Security and Robustness Enhancement for Image Data Hiding

Ning Liu, Palak Amin, and K.P. Subbalakshmi* (Contact Author: K.P. Subbalakshmi)

Abstract

In many applications, data hiding in images can be viewed as a trade-off between capacity, robustness (against attacks) and embedding induced distortion. In this paper, we consider a fourth parameter: the security of the hidden information. Specifically, we propose a hash based randomized embedding algorithm (HRE) that increases the security of the hidden data. We then optimize this algorithm against JPEG attacks. We derive a mathematical expression for the security of our algorithm, using which we show that the security of our algorithm can be increased independent of capacity, robustness and embedding induced distortion. The maximum security depends only on the length of the key sequence, which is limited only by the size of the host image. Using a joint security and capacity measure, we show that the proposed scheme performs better than current secure quantization based data hiding schemes. We also derive the optimal value of distortion compensation factor of the HRE algorithm against JPEG compression attack. Experimental results show that the operating points achieved by the proposed scheme are 7 dB better than current *blind data hiding* schemes against the JPEG attack.

Index Terms

Secure image data-hiding, Steganography, blind data hiding, JPEG compression attack, Distortion compensation.

This work was funded by National Science Foundation (NSF) award number NSF-DAS 0242417

N. Liu is with the ECE Department, Stevens Institute of Technology, Hoboken, NJ 07030 USA. e-mail: nliu@stevens.edu

P. Amin is with the ECE Department, Stevens Institute of Technology, Hoboken, NJ 07030 USA. e-mail: pamin@stevens.edu

K.P. Subbalakshmi is with the ECE Department, Burchard 208, Stevens Institute of Technology, Hoboken, NJ 07030 USA, e-mail: ksubbala@stevens.edu, Phone: 201-216-8641, Fax: 201-216-8246

EDICS Category: 1-ENCR

I. Introduction

Digital data hiding refers to the process of hiding secondary data in host data [1]–[15]. Covert communications, access control, ownership assertion and annotation are some applications of data hiding. Data is hidden without distorting the original multimedia content to a noticeable level and transferred without requiring additional channel bandwidth. A fundamental issue in data hiding is to achieve a trade off between capacity, robustness and distortion. Several approaches have been proposed to achieve this: some in the spatial domain [9]–[11], [16], some in the frequency domain [17], [18]; some based on quantization [19]–[23], and some based on spread spectrum methods [24]–[26]. Work has also been done in achieving capacity against worst case additive noise attack [27]–[29].

There is another equally important parameter, namely the security of the hidden data. Several researchers have addressed this problem [30]–[32], but often not in conjunction with the other three parameters. In [32], the authors propose a lattice based embedding algorithm where security is achieved by randomly picking a set of host coefficients to embed. It is noted this algorithm can be made more secure by embedding smaller amount data [32]. Wu addressed the trade-off between security and the other parameters [33] and proposed a data hiding scheme using a lookup table (LUT) [34] to enhance the security of the embedded information. It was shown [33] that the security of the LUT based algorithm is enhanced and that at lower WNR ranges, the LUT based scheme can achieve higher embedding rate than the odd-even embedding algorithm [35]. The probability of detection error could be considerably reduced below the traditional quantization based embedding, if we use a lookup table (LUT) of nontrivial runs that map quantized multimedia features randomly to binary data. However, this increased detection probability comes at the cost of increased distortion to the host.

In this paper we *(a) propose an algorithm that increases the security of the hidden data and (b) optimize it for JPEG attacks.* In the first part of this paper, we propose a hash-based randomized embedding algorithm (HRE) which does not impair the capacity, embedding induced distortion, and robustness of the hidden data to additive noise. This algorithm can be used in either time or frequency domain. We develop a mathematical expression for the security of this algorithm and show that the security can be increased without impairing the capacity, embedding induced distortion or robustness to additive noise attacks, unlike in [32], [33]. We also show that the security

is limited only by the length of the key sequence, which in turn is limited only by the size of the image. Note that, in our proposed algorithm, the embedding positions in the host image are fixed and assumed to be known to the adversary, unlike in [32] where the security depends on the secrecy of the embedding locations. The security in our algorithm is achieved by randomizing the quantizers used in these positions (details in Section III).

In the second part of the paper, we apply the proposed HRE algorithm in the DCT domain, and model both the embedding induced noise and quantization error due to JPEG compression as additive uniform noise. The *pdf* of the attacked stego-signal is equivalent to the convolution of the *pdf*s of the embedding induced noise and the JPEG compression noise. The expression of the bit error rate, P_e, is then derived based on the *pdf* of the attacked stego-signal. The optimal distortion compensation factor, $\alpha^*_{HRE-JPEG}$, is obtained by minimizing P_e over α. The optimal quantizer based embedding (against JPEG compression attack) is achieved by applying $\alpha^*_{HRE-JPEG}$ in the proposed HRE algorithm. Experimental results show that the operating points achieved by the proposed scheme are 7 dB better than spread transform dither modulation (STDM) [36] and 12 dB over unspread dither modulation (UDM) [36].

In Section-II, we briefly present the details of the algorithm proposed by Wu [33], with which the performance of our algorithm will be compared in terms of security, robustness, distortion and capacity. Section-III describes the details of our algorithm and explains the encoding and decoding operations. We also derive a mathematical expression for the security of our scheme in this section. In Section-IV we derive the optimal distortion compensation factor for the HRE scheme against *JPEG compression attack*. Section-V provides simulation results and Section-VI concludes the paper.

II. Related Work: Lookup Table (LUT) Embedding

The algorithm proposed in [33] is based on a general embedding technique known as lookup table (LUT) embedding [34], [37]. The encoder generates a LUT beforehand, denoted by $T(\cdot)$. To embed a "0" (or a "1"), the host signal is quantized to the closest representation value that is mapped to a "0" (or a "1") as seen in Equation-1 based on the entries in the LUT.

$$Y = \begin{cases} Quant(X_0) & \text{if} \quad T\left[\frac{Quant(X_0)}{q}\right] = b \\ X_0 + \delta, & \text{otherwise} \end{cases} \tag{1}$$

where, X_0 is the original feature (could be a gray value pixel $X_0 \in (0, 255)$), Y is the marked feature, b is the bit that is to be hidden, $Quant(\cdot)$ is the quantization operation, and

$$\delta \triangleq \min_{|d|}\{d = Quant(X_0) - X_0, \quad \text{s.t.} \quad T(Quant(X_0)/q) = b\}. \tag{2}$$

Basically, the security lies in the permutation of (0 and 1) in the "lookup table". For example, let us assume a uniform quantizer with quantization step size $q = 10$ and a lookup table $\{..., T(6) = 1, T(7) = 0, T(8) = 0, T(9) = 0, T(10) = 1, T(11) = 1, ...\}$. To embed a "1" in a pixel with value "78", the encoder rounds it to the nearest multiple of ten such that the multiple is mapped to a "1" by the LUT. In this example, 2, reduces to

$$\delta \triangleq \min_{|d|}\{d = Quant(78) - 78, \quad \text{s.t.} \quad T(Quant(78)/10) = 1\}. \tag{3}$$

Although, the closest multiple of 10 to 78 is 80, T(80) = 0. The algorithm, hence, searches for the closest multiple of 10, that will result in a mapping to 1, based on the LUT. This, in our case, is "60", which is then taken as the watermarked pixel value. Similarly, to embed a "0" in this pixel, the encoder would round it to "80".

The extracted bit, $\hat{b}$, is given by: $\hat{b} = T\left[\frac{Quant(Y)}{q}\right]$. From Equation-1, when $T(Quant(X_0)/q)$ does not correspond to the hidden bit, the encoder quantizes X_0 to the closest representation value that is mapped to the bit that is to be hidden [33]. In order to prevent excessive modification of the host, both the number of successive "1"s or "0"s and the overall number of bits in the LUT mapping must be limited. If "r" denotes maximum allowable run, then the security of the scheme is given by:

$$H_{LUT} = 1 - \frac{1}{2^r - 1}\text{bits} \tag{4}$$

As seen from Equation-4, the security increases if r increases. However, increasing the security of the embedded data would inevitably lead to higher distortion to the feature values that are not mapped to the appropriate host [33]. The mean squared error of the LUT scheme (MSE_A) for run $r = 2$ is calculated as seen in Equation-5.

$$MSE_A = \frac{1}{2} * \frac{q^2}{12} + \frac{1}{2} * \frac{11}{12} = \frac{q^2}{2} \tag{5}$$

where, q is the quantization step size. Note that MSE_A is greater than the distortion caused by the generic odd-even quantizer based scheme, which is $q^2/3$.

