data hiding techniques is the quantization-based method.[6,7] In this scheme, the watermark, often a binary sequence, is embedded into the host data by quantize-replace strategies that replace a quantized host signal with another quantization value. A simple example belonging to the class is the so called odd-even embedding: the host signal is replaced by the nearest even integer to embed a '0' and the nearest odd integer to embed a '1'.[8] This class of data hiding schemes are free from the interference from host data. However, the quantization-based data hiding method is not very robust against signal distortion.

Spread spectrum and quantization-based data hiding schemes employ different techniques to hide the watermark information, so they have different characteristics of robustness against JPEG compression attack. This motivates the idea of adopting different data hiding methods in different frequency bands to maximize the overall data hiding efficiency. In this paper, we propose a novel hybrid data hiding algorithm which exploits the "best of both worlds" of spread spectrum and quantization-based data hiding techniques. The choice of spread spectrum or quantization-based data hiding methods in different frequency bands is determined by their expected performance in these bands.

Email: fei@control.toronto.edu, deepa@comm.toronto.edu, kwong@control.toronto.edu

The idea of combining two typical data hiding methods has been proposed in the literature.[8,9] M. Wu *et al.*[9] propose a multi-level data hiding algorithm for digital video which is able to convey high data rate when the noise is not severe and can also convey a small amount of data reliably under heavy distortion. In their technique, the DCT coefficients of each 8×8 block is partitioned into two parts: low frequency coefficients are used to hide a large number of bits via odd-even embedding, while other coefficients are used to hide a small number of bits via antipodal spread spectrum embedding. However, their selection of the DCT coefficients to hide information bits via different embedding methods is fixed, that is, it is not optimally and adaptively determined.

The paper is organized as follows. Section 2 describes the mathematical models for the spread spectrum and quantization-based data hiding. Section 3 describes the hybrid algorithm in detail. The simulation results are shown in Section 4.

2. MODELS

2.1. Communication Analogy

One popular analogy for watermark embedding and detection in the presence of compression is data communications over a noisy channel. Communicating the watermark is analogous to transmission of the watermark information through an associated *watermark channel*. This section describes the communication channel models for both spread spectrum and quantization-based data hiding schemes.

2.2. Spread Spectrum Data Hiding

Spread spectrum data hiding schemes borrow ideas from spread spectrum communications. In these schemes, a watermark is embedded into the host signal by adding a low energy pseudo-randomly generated white noise sequence. This specific pseudonoise sequence is detected by correlating the original watermark sequence with either the extracted watermark or the watermarked signal itself (if the host image is not available for extraction).

Generally, the watermark embedding process occurs in a *watermark domain*. An orthogonal transformation is applied to the host image. The transformation decomposes the host image into coefficients to which the watermark is embedded.

Let $\mathbf{x} = [x_1, x_2, \cdots, x_N]$ be the image coefficients in watermark domain. The watermark consists of a sequence of numbers, $\mathbf{w} = [w_1, w_2, \cdots, w_N]$ with a given statistical distribution. The watermark sequence is embedded into the coefficients $\mathbf{x}$ according to the relationship

$$\mathbf{y} = \mathbf{x} + \mathbf{w}, \tag{1}$$

where $\mathbf{y}$ is the watermarked coefficient.

The lossy compression involves quantization of signal coefficients in a *compression domain* such as the DCT domain (for JPEG). For simplicity, we assume that the data hiding domain is the same as compression domain. In compression domain, both the host image signal and the watermark signal pass through a quantizer, as shown in Figure 1, where w is the watermark information and x is the host image in the watermark domain. Since each image coefficient experiences the same spread spectrum embedding and perceptual coding process, for the remainder of the analysis, we drop off the subscript i.