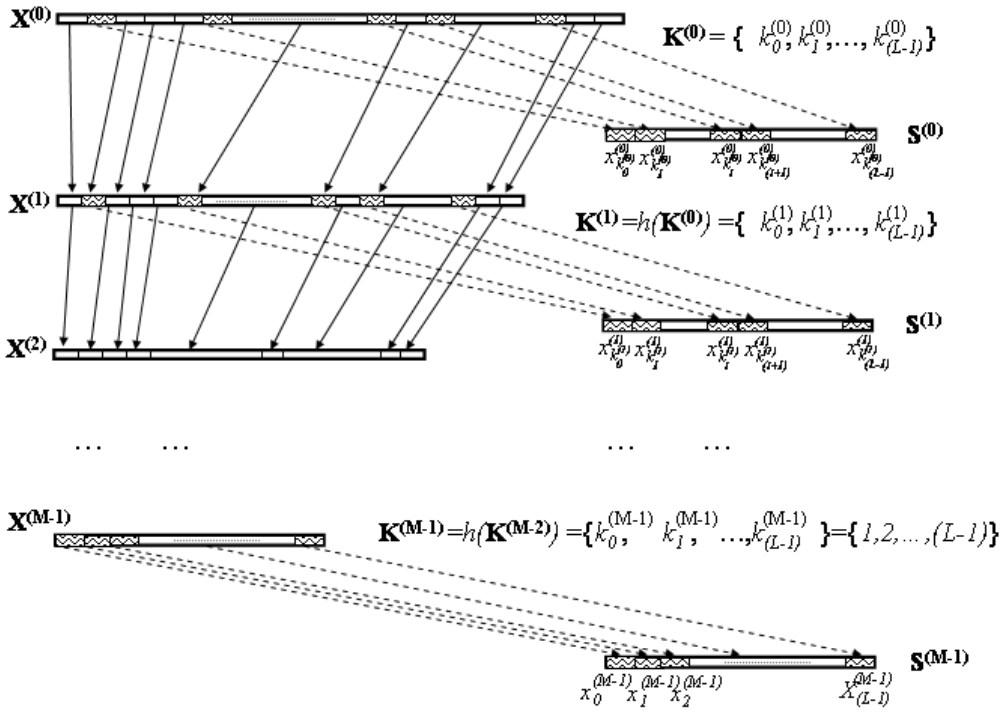

Fig. 1. **Key sequences, host sequences and the relations between them**

III. The Proposed Hash-based Randomized embedding Algorithm

LUT based data hiding scheme increases distortion to enhance security for a fixed embedding capacity and robustness. In this paper, we propose a new scheme, which can achieve greater security without increasing the distortion for the same embedding capacity and robustness. Although we describe the encoder/decoder algorithm in time domain, the same algorithm can be used in the frequency domain without any modification to its structure.

A. Encoder Framework

Our scheme is based on embedding hidden data in randomly generated subsequences of host images. The indices of the pixels in the subsequences are generated using a key sequence and successive hashes of this key sequence. The capacity achieved by our scheme is the same as the scalar Costa scheme (SCS) [20], and the security of our scheme depends only on the length of the adopted key sequence. This embedding algorithm is shown below.

1. **Partition Image into Subsequences:** Consider an $N \times N$ host image X. Division of image into $M = N \times N/L$ subsequences, where M is an even integer, is done as follows (See Figure-1):

   Set $i = 0$ and $X^{(0)} = X = \{x_0^{(0)}, x_1^{(0)}, \cdots, x_{N\times N-1}^{(0)}\}$, which is the host image treated as a vector of length $N \times N$. Generate a random key sequence $K^{(0)} = \{k_0^{(0)}, k_1^{(0)}, k_2^{(0)}, \cdots, k_{(L-1)}^{(0)}\}$ of length L.

   $\star$: Generate the i^{th} image subsequence $S^{(i)}$: $S^{(i)} = \{x_{k_0^{(i)}}^{(i)}, x_{k_1^{(i)}}^{(i)}, x_{k_2^{(i)}}^{(i)}, \cdots, x_{k_{(L-1)}^{(i)}}^{(i)}\}$.

   From $X^{(i)}$ remove all elements in $S^{(i)}$ to get: $X^{(i+1)} = \{x_0^{(i+1)}, x_1^{(i+1)}, \cdots, x_{N\times N-i\times(L-1)}^{(i+1)}\}$.

   Set $K^{(i+1)} = h(K^{(i)})$.[a]

   If $i == M$

   Stop;

   Else

   $i \leftarrow i + 1$ and Goto $\star$;

   End

2. **Parameter Calculation:** If using the SCS scheme [20], to compensate for distortion, calculate the distortion compensation factor as follows:

$$\Delta = \sqrt{12(\sigma_w^2 + 2.71\sigma_n^2)} \tag{6}$$

$$\alpha = \sqrt{\frac{\sigma_w^2}{\sigma_w^2 + 2.71\sigma_n^2}} \tag{7}$$

   Else, if compensating for distortion due to JPEG attack, calculate distortion compensation factor , $\alpha^*_{HRE-JPEG}$ as given in SectionIV.

3. **Embedding Process:** Set a parameter $t = \frac{\Delta}{M}$. For each subsequence $S^{(i)}$, we assign an initial value, $d_i = t \times i$, for the quantizer, where "initial value" is defined as the first element of the left most bin of the quantizer. For each subsequence $S^{(i)}$, we embed one bit in each component of $S^{(i)}$ by using the SCS scheme.

[a] $h(\cdot)$ could be any hash function. In this paper, we use the MD5 hash function [38]. If there is position collusion, the hash value increase by 1 until no collusion like open addressing hash table [39].

B. Decoder Framework

With the hash function and the initial key sequence $K^{(0)}$, the received stego-image can be split into subsequences $\hat{S}^{(i)}, i = \{0, 1, \cdots, M-1\}$. With corresponding initial value d_i, we can rebuild the odd-even uniform quantizers for each subsequence $\hat{S}^{(i)}$. The embedded bit for each component of $\hat{S}^{(i)}$ can be decoded by comparing the minimum distances between each of these two quantizers and each component of $\hat{S}^{(i)}$ and choosing the quantizer with the smaller minimum distance.

C. Security Analysis

Several researchers proposed secure data hiding algorithms [32], [33], which incorporate the security in the process of embedding and are therefore integrated approaches to achieve secure embedding. But the improvement of the security of these algorithms is at the cost of embedding capacity or robustness. In the rest of this section, we will show that the security of the proposed scheme depends only on the length of the key sequence and is independent of the embedding capacity, robustness and distortion caused by embedding.

In this analysis, we assume that the attacker knows the embedding algorithm, the initial value of the quantizers, the dither value $\frac{\Delta}{M}$, and the hash function. The attacker does not know the key sequences and must guess it. The attacker can use the following two methods to crack the key sequences:

1) Exhaustive search in the entire key space.
2) Statistical analysis from the probability distribution of watermarked image.

Option (1) involves searching $\binom{N\times N}{L}$ key sequences. Since $N \times N$ is a large number, this method is computationally expensive if we choose a suitable length for the key sequence. It is possible for an attacker to discover "orthogonal quantizer pairs" (to be described in the next paragraph) by using a statistical analysis of the watermarked image (Option (2)). In the rest of this section, we will focus on the description of the statistical analysis attack method and analysis of the security strength of HRE against this attack.