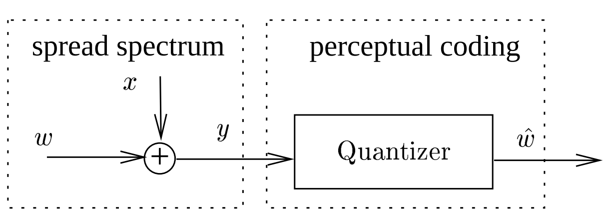

Figure 1. Spread spectrum data hiding in the presence of perceptual coding

Suppose the quantization parameter of perceptual coding is Δ_c, then

$$\hat{w} = [y]_{\Delta_c} = \text{round}(\frac{y}{\Delta_c})\Delta_c = \text{round}(\frac{w+x}{\Delta_c})\Delta_c, \tag{2}$$

where round$(\cdot)$ denotes rounding to the nearest integer, and $[\cdot]_{\Delta_c}$ denotes the quantization operation with step Δ_c.

The dependency between the embedded watermark and the extracted watermark can be measured as

$$\mathrm{Cov}(w, \hat{w}) = E\{w\hat{w}\} = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f_w(u) f_x(v) u [u+v]_{\Delta_c} du dv. \tag{3}$$

The variance of the extracted watermark is

$$\mathrm{Var}(\hat{w}) = E\{\hat{w}^2\} = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f_w(u) f_x(v) [u+v]_{\Delta_c}^2 du dv. \tag{4}$$

Then, the correlation coefficient between the embedded watermark and the extracted watermark is

$$\rho^S(w, \hat{w}) = \frac{\mathrm{Cov}(w, \hat{w})}{\sqrt{\mathrm{Var}(w)\,\mathrm{Var}(\hat{w})}} \tag{5}$$

For data hiding scheme, a correlation receiver is often used in the watermark detection process. Thus, we choose correlation coefficient as a measure to evaluate the success of a data hiding scheme.

2.3. Quantization-based Data Hiding

In quantization-based data hiding scheme, the watermark, often a binary sequence, is embedded into the host data by quantize-replace strategies that replace a quantized host signal with another quantization value. This class of data hiding schemes are free from the interference from host data. There are many different data hiding algorithms using quantization-based idea,[6,7] but there is no general framework to analyze this class of data hiding schemes. In this work, we focus on a simple type of quantization-based data hiding scheme described as follows. First, we define a quantization function $Q_{\Delta_w}(x)$ which maps the real number set $\mathbb{R}$ to $\{0, 1\}$ as shown in Figure 2.

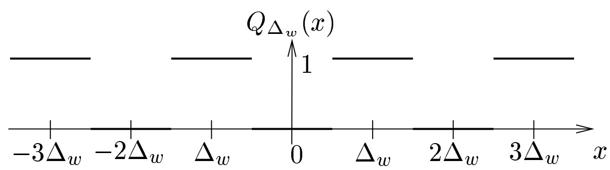

Figure 2. Quantization Function $Q_{\Delta_w}(x)$

$$Q_{\Delta_w}(x) = \mathrm{mod}\Big(\mathrm{round}(\frac{x}{\Delta_w}), 2\Big) = \begin{cases} 0 & \text{if round}(\frac{x}{\Delta_w}) \text{ is even} \\ 1 & \text{if round}(\frac{x}{\Delta_w}) \text{ is odd} \end{cases} \tag{6}$$

where Δ_w is a positive real number called the quantization parameter for data hiding; round$(\cdot)$ denotes rounding to the nearest integer; mod$(\cdot, 2)$ denotes modulo by 2.

The following assignment rule is used to embed the watermark bit w_i into the corresponding image coefficient x_i. We denote the watermarked coefficient as y_i.

$$y_i = \begin{cases} [x_i]_{\Delta_w} & \text{If } Q_{\Delta_w}(x_i) = w_i \\ [x_i]_{\Delta_w} + \Delta_w & \text{If } Q_{\Delta_w}(x_i) \neq w_i \ \& \ x_i \geq [x_i]_{\Delta_w} \\ [x_i]_{\Delta_w} - \Delta_w & \text{If } Q_{\Delta_w}(x_i) \neq w_i \ \& \ x_i < [x_i]_{\Delta_w} \end{cases} \tag{7}$$

where $[x_i]_{\Delta_w} = \mathrm{round}(\frac{x_i}{\Delta_w})\Delta_w$. The parameter Δ_w is user-defined and is set to make the changes in image unnoticeable. A smaller value of Δ_w will make the quantization process finer, and hence introduces less degradation in the image.

The watermark bit is extracted by the following algorithm

$$\hat{w}_i = Q_{\Delta_w}(\hat{y}_i) \tag{8}$$

where $\hat{y}_i$ is the possibly "corrupted" watermarked image coefficient.

If there is no distortion on watermarked image, $\hat{y}_i$ is identical to y_i. Because the embedding algorithm enforces that $Q_{\Delta_w}(y_i) = w_i$, the extraction is perfect in the case that no distortion occurs in the transmission of watermarked image.

2.3.1. Quantization Noise in Quantization-based Data Hiding

Lossy compression involves a quantization process on image coefficients in compression domain. In this section, we characterize the distribution of quantization noise due to the compression process.

A uniform quantizer is shown in Fig 3. Let the quantization step be Δ_c, then the quantized output is

$$\hat{x} = [x]_{\Delta_c} = \text{round}(\frac{x}{\Delta_c})\Delta_c, \tag{9}$$

where round($\cdot$) denotes rounding to the nearest integer.

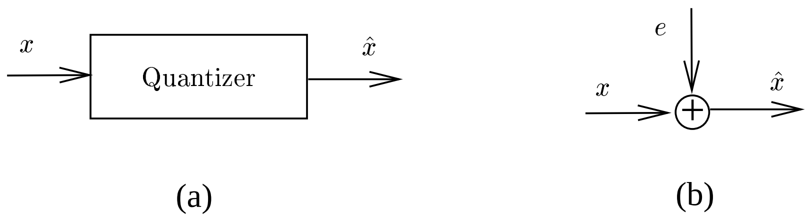

Figure 3. (a) General "black box" quantizer, (b) Quantization noise error model

The quantization error e is defined as

$$e = \hat{x} - x = [x]_{\Delta_c} - x. \tag{10}$$

The distribution of quantization error depends on the distribution of the input variable x. Suppose the probability density function of x is $f_x(u)$, and the probability density function of quantization error e is $f_e(v)$. Obviously the quantization error is bounded in $-\frac{\Delta_c}{2} \leq e \leq \frac{\Delta_c}{2}$, so the probability density function $f_e(v) = 0$ if $|v| > \frac{\Delta_c}{2}$. Define I_A, the indicator function of an event A, as follows,

$$I_A(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{Otherwise} \end{cases}. \tag{11}$$

Let $-\frac{\Delta_c}{2} \leq v \leq \frac{\Delta_c}{2}$, then

$$\begin{aligned} P(e \leq v) &= P(\text{round}(\frac{x}{\Delta_c})\Delta_c - x \leq v) = \int_{-\infty}^{\infty} f_x(u) I_{\text{round}(\frac{u}{\Delta_c})\Delta_c - u \leq v} du \\ &= \sum_{k=-\infty}^{\infty} \int_{k\Delta_c - \frac{\Delta_c}{2}}^{k\Delta_c + \frac{\Delta_c}{2}} f_x(u) I_{k\Delta_c - u \leq v} du = \sum_{k=-\infty}^{\infty} \int_{k\Delta_c - v}^{k\Delta_c + \frac{\Delta_c}{2}} f_x(u) du \\ &= \sum_{k=-\infty}^{\infty} \int_{-\frac{\Delta_c}{2}}^{v} f_x(k\Delta_c - u) du = \int_{-\frac{\Delta_c}{2}}^{v} \sum_{k=-\infty}^{\infty} f_x(k\Delta_c - u) du \end{aligned} \tag{12}$$

Then the probability density function of the quantization error e is

$$f_e(v) = \text{rect}(\frac{v}{\Delta_c}) \sum_{k=-\infty}^{\infty} f_x(k\Delta_c - v), \tag{13}$$

where $\text{rect}(v) = \begin{cases} 1 \text{ if } |v| \leq 0.5 \\ 0 \text{ if } |v| > 0.5 \end{cases}$.