Since the quantizers for the successive $S^{(i)}$s are separated by $t = \frac{\Delta}{M}$, where Δ is the step size, the quantizer used for embedding a "1" in the subsequence $S^{(i)}$ will coincide exactly with the quantizer used for embedding a "0" in the subsequence $S^{(i+M/2)}$ as seen in Figure-2. We will refer to the quantizers for subsequences $S^{(i)}$ and $S^{(i+M/2)}$ as an orthogonal quantizer pair. So the set of subsequences $\{S^{(i)}\}_{i=0,1,\cdots,M-1}$ can be split into pairs whose quantizers for each member are orthogonal to each other. There are $M/2$ such orthogonal quantizer pairs, one for each pair of

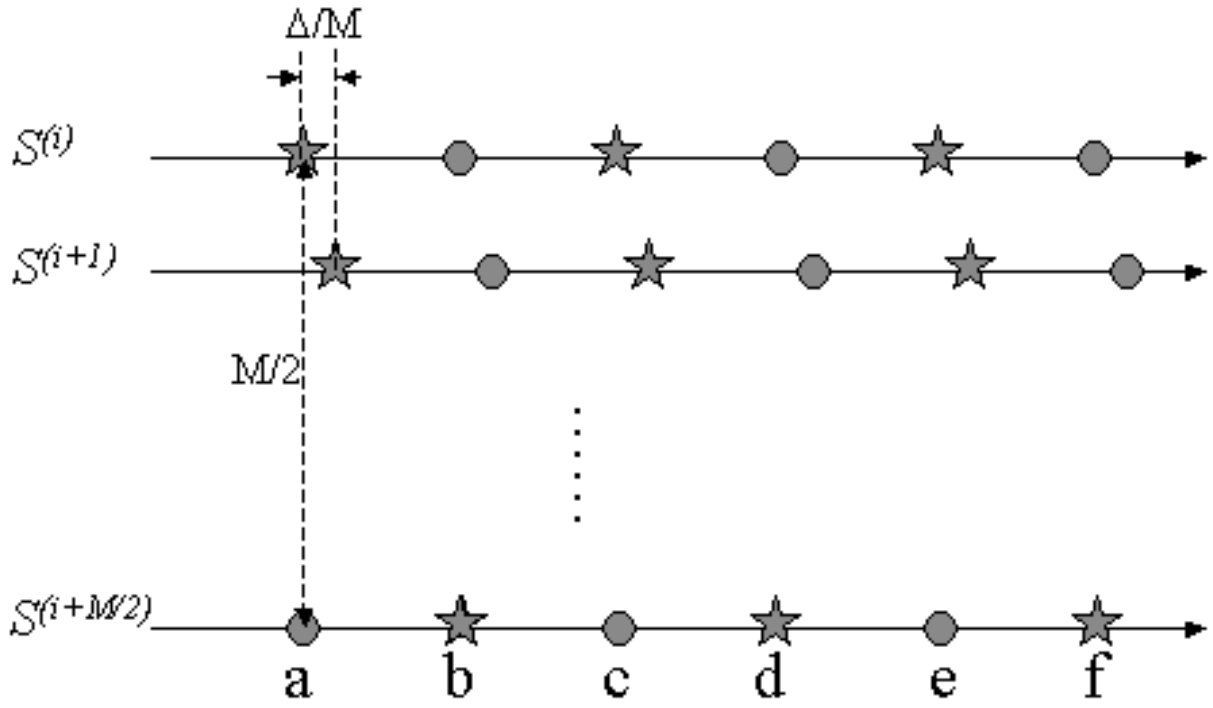

Fig. 2. The quantizer pairs for subsequences $S^{(i)}$, $S^{(i+1)}$,..., and $S^{(i+M/2)}$. The quantizer pair for $S^{(i)}$ and the quantizer pair for $S^{(i+M/2)}$ are orthogonal to each other. $a \backsim f$ are the representation points of the orthogonal quantizer pair for $S^{(i)}$ and $S^{(i+M/2)}$

subsequences $\{S^{(i)}, S^{(i+M/2)}\}_{i=0,1,\cdots,M/2-1}$. We assume that there is no channel noise, $\sigma_n^2 = 0$, hence there is no distortion compensation at the embedder. However, note that distortion compensation can contribute to higher security of our algorithm. The embedding process will replace the pixel values of the subsequences with appropriate representation points from the qantizers.

In order to launch a successful attack, the attacker needs to read the pixel values of the stego-image and maintain a table for each of the orthogonal quantizer pairs. The first row of the table is a list of all the representation points in the orthogonal quantizer pair. For example, for the orthogonal quantizer pair corresponding to subsequences $\{S^{(i)}, S^{(i+M/2)}\}$ in Figure-2, the first row of the table will read a,b,c,d,e,f. The column corresponding to each of these representation points is filled with the positions (in the stego-image) where the corresponding representation point occurs. The number of entries in each table will equal $2L$. There are $M/2$ such tables. Consider the table corresponding to the orthogonal quantizer pair for $\{S^{(0)}, S^{(M/2)}\}$. Obviously,

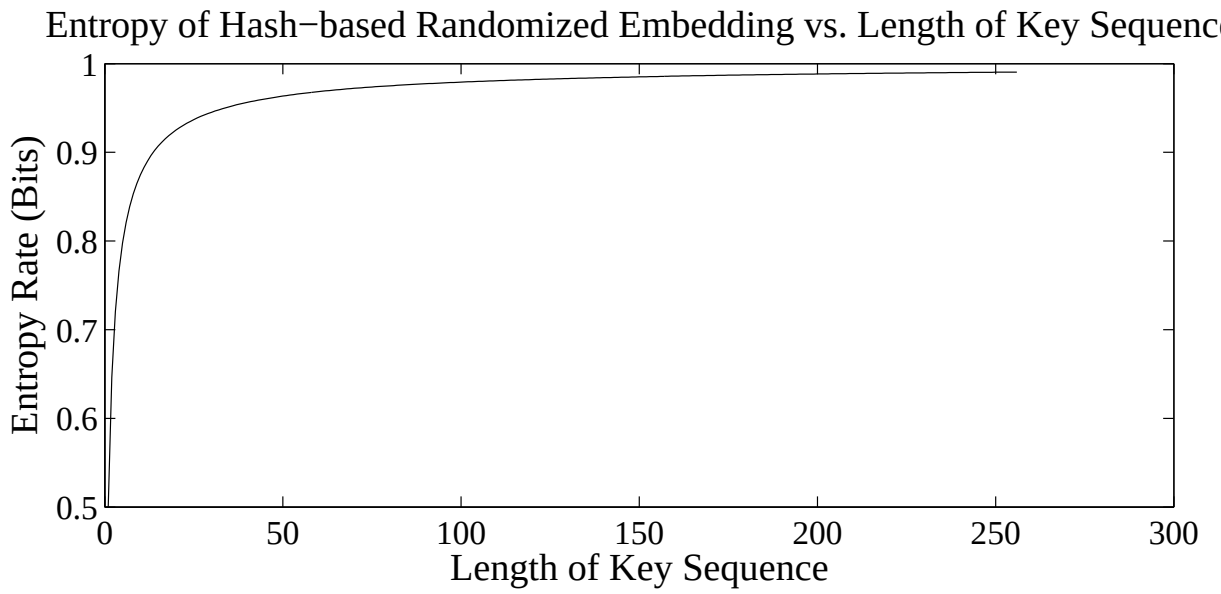

Fig. 3. **The entropy rate for the proposed scheme as a function of the length of the key sequence.**

the $2L$ components in this table belong to sequences $\hat{S}^{(0)}$ and $\hat{S}^{(M/2)}$ with L components each. If the attacker could identify the image positions that belong to $\hat{S}^{(0)}$, the key sequence $K^{(0)}$ is revealed and the security of the proposed algorithm is compromised. There are $\binom{2L}{L}$ possible ways to construct two subsequences of length L from the $2L$ components of the table (corresponding to the orthogonal pair $\{S^{(0)}, S^{(M/2)}\}$). Let $X = \{x_0, x_1, \cdots, x_{(2L-1)}\}$ denote the elements of the table. The entropy of X is given by,

$$\begin{aligned} H(x_0, x_1, \cdots, x_{(2L-1)}) &= \binom{2L}{L}\left[-\frac{1}{\binom{2L}{L}}\right]\log\left[\frac{1}{\binom{2L}{L}}\right] \\ &= \log\binom{2L}{L} \end{aligned} \tag{8}$$

Assuming that the hash function used for key sequence generation is truly secure, the security of our algorithm can be quantified by the average entropy rate, given by

$$H_{HRE} = \frac{1}{2L}H(x_0, x_1, \cdots, x_{(2L-1)}) = \frac{1}{2L}\log\binom{2L}{L}\text{bits} \tag{9}$$

As shown in Figure-3, the strength of the security of our scheme depends only on the length of the key sequence, L. Since the length of the key sequence does not affect the embedding capacity of quantization-based schemes, our scheme has the same capacity as the SCS scheme for the entire watermark noise rate (WNR) range. Moreover, the proposed scheme can achieve stronger security

than LUT embedding by choosing a suitable length for the key sequence.