2.3.2. Data Hiding in the Presence of Compression

The general quantization-based data hiding process is shown in Figure. 4. From the embedding algorithm equation (7), we know

$$y = k\Delta_w, \tag{14}$$

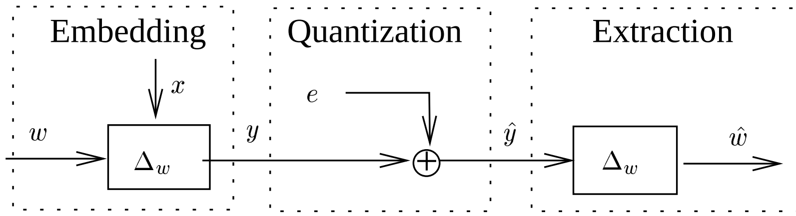

Figure 4. General quantization based data hiding process

where k is an integer with $\mathrm{mod}(k, 2) = w$, and Δ_w is the quantization parameter for data hiding.

From the extraction algorithm equation (8), we have the following relation between the original watermark w and the extracted watermark $\hat{w}$.

$$\begin{aligned}\hat{w} &= Q_{\Delta_w}(\hat{y}) = Q_{\Delta_w}(k\Delta_w + e) = \mathrm{mod}\Big(\mathrm{round}\,(\frac{k\Delta_w + e}{\Delta_w}), 2\Big) \\ &= \mathrm{mod}\Big(k + \mathrm{round}(\frac{e}{\Delta_w}), 2\Big) = \mathrm{mod}(k, 2) \oplus \mathrm{mod}\Big(\mathrm{round}(\frac{e}{\Delta_w}), 2\Big) \\ &= w \oplus Q_{\Delta_w}(e) \end{aligned} \tag{15}$$

where $\oplus$ represents modulo 2 addition.

From Equation (15), the relation between the watermark bit w and the extracted watermark bit $\hat{w}$ is only affected by quantization noise $e = \hat{y} - y$.

2.3.3. Watermark Channel for Quantization-based Data Hiding

The watermark channel is characterized by the compression algorithm applied to the watermarked signal. In this section we model the effect of perceptual coding on quantization-based data hiding.

For the quantization-based algorithm, we represent the watermark channel as a discrete memoryless channel. Transmission of one watermark bit can be modeled with the binary symmetric channel (BSC) shown in Figure 5 .[10] A message, '0' or '1', is transmitted though the channel with probability of bit error p_e.

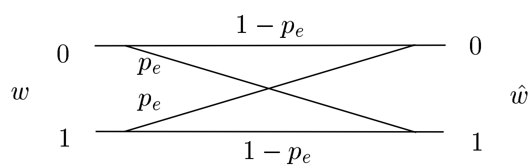

Figure 5. Binary Symmetric Channel

The probability of bit error p_e is defined as $P\{\hat{w} \neq w\}$. Then we have

$$p_e = P\{w \oplus Q_{\Delta_w}(e) \neq w\} = P\{Q_{\Delta_w}(e) = 1\} \tag{16}$$

The probability density function of quantization noise, $f_e(v)$, is calculated according to Equation (13). Therefore,

$$p_e = \int_{-\frac{\Delta_c}{2}}^{\frac{\Delta_c}{2}} f_e(v) I_{Q_{\Delta_w}(v)=1} dv = \int_{-\frac{\Delta_c}{2}}^{\frac{\Delta_c}{2}} f_e(v) Q_{\Delta_w}(v) dv = E_e\{Q_{\Delta_w}(e)\} \tag{17}$$

because the indicator function $I_{Q_{\Delta_w}(e)=1}$ is equal to $Q_{\Delta_w}(e)$ itself.

It can be shown that the correlation coefficient between the embedded watermark and the extracted watermark in this case is given by

$$\rho^Q(w, \hat{w}) = \frac{\mathrm{Cov}(w, \hat{w})}{\sqrt{\mathrm{Var}(w)\,\mathrm{Var}(\hat{w})}} = 1 - 2p_e \tag{18}$$

3. HYBRID DATA HIDING

3.1. Motivation

Spread spectrum and quantization-based data hiding schemes employ different techniques to hide the watermark information, so they have different characteristics of robustness against JPEG compression attack in different DCT frequency bands. As discussed in the introduction, the spread spectrum method is robust even against a high degree of JPEG compression. However, it experiences interference from the host image for blind detection. The quantization-based method is free from the the interference from the host image, but is not very robust against severe compression.

JPEG compression involves a quantization process which has varying distortions for different frequencies of the 8×8 DCT matrix. This motivates the idea of adopting different methods in different frequency bands to increase the robustness of the data hiding scheme. We propose a hybrid data hiding algorithm which exploits the "best of both worlds" of spread spectrum and quantization-based methods. The choice of using spread spectrum or quantization-based method in the 8×8 DCT bands is determined according to their predicted behavior.

3.2. Switching Table

In order to determine the watermark embedding strategy that should be employed in each coefficient band to maximize robustness, we introduce a *switching table.* A switching table S is a 8×8 matrix whose elements $S(i,j), 1 \leq i,j \leq 8$ has a binary value $\{0,1\}$ with the following meaning

If $S(i,j) = 0$
    Embed the watermark in the DCT band (i,j) using the spread spectrum method
If $S(i,j) = 1$
    Embed the watermark in the DCT band (i,j) using the quantization-based method

There is a one-to-one correspondence between each element in S and each DCT coefficient band. Thus, a switching table S determines the watermark embedding method to be used in every DCT coefficient band $(i,j), 1 \leq i,j \leq 8$.

As pointed out in the introduction, robustness and imperceptibility are two basic but rather contradictory requirements for data hiding applications. In order to compare the efficiency of the two data hiding algorithms, we fix the imperceptibility condition, and evaluate the measure of robustness. The imperceptibility condition can be characterized by the extent of distortion on the original host image due to watermark embedding. In the spread spectrum embedding process, the watermark is assumed to have energy σ_w^2. In the quantization-based embedding algorithm, the quantization parameter for data hiding is assumed to be Δ_w, then the distortion introduced into the host has variance approximately equal to $\frac{\Delta_w^2}{3}$. Therefore, in order to ensure each data hiding method introduces the same amount of unnoticeable distortion in the host data, the watermark energy parameter σ_w of spread spectrum algorithm and the quantization parameter Δ_w of quantization-based algorithm must satisfy the following relationship

$$\Delta_w = \sqrt{3}\sigma_w. \tag{19}$$

In practice, a correlation receiver is often used in the watermark detection process because of its simplicity. Thus, the correlation coefficient between the original watermark and the extracted watermark is used as an objective measure to compare the performance of these two data hiding schemes.

Let $\rho_{ij}^S, 1 \leq i,j \leq 8$ be the correlation coefficient of the original and extracted watermark in the DCT frequency band (i,j) using the spread spectrum method and ρ_{ij}^Q be the correlation coefficients using the quantization-based method. The values of ρ_{ij}^S and ρ_{ij}^Q are calculated by Equations (5) and (18), respectively. Thus, the optimal switching table S to maximize the overall performance is easily determined by just comparing the two individual correlation coefficients such that

$$S(i,j) = \begin{cases} 0 & \text{If } \rho_{ij}^S > \rho_{ij}^Q \\ 1 & \text{If } \rho_{ij}^S < \rho_{ij}^Q \\ 0 \text{ or } 1 & \text{If } \rho_{ij}^S = \rho_{ij}^Q \end{cases}. \tag{20}$$

3.3. Algorithm

In this section, we propose our novel joint spread spectrum and quantization based data hiding algorithm in detail. Let σ_w be the watermark parameter in spread spectrum data hiding method and Δ_w be the quantization parameter of watermark embedding in quantization-based method. The parameters σ_w and Δ_w are chosen to satisfy the relation in Equation (19) and to be small enough such that the watermark embedding does not cause perceptible notice in the original host image. In this work, we only consider 8×8 DCT block transform. Let $f_k(i,j)$ be the DCT image coefficient and $w_k(i,j)$ be the watermark signal where $(i,j), 1 \leq i,j \leq 8$ represents the position in a 8×8 image block; the subscript k represents the index of image blocks and $1 \leq k \leq K$ where K is the total number of blocks in an image. The watermark signal sequence $w_k(i,j)$ is independently generated as follows to suit the characteristics of the particular embedding strategy for each 8×8 image block coefficient.