IV. Optimizing HRE against JPEG Attack

The JPEG standard [40] is widely used for lossy image compression. Using multidimensional lattice structure, Chae et al. proposed an image embedding in DWT domain to improve the robustness of the signature image against JPEG compression attack with host image known at both encoder and receiver end [32], [41]. Several researchers have worked on achieving embedding capacity under JPEG compression attack [36], [42], [43]. Chen et al. [36] experimentally determined the achievable rate-distortion-robustness operating points for both spread transform dither modulation (STDM) and unspread dither modulation(UDM). However, to the best of our knowledge, there is no work on distortion compensation for JPEG compression with different quality factors in STDM and UDM. Moreover, the experimentally obtained operating points for STDM and UDM are not optimal for JPEG compression attack. In this section, we optimize the HRE against JPEG compression attack. Since the JPEG attack is performed in the DCT domain, we assume, in the rest of this section, that our algorithm is also applied in the DCT domain.

JPEG is a transform coding approach based on 8×8 forward digital cosine transform (DCT). The JPEG algorithm uses uniform midtread quantizers with step sizes organized in a table called the *quantization table*, Q. Table-I is an example of a quantization table recommended by ISO and ITU-T [40]. The quality of compression is determined by the quality factor q_f. The quantized value, l_{ij}, of the transform coefficient, θ_{ij}, is given by

$$l_{ij} = \left\lfloor \frac{\theta_{ij}}{s_q Q_{ij}} + 0.5 \right\rfloor \tag{10}$$

where $\lfloor \cdot \rfloor$ is the floor function and s_q is a scalar factor obtained from the quality factor as follows,

$$s_2 = \begin{cases} \frac{50}{q_f}, & \text{if} \quad 0 < q_f < 50; \\ 2 - \frac{q_f}{50}, & \text{if} \quad 50 \leq q_f < 100. \end{cases} \tag{11}$$

The quantization process is the only lossy component in JPEG compression and hence the distortion due to compression is equal to the quantization error.

A. Optimal Embedding for the JPEG Compression Attack

From quantization theory [44], we know that if the standard derivation of the original signal is much greater than the step size of a uniform quantizer (true for low frequency band of DCT

TABLE I

QUANTIZATION TABLE RECOMMENDED BY ISO

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

blocks), the uniform quantizer can be modeled as an additive uniform noise channel, with variance

$$\sigma_q^2(i,j) = \frac{(\Delta_{ij}^{(q)})^2}{12} \tag{12}$$

where $\Delta_{ij}^{(q)}$ is the step size of the uniform quantizer used for compressing the $(i,j)^{\text{th}}$ DCT coefficient and is given by

$$\Delta_{ij}^{(q)} = s_q Q_{ij} \tag{13}$$

Hence JPEG compression can be modeled as a set of uniform noise channels. Note that since the uniform quantizer can be different for each coefficient, the value of $\sigma_{ij}^{(q)}$ can be potentially different for different (i,j). We will refer to the position (i,j) as channel (i,j) in the rest of this paper.

Since our HRE scheme is also uniform quantizer based, the effect of data hiding can also be modeled as an additive uniform noise, W_{ij}, on the host. In order to improve capacity in lower WNR range, a standard trick called distortion compensation (DC) [19] is employed in quantizer based embedding schemes. Figure-6 shows an example of quantizer based embedding with DC for the $(0,1)^{\text{th}}$ channel.

For power constrained AWGN attack, Costa showed that the optimal value of α, $\alpha^*_{ICS} = \frac{\sigma_w^2}{\sigma_w^2+\sigma_n^2}$, where σ_w^2 is the watermark power and σ_n^2 is the power of the AWGN attack [45]. Eggers et al. [20] derived the optimal value of α, α^*_{SCS} for the scalar Costa scheme (SCS) based on a suboptimal codebook, e.g., the product codebook of scalar uniform quantizers. However, no optimal solution for quantization based embedding has been found yet for JPEG compression attack.

In this paper, we derive an expression for the optimal value of α, $\alpha^*_{HRE-JPEG}$, for JPEG attack on our proposed HRE based embedding algorithm. We assume that the hidden data is uniformly

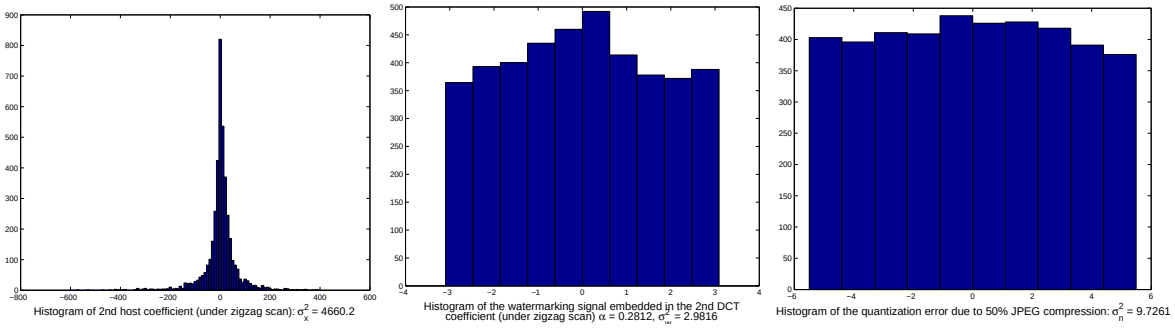

Fig. 4. **The histogram of the second coefficient (under zigzag scan), the histogram of the embedding noise due to embedding a bit '0', and the histogram of the attack noise due to 50% JPEG compression.**

i.i.d. Our analysis is based on the assumption that the power of the host signal is much greater than the power of the embedding induced distortion and the power of the attack noise ($\sigma_x^2 >> \sigma_w^2$ & $\sigma_x^2 >> \sigma_n^2$). This assumption is valid if we choose low frequency DCT coefficients as the host. Figure-4 shows the histograms of the host (2^{nd} DCT coefficient in the zig-zag scan order), the embedded signal, and the noise due to JPEG attack for an example where, WNR $= -5.135dB$, $\alpha = 0.2812$ and the JPEG compression attack is at a quality factor of 50% . In this case, $\sigma_x^2 = 4660.2$, $\sigma_w^2 = 2.9816$, $\sigma_n^2 = 9.7261$. This example clearly illustrates the validity of the assumption.

Uniform quantizer based embedding with distortion compensation depends on two parameters: the quantization step size, Δ, and the distortion compensation factor, α. The embedding power σ_w^2 is given by $\sum_{i,j} \sigma_w^2(i,j)$. Since the noise due to uniform quantizer based embedding, w_{ij}, is uniformly distributed [20] with zero mean, we denote that w_{ij} is uniformly distributed in $[-a, a]$. Let us assume that a is of the form $\frac{s_w Q_{ij}}{2}$, where s_w is a scalar factor determining the strength of watermarking. Then $\sigma_w^2(i,j) = \frac{(s_w Q_{ij})^2}{12}$. Meanwhile, for quantizer based embedding scheme with distortion compensation,

$$\sigma_w^2(i,j) = \frac{(\alpha_{ij}\Delta_{ij}^{(w)})^2}{12}, \tag{14}$$

where $\Delta_{ij}^{(w)}$ is the step size of the quantizer used in the actual embedding process. Then,

$$\Delta_{ij}^{(w)} = \frac{\sqrt{12\sigma_w^2(i,j)}}{\alpha_{ij}} \tag{15}$$

$$\Delta_{ij}^{(w)} = \frac{\sqrt{12\frac{(s_w Q_{ij})^2}{12}}}{\alpha_{ij}} = \frac{s_w Q_{ij}}{\alpha_{ij}} \tag{16}$$

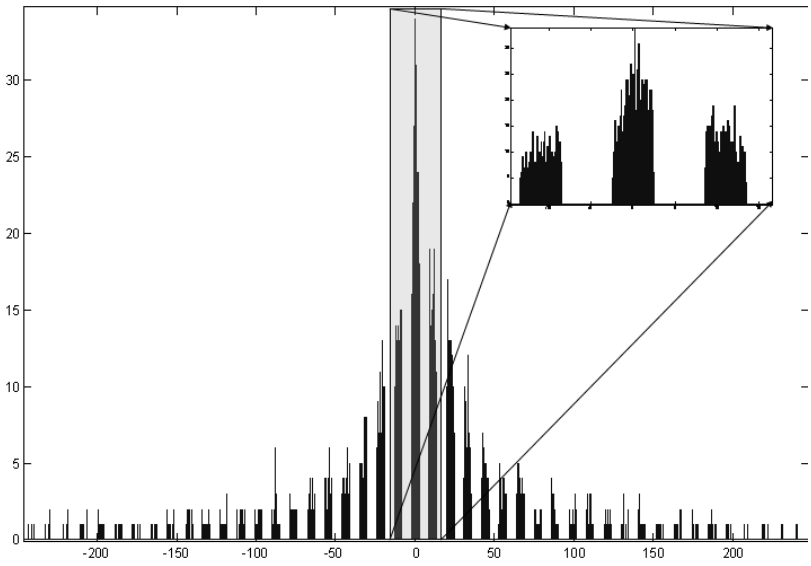

Fig. 5. **The histogram of the second stego coefficient with zigzag scan.**

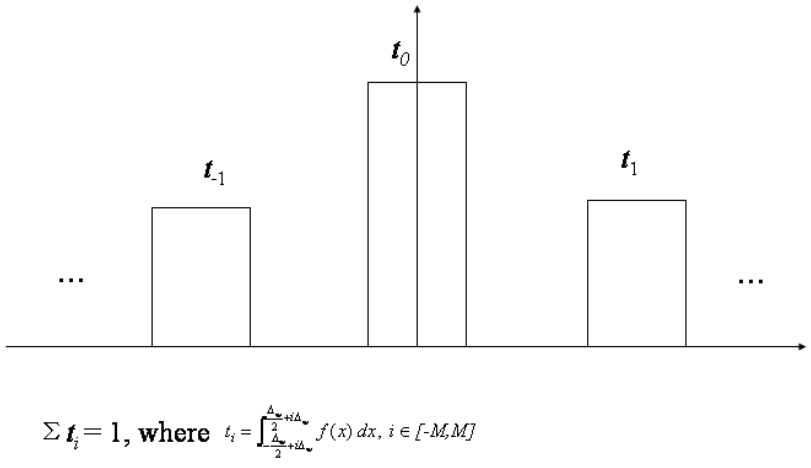

Fig. 6. **The analysis model approximating the *pdf* of the stego-coefficient with uniform distributed bars**

Since the rest of our analysis is based on the $(i,j)^{\text{th}}$ channel, we drop the suffix (i,j) from the parameters. For example: $\Delta_w = \Delta_{ij}^{(w)}, \Delta_q = \Delta_{ij}^{(q)}$, and $\alpha = \alpha_{ij}$.

Figure-5 is the histogram of the 2nd stego-coefficient $\hat{X}$ under zigzag scan, if we use the uniform quantization based data hiding scheme with distortion compensation. Figure-4 shows the histogram of the quantization error of the second coefficient caused by the 50% JPEG compression. We can

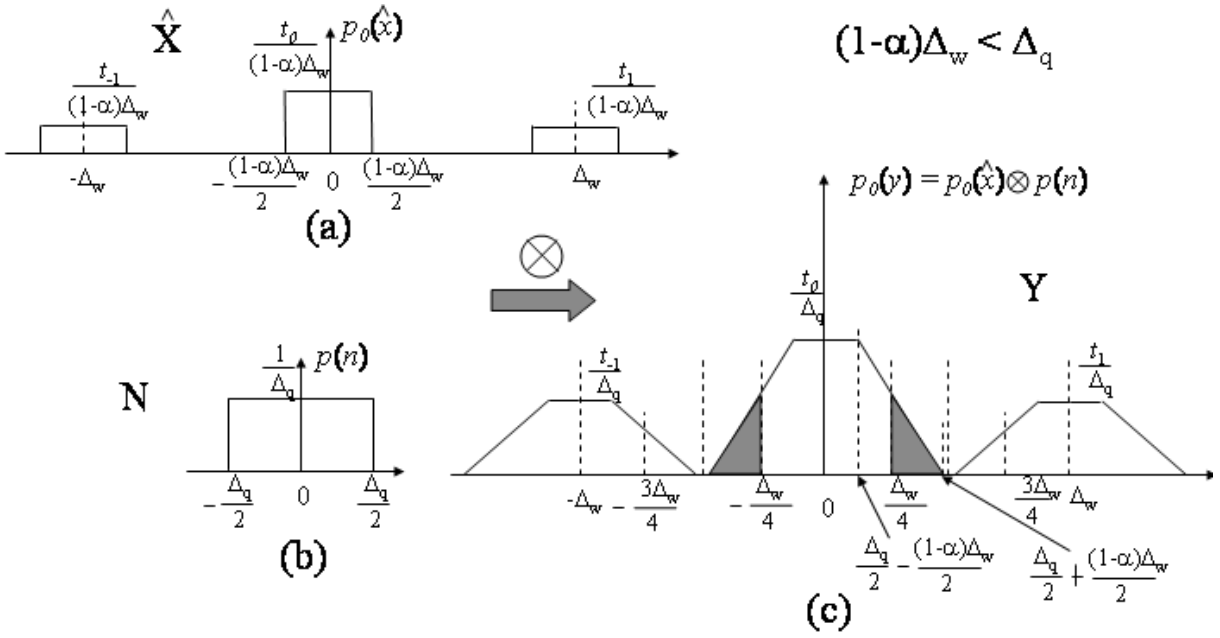

Fig. 7. **The *pdf* of Stego-signal for embedding bit "0" ($p_0(\hat{x})$),the *pdf* of the uniform noise ($p(n)$) and the *pdf* of the attacked stego-signal ($p_0(y)$) in the $(i,j)^{\text{th}}$ channel, if $(1-\alpha)\Delta_w < \Delta_q$**

model the *pdf* of $\hat{X}$ as a bunch of rectangle bars shown in Figure-6, in which the area of each bar

$$t_i = \int_{\frac{-\Delta_w}{2}+i\Delta_w}^{\frac{\Delta_w}{2}+i\Delta_w} f(x)\ dx, \tag{17}$$

where $f(x)$ is the pdf of the host coefficient X.

Let $\hat{X}$ denote the stego-signal in the $(i,j)^{\text{th}}$ channel , N denote the uniform channel noise due to JPEG attack, and Y be the signal at the receiver end of the $(i,j)^{\text{th}}$ channel. We denote the pdf of $\hat{X}$ corresponding to embedding a bit "k" as $p_k(\hat{x})$, the pdf of N as $p(n)$, and the corresponding pdf of Y as $p_k(y)$, where $k = \{0,1\}$. Then

$$p_k(y) = p_k(\hat{x}) \otimes p(n), \quad k = 0,1 \tag{18}$$

where $\otimes$ denotes "convolution". Depending on the relation between Δ_q and $(1-\alpha)\Delta_w$, there are two cases of $p_k(y)$. In the rest of this section, we will derive the optimal value of α for both cases.