If $S(i,j) = 0$, then
  For all $1 \leq k \leq K$, generate $w_k(i,j)$ randomly with a given distribution such as Gaussian $\mathcal{N}(0, \sigma_w^2)$.
If $S(i,j) = 1$, then
  For all $1 \leq k \leq K$, generate $w_k(i,j)$ randomly with equi-probable binary distribution

3.3.1. Watermark Embedding

1. The embedding process occurs in the watermark domain. The DCT transform is applied to each 8×8 image block of the host image. We denote each image coefficient by $f_k(i,j)$, where $(i,j), 1 \leq i,j \leq 8$ is the position of DCT coefficient in the kth block.

2. For each block k, and for each $(i,j), 1 \leq i,j \leq 8$,

   (a) If $S(i,j) = 0$, then embed $w_k(i,j)$ in $f_k(i,j)$ using the spread spectrum embedding algorithm as follows.

   $$f_k(i,j) := f_k(i,j) + w_k(i,j) \tag{21}$$

   (b) If $S(i,j) = 1$, then embed $w_k(i,j)$ in $f_k(i,j)$ using the quantization-based embedding algorithm; that is, change $f_k(i,j)$ with the following assignment

   i. If $Q_{\Delta_w}(f_k(i,j)) = w_k(i,j)$, then

   $$f_k(i,j) := [f_k(i,j)]_{\Delta_w} \tag{22}$$

   where $[x]_{\Delta_w} = \text{round}(\frac{x}{\Delta_w})\Delta_w$ and function $Q_{\Delta_w}(x)$ is defined in Equation (6).

   ii. Otherwise,

   $$f_k(i,j) := \begin{cases} [f_k(i,j)]_{\Delta_w} + \Delta_w & \text{if } f_k(k,j) \geq [f_k(i,j)]_{\Delta_w} \\ [f_k(i,j)]_{\Delta_w} - \Delta_w & \text{if } f_k(i,j) < [f_k(i,j)]_{\Delta_w} \end{cases} \tag{23}$$

3. The corresponding inverse transformation is computed to form the watermarked image.

3.3.2. Watermark Detection

1. Taking the DCT block transform on the watermarked image yields the DCT coefficients $\hat{f}_k(i,j)$ in the DCT domain.

2. Extraction of the watermark from the watermarked image coefficients $\hat{f}_k(i,j)$ occurs as follows.

   (a) If $S(i,j) = 0$, then extract the watermark information with the spread spectrum extraction algorithm. The extracted watermark is the watermarked image coefficient itself in *blind* data hiding where the original image is not available.

   $$\hat{w}_k(i,j) = \hat{f}_k(i,j) \tag{24}$$

   (b) If $S(i,j) = 1$, then extract the watermark bit with the following quantization-based extraction algorithm

   $$\hat{w}_k(i,j) = Q_{\Delta_w}(\hat{f}_k(i,j)) \tag{25}$$

3. The individual correlation coefficient of each channel is calculated in the corresponding standard way as follows.
   (a) If $S(i,j) = 0$,

$$\rho(i,j) = \frac{\frac{1}{K}\sum_{k=1}^{K} w_k(i,j)\hat{w}_k(i,j)}{\sigma_w \sqrt{\frac{1}{K}\sum_{k=1}^{K} \hat{w}_k^2(i,j)}} \tag{26}$$

   (b) If $S(i,j) = 1$,

$$\rho(i,j) = \frac{1}{K}\sum_{k=1}^{K} w_k(i,j) \oplus \hat{w}_k(i,j) \tag{27}$$

   where $\oplus$ denotes modulo 2 addition.

4. To detect the existence of original watermark, the average correlation coefficient is calculated using

$$\rho = \frac{1}{8 \times 8}\sum_{i=1}^{8}\sum_{j=1}^{8} \rho(i,j). \tag{28}$$

   To assess the existence of the original watermark, that is, to give yes-or-no watermark detection decision, we compare the average correlation coefficient ρ to a pre-defined threshold $\mathcal{T}$,
   (a) If $\rho > \mathcal{T}$, the original watermark is considered to be present.
   (b) Otherwise, the original watermark is considered not to be present.