B. The Optimization of α

Case 1: $(1-\alpha)\Delta_w < \Delta_q$: $p_0(\hat{x})$ is shown in Figure-7-(a). $p_1(\hat{x})$ is the same as $p_0(\hat{x})$ with a shift of $\Delta_w/2$. According to the Equation-18, $p_0(y)$ is shown in Figure-7-(c). It is obvious that the hidden

"0" can be decoded without error if y_0 lies in $(-\frac{\Delta_w}{4}+i\Delta_w, \frac{\Delta_w}{4}+i\Delta_w)$, where $i \in \{-M, ..., 0, 1, M\}$ and M is the level of the uniform quantizer used for embedding. On the other hand, the probability of error $P_e = \int_{\frac{\Delta_w}{4}+i\Delta_w}^{\frac{3\Delta_w}{4}+i\Delta_w} f(x)dx$. As shown in Figure-7, concerning $\hat{X}$ lying in $[-\frac{(1-\alpha)\Delta_w}{2}, \frac{(1-\alpha)\Delta_w}{2}]$, $\hat{X}_{t_0}$, the caused probability of error by N,

$$P_e^{(t_0)} = \int_{\frac{\Delta_w}{4}}^{\frac{(1-\alpha)\Delta_w}{2}+\frac{\Delta_q}{2}} f(y_{t_0})dy + \int_{-\frac{(1-\alpha)\Delta_w}{2}-\frac{\Delta_q}{2}}^{-\frac{\Delta_w}{4}} f(y_{t_0})dy, \tag{19}$$

$$= 2\int_{\frac{\Delta_w}{4}}^{\frac{(1-\alpha)\Delta_w}{2}+\frac{\Delta_q}{2}} f(y_{t_0})dy \tag{20}$$

which is equal to the area of these two shaded triangles. Using geometrical analysis, we can get the area of both shaded triangles $S = 2 * \frac{1}{2}t_0 * (\frac{(1-2\alpha)\Delta_w+2\Delta_q}{4(1-\alpha)\Delta_w\Delta_q}) * (\frac{(1-\alpha)\Delta_w}{2} + \frac{\Delta_q}{2} - \frac{\Delta_w}{4})$. So,

$$P_e^{(t_0)} = S = 2 * \frac{1}{2}t_0 * (\frac{(1-2\alpha)\Delta_w + 2\Delta_q}{4(1-\alpha)\Delta_w\Delta_q}) * (\frac{(1-\alpha)\Delta_w}{2} + \frac{\Delta_q}{2} - \frac{\Delta_w}{4}), \tag{21}$$

Using Equation-16and 13,

$$P_e^{(t_0)} = t_0\frac{((1-2\alpha)s_w + 2\alpha s_q)^2}{8(1-\alpha)\alpha s_w s_q} \tag{22}$$

Using the same method, we can get the probability of error for each bar,

$$P_e^{(t_i)} = t_i\frac{((1-2\alpha)s_w + 2\alpha s_q)^2}{8(1-\alpha)\alpha s_w s_q} \tag{23}$$

According to Equation 17,

$$\sum_{i=-M}^{M} t_i = 1; \tag{24}$$

So,

$$P_e = \sum_{i=-M}^{M} P_e^{(t_i)} \tag{25}$$

$$= \sum_{i=-M}^{M} t_i\frac{((1-2\alpha)s_w + 2\alpha s_q)^2}{8(1-\alpha)\alpha s_w s_q} \tag{26}$$

$$= \frac{((1-2\alpha)s_w + 2\alpha s_q)^2}{8(1-\alpha)\alpha s_w s_q} \tag{27}$$

The stego-signal $\hat{X}_{ij}$ for embedding a bit "1" is equal to the stego-signal $\hat{X}_{ij}$ for embedding a bit "0" with a $\Delta_w/2$ shift. Obviously, the attacked stego-signal for embedding bit "1" of the $(ij)^{th}$ *channel* is also equal to $p_0(y_{ij})$ with a $\Delta_w/2$ shift. Using the same method, we can get the probability of error for embedding a bit "1" is equal to P_e.

To minimize P_e with respect to α, we set $\frac{\partial P_e}{\partial \alpha} = 0$ and solve for α to get α^*. The solutions are:

$$\alpha^* = \{\frac{s_w}{2s_q}, \frac{s_w}{2(s_w - s_q)}\} \tag{28}$$

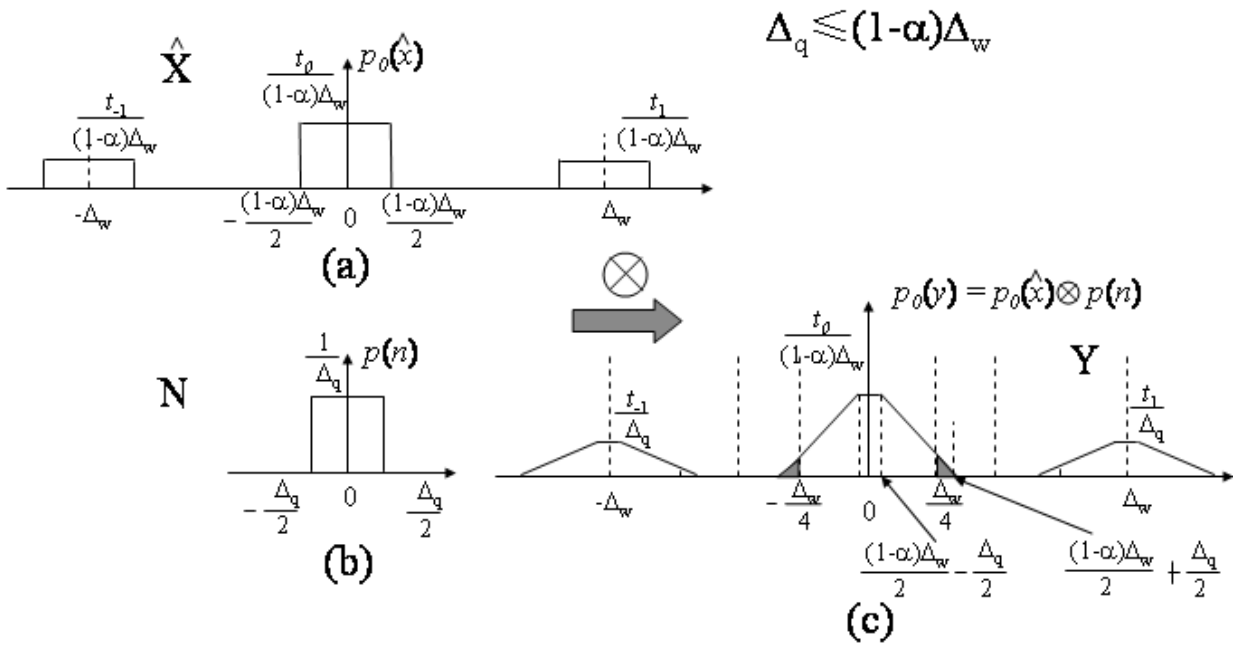

Fig. 8. **The *pdf* of Stego-signal for embedding bit "0" ($p_0(\hat{x})$),the *pdf* of the uniform noise ($p(n)$) and the *pdf* of the attacked stego-signal ($p_0(y)$) in the $(i,j)^{\text{th}}$ channel, if $\Delta_q \leq (1-\alpha)\Delta_w$**

Consider $\alpha^* = \frac{s_w}{2(s_w - s_q)}$. We know that $0 < \alpha^* < 1$, therefore $2(s_w - s_q)\alpha^* = s_w \Rightarrow s_w \geq 2s_q$. However, if this is true, it implies that the attack noise (s_q) is only half the watermark induced noise (s_w). So there is no need for distortion compensation in this case. So we take the other result for α^*, viz, $\alpha^* = \frac{s_w}{2s_q}$.