It should be noted that the switching table S is generated according to the predicted behaviors of the spread spectrum and quantization-based methods to perceptual coding. In the next section, we justify our use of the models introduced in Section 2 by verifying the improved performance of our novel hybrid scheme in comparison to standard spread spectrum and quantization-based methods.

4. SIMULATION AND COMPARISON

We perform simulations on the real test image Lena of size 512×512 using the proposed hybrid watermarking algorithm. A watermark sequence containing both the continuous Gaussian and the binary signal components is embedded into the image. In order to keep the watermarked image perceptually identical to the original image, the parameter of Gaussian signal σ_w is set to be 2, so according to the Equation (19), the quantization parameter Δ_w of quantization embedding is set to $2\sqrt{3}$. In order to determine the switching table, we assume that the image coefficients in DCT domain have Gaussian distribution, and the parameters of Gaussian distribution are estimated based on the sample image Lena.

In the implementation of our method, we assume that the JPEG compression quality factor is known in the watermark embedding process. The switching table is determined by calculating and comparing the correlation coefficients of both spread spectrum and quantization-based data hiding scheme in all DCT frequency bands. Both the spread spectrum and the quantization-based data hiding methods have also been implemented for performance comparison. The average sample correlation coefficient is computed to measure the success of the data hiding scheme. For transparency of data hiding, we do not embed data into the DC components of image coefficients.

Figure 6 shows the average correlation coefficient of each algorithm when JPEG compression quality factor varies from 100 down to 60. We see that in the low compression case, that is, high JPEG quality factor near 100, the plot of the average correlation coefficient of the hybrid algorithm is close to that of the quantization-based algorithm. This is because in the low compression case, the quantization-based method is superior to the spread spectrum method. Thus the hybrid algorithm switches to the quantization-based technique in all frequency bands. In high compression cases, that is, when JPEG compression quality is less than 75, the hybrid algorithm is close to the spread spectrum method. It is because in high compression case the spread spectrum algorithm is much better than the quantization-based algorithm, thus, accordingly, the hybrid algorithm switches to spread spectrum technique in all frequency bands. In medium compression cases when JPEG compression quality ranges from 75 to 95, the hybrid

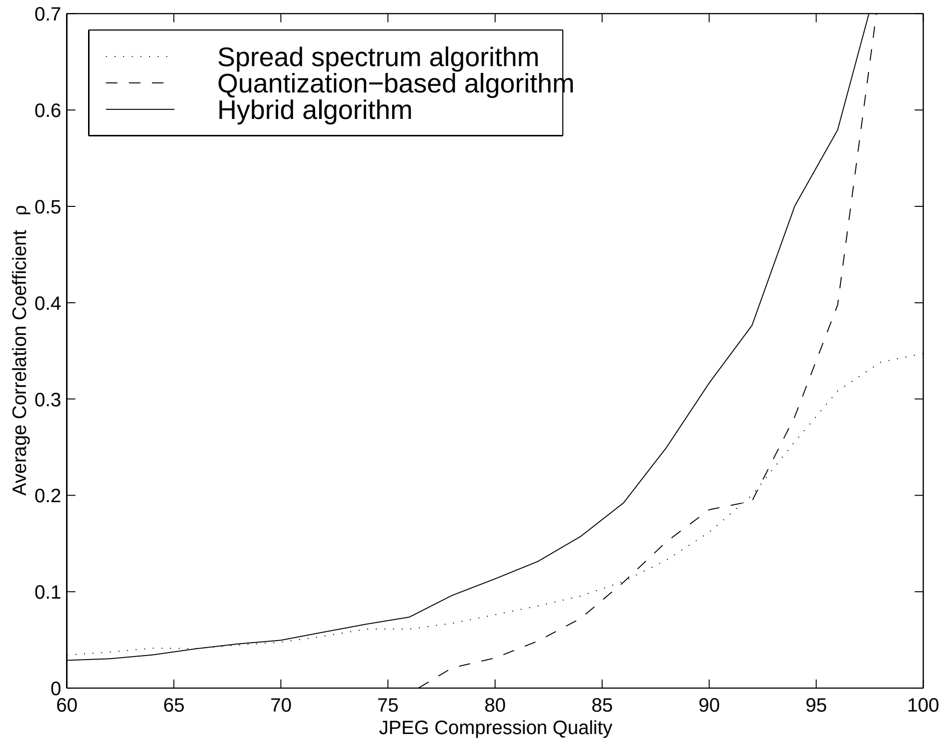

Figure 6. The average sample correlation coefficient vs. JPEG compression quality (The dotted line represents the results for the single quantization-based method, the dashed line corresponds single spread spectrum method and the solid line corresponds our hybrid method)