To show that P_e over α^* is indeed the minimum value, we compute

$$\frac{\partial^2 P_e}{\partial \alpha^2}|_{\alpha=\frac{s_w}{2s_q}} = \frac{4s_q}{2s_w - s_w^{3/2}}, \tag{29}$$

$\frac{\partial^2 P_e}{\partial \alpha^2}|_{\alpha=\frac{s_w}{2s_q}} > 0$, if $s_w < 2s_q$. So

$$P_e|_{\alpha^*=\frac{s_w}{2s_q}} = \min_{0<\alpha<1} P_e, \quad \text{if} \quad s_w < 2s_q. \tag{30}$$

We note that α^* is independent of (i,j), which means it is the same for all *channels*. Therefore, we get the optimal α, α^* of HRE for JPEG compression attack as:

$$\alpha^*_{HRE-JPEG} = \begin{cases} \frac{s_w}{2s_q}, & \text{if} \quad s_w < 2s_q \\ 1 & \text{if} \quad s_w \geq 2s_q \end{cases} \tag{31}$$

Case 2: $\Delta_q \leq (1-\alpha)\Delta_w$:

In this case, the received signal Y is slightly different from Case 1, as shown in Figure-8-(c). Consider $\hat{X}$ lying in $[-\frac{(1-\alpha)\Delta_w}{2}, \frac{(1-\alpha)\Delta_w}{2}]$, $\hat{X}_{t_0}$, the probability of error caused by addition of noise N is,

$$P_e^{(t_0)} = \int_{\frac{\Delta_w}{4}}^{\frac{(1-\alpha)\Delta_w}{2}+\frac{\Delta_q}{2}} f(y_{t_0})dy + \int_{-\frac{(1-\alpha)\Delta_w}{2}-\frac{\Delta_q}{2}}^{-\frac{\Delta_w}{4}} f(y_{t_0})dy, \tag{32}$$

$$= 2\int_{\frac{\Delta_w}{4}}^{\frac{(1-\alpha)\Delta_w}{2}+\frac{\Delta_q}{2}} f(y_{t_0})dy \tag{33}$$

which is equal to the area of these two shaded triangles.

$$P_e^{(t_0)} = 2 * \frac{1}{2} t_0 * (\frac{(1-2\alpha)\Delta_w + 2\Delta_q}{4(1-\alpha)\Delta_w\Delta_q}) * (\frac{(1-\alpha)\Delta_w}{2} + \frac{\Delta_q}{2} - \frac{\Delta_w}{4}), \tag{34}$$

Using Equation-16and 13,

$$P_e^{(t_0)} = t_0 \frac{((1-2\alpha)s_w + 2\alpha s_q)^2}{8(1-\alpha)\alpha s_w s_q} \tag{35}$$

Then following similar logic as in Case 1, we have

$$P_e = \frac{((1-2\alpha)s_w + 2\alpha s_q)^2}{8(1-\alpha)\alpha s_w s_q} \tag{36}$$

Obviously, the optimal value of α, α^*, in this case will also be the same as Equation-31. Hence, the optimal value of α for JPEG attack, $\alpha^*_{HRE-JPEG}$, is given by Equation-31. The WNR in this case is given by

$$\text{WNR} = \frac{\sigma_w^2}{\sigma_n^2} = \frac{(s_w\Delta_q)^2/12}{(s_q\Delta_q)^2/12} = \frac{s_w^2}{s_q^2} \tag{37}$$

Expressing $\alpha^*_{HRE-JPEG}$ in terms of the WNR gives

$$\alpha^*_{HRE-JPEG} = \begin{cases} \frac{\sqrt{\text{WNR}}}{2}, & \text{if} \quad \text{WNR} < 4 \\ 1 & \text{if} \quad \text{WNR} \geq 4 \end{cases} \tag{38}$$

The graph of α^* versus WNR are shown in Figure-9 for the ICS, SCS and HRE-JPEG.

V. Experimental Results

A. Joint Security and Capacity Measure under AWGN Attack

We used the 512x512 Barbara image as the host and a random bit sequence with $Pr(0) = Pr(1) = 1/2$, was embedded. Figure-10 compares the performance of the proposed HRE algorithm against that of the LUT embedding [33] in terms of the capacity achieved under AWGN attacks. We base the robustness comparison on the watermark distortion to noise ratio (WNR $= \sigma_w^2/\sigma_n^2$) in order to ensure a fair comparison. The results of our comparison are presented as capacity

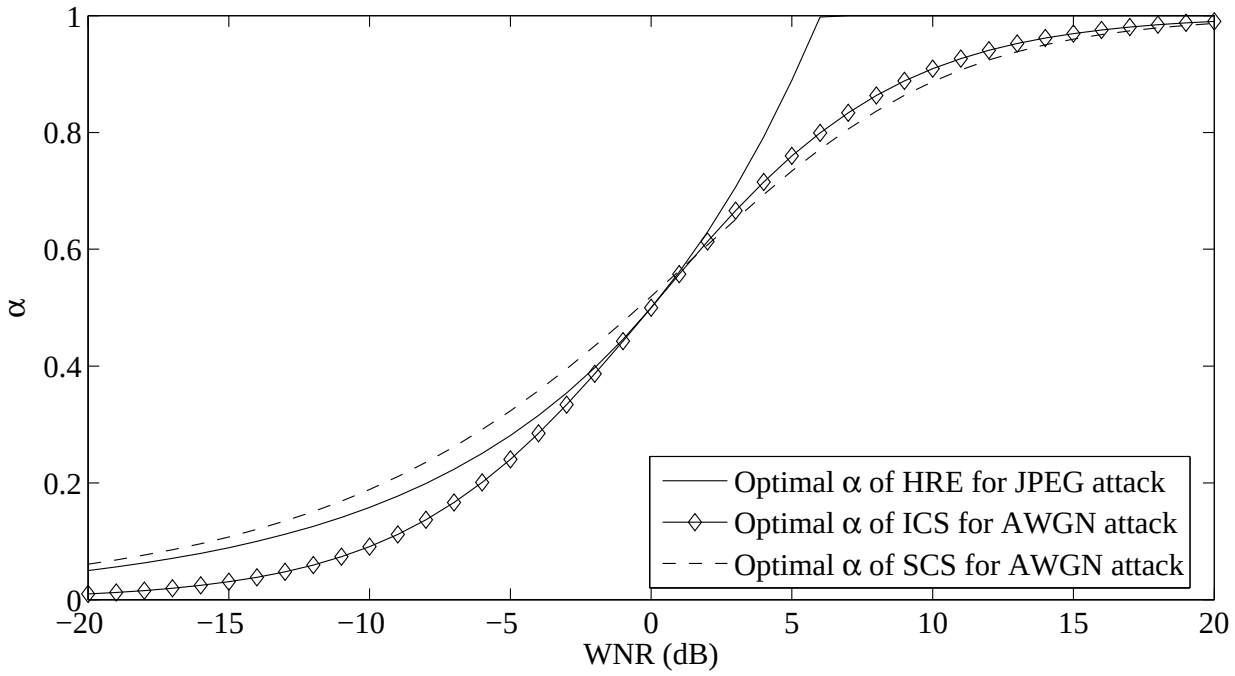

Fig. 9. **Comparison between the optimal α^* of ICS, SCS for the AWGN attack and HRE for the JPEG attack vs WNR**

versus WNR plot in the Figure-10. As seen from this figure, the HRE scheme has almost the same performance as $run = 1$ LUT embedding with compensation. However, the LUT embedding with $run = 1$ does not have any security. If we use a long key sequence in the HRE scheme ($l_k = 400$), we can achieve better security than run $r \leq 8$ LUT embedding, as measured by H_{LUT} and H_{HRE}. We compare joint security and robustness between HRE and LUT embedding schemes in Figure-11, using the joint measure $J(H, C)$ defined in [33], $J = \omega H + (1 - \omega)C$, where H is the entropy rate of the schemes, C is the embedding capacity and ω is a linear factor between 0 and 1. As shown in Figure-11, the HRE scheme enhances the joint security and robustness significantly compared to LUT embedding. The capacity achieved by the HRE scheme is equal to the capacity achieved by the LUT scheme without security ($r = 1$), meanwhile the HRE scheme with length of key sequence ($l_k = 50$) can yield better security than the LUT scheme with $r \leq 5$. Moreover, the capacity achieved by the LUT scheme will decrease drastically as r increases. On the other hand, the capacity achieved by the HRE scheme is not affected by the length of the key sequence (l_k).