algorithm is much better than both of single algorithms. This is because the hybrid algorithm always chooses the better algorithm in all frequency bands to transmit watermark information.

The major advantage of this hybrid algorithm is that the switching table is optimally determined according to the expected performance of the spread spectrum and quantization-based methods. However, this requires a priori knowledge of the JPEG compression degree in the transmission of watermarked image.

By modeling the image as noise with a given distribution, the switching table can be pre-computed prior to data embedding process. Thus, the complexity of calculating the switching table does not influence real time implementation of data embedding and extraction algorithms.

Although in the paper we assume that the data hiding domain is the same as that of compression, that is, DCT for JPEG compression, the mathematical models for spread spectrum and quantization-based data hiding methods can be extended to any data hiding domain. For details of these models, please refer to Ref. 11,12.

5. CONCLUSION

We propose a novel hybrid data hiding algorithm which exploits the best merits of both spread spectrum and quantization based data hiding algorithms. The switching table which determines how to choose the embedding method is computed with the mathematical models of both spread spectrum and quantization-based data hiding schemes. Simulation results verify its superiority to the single spread spectrum or quantization-based technique. Future research includes incorporating human perceptual model into data hiding process and extending this idea to address other common signal attacks.

REFERENCES

1. I. J. Cox, J. Killian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. on Image Processing* **6**(12), pp. 1673–1687, 1997.

2. X. G. Xia, C. G. Boncelet, and G. R. Arce, "A multiresolution watermark for digital images," *Proc. IEEE Int. Conference in Image Processing* **1**, pp. 548–551, November 1998.
3. M. Barni, F. Bartolini, V. Cappellini, and A. Piva, "A DCT domain system for robust image watermarking," *Signal Processing* **66**, pp. 357–372, 1998.
4. F. Hartung and B. Girod, "Watermarking of uncompressed and compressed video," *Signal Processing* **66**, pp. 283–801, 1998.
5. R. B. Wolfgang, C. I. Podilchuk, and E. J. Delp, "Perceptual watermarks for digital images and video," *Proceedings of the IEEE – Special Issue on Identification and Protection of Multimedia* **87**, pp. 1108–1126, July 1999.
6. B. Chen and G. W. Wornell, "Dither modulation: a new approach to digital watermarking and information embedding," in *Proceedings of the SPIE: Security and Watermarking of Multimedia Contents*, vol. 3657, pp. 342–353, Jan 1999.
7. D. Kundur and D. Hatzinakos, "Digital watermarking using multiresolution wavelet decomposition," in *Proc. IEEE Int. Conf. On Acoustics, Speech and Signal Processing*, vol. 5, pp. 2969–2972, (Seattle, Washington), May 1998.
8. M. Wu, H. Yu, and A. Gelman, "Multi-level data hiding for digital image and video," in *SPIE Photonics East '99*, (Boston), 1999.
9. M. Wu and H. Yu, "Video access control via multi-level data hiding," in *IEEE Int. Conf. on Multimedia & Expo (ICME'00)*, (New York City), 2000.
10. D. Kundur, *Multiresolution digital watermarking: algorithm and implication for multimedia signals.* PhD thesis, University of Toronto, Toronto, 1999.
11. C. Fei, "On the choice of transform for robust watermarking in the presence of lossy compression," Master's thesis, University of Toronto, Toronto, 2001.
12. C. Fei, D. Kundur, and R. Kwong, "The choice of watermark domain in the presence of compression," in *Proc. IEEE Int. Conf. on Information Technology: Coding and Computing*, (Las Vegas, Nevada), April 2001.