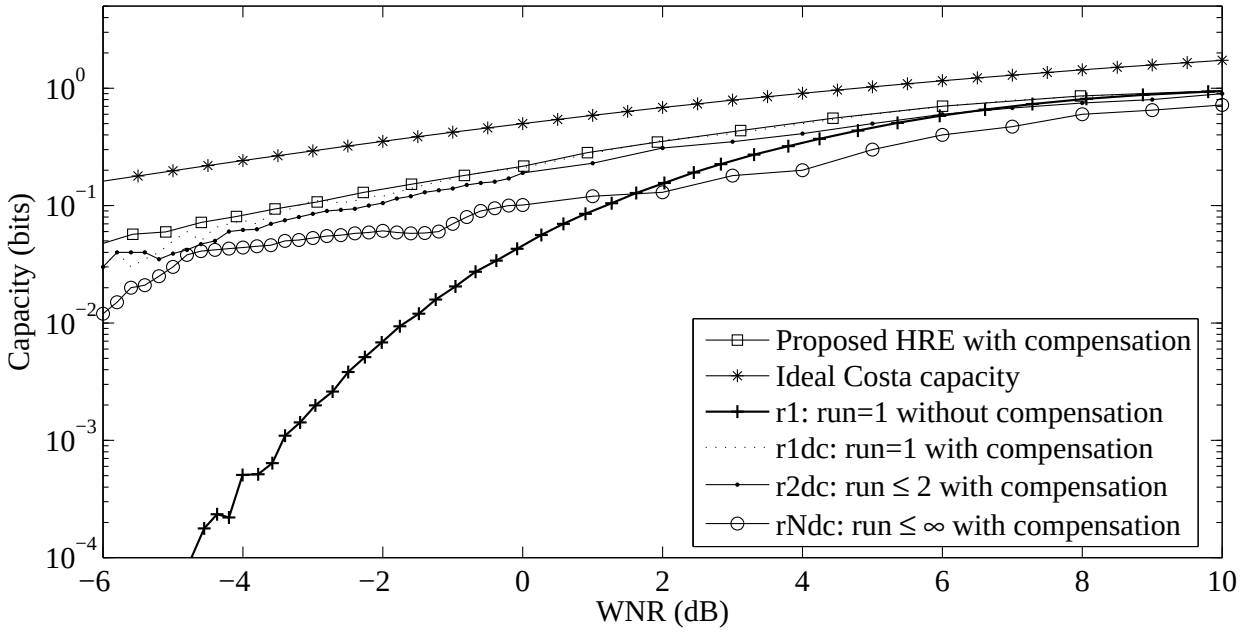

Fig. 10. **Comparison of embedding capacity of the proposed algorithm with the LUT algorithm under different maximum allowable LUT runs and different compensation settings**

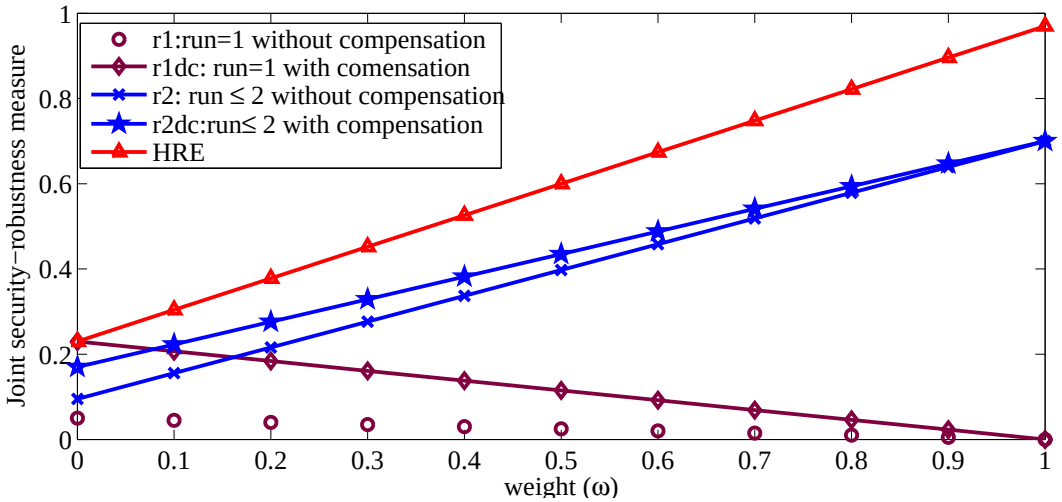

Fig. 11. **Joint security and capacity measure comparison of LUT and HRE embedding as a function of weight ω at a WNR of 0 dB.**

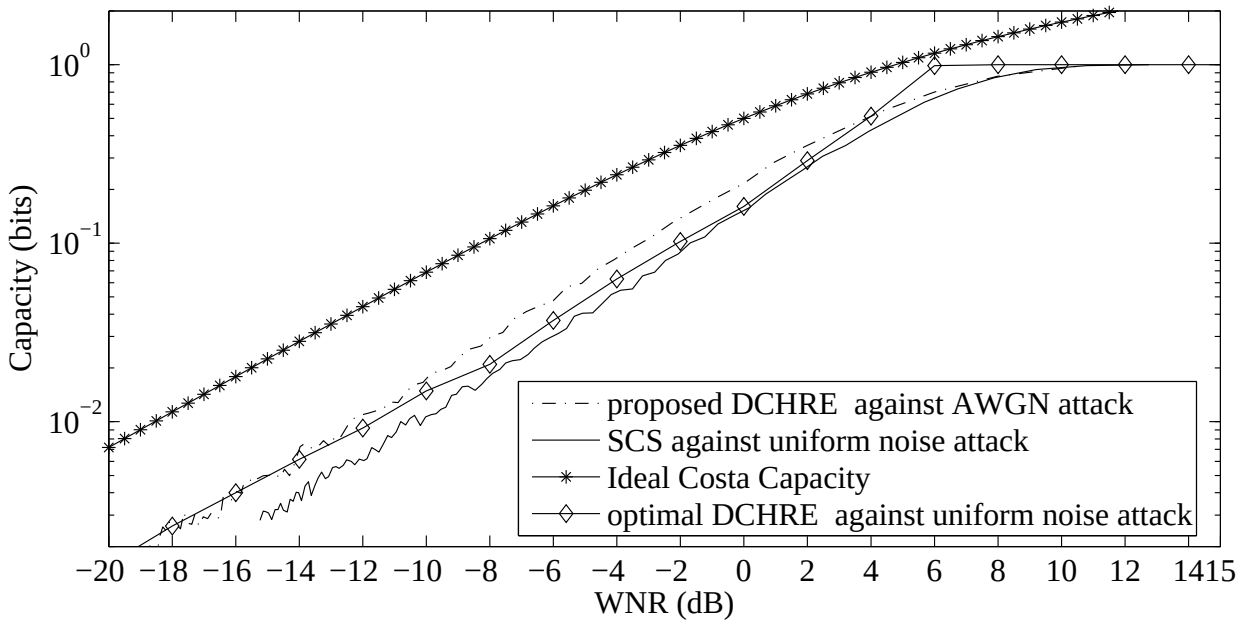

Fig. 12. **Capacity comparison between SCS and HRE for AWGN attack and JPEG attack**

B. Performance of HRE under JPEG Attack

Using the HRE algorithm, we embed the hidden data in the midband coefficients of DCT domain. As shown in Figure-12, the HRE scheme with $\alpha^*_{HRE-JPEG}$ as given by Equation-31 achieves better capacity than the SCS scheme over the entire WNR range. Figure-13 shows the watermarked image with embedding rate 1/64. After 25 % JPEG compression, all embedded bits can be extracted with no error. Figure-14 shows the achievable distortion-robustness trade-offs for the HRE, STDM and UDM schemes [36] at an embedding rate, R_m, of 1/320 bits per grayscale pixel and various JPEG quality factors (Q_{JPEG}). In this figure, we measure the distortion in terms of the peak signal-to-distortion ratio (PSDR) which is defined as the ratio between the square of the maximum possible pixel value and the average embedding-induced distortion per pixel. From Figure-14,we can see that HRE_{JPEG} is better than STDM by about 7 dB at a robustness$(100 - Q_{JPEG})$ [36] of 50 and 75.

VI. Conclusion

In this paper we proposed a new secure quantization based data embedding algorithm and derived a mathematical expression for its security. Using this metric, we showed that the security of our algorithm can be increased independent of capacity, robustness and embedding induced

Fig. 13. **Left: Original Barbara image, Right: Watermarked Barbara image(PSNR = 42.11 dB). The embedding rate is 1/64. After 25% JPEG compression, all embedded bits can be extracted with no error**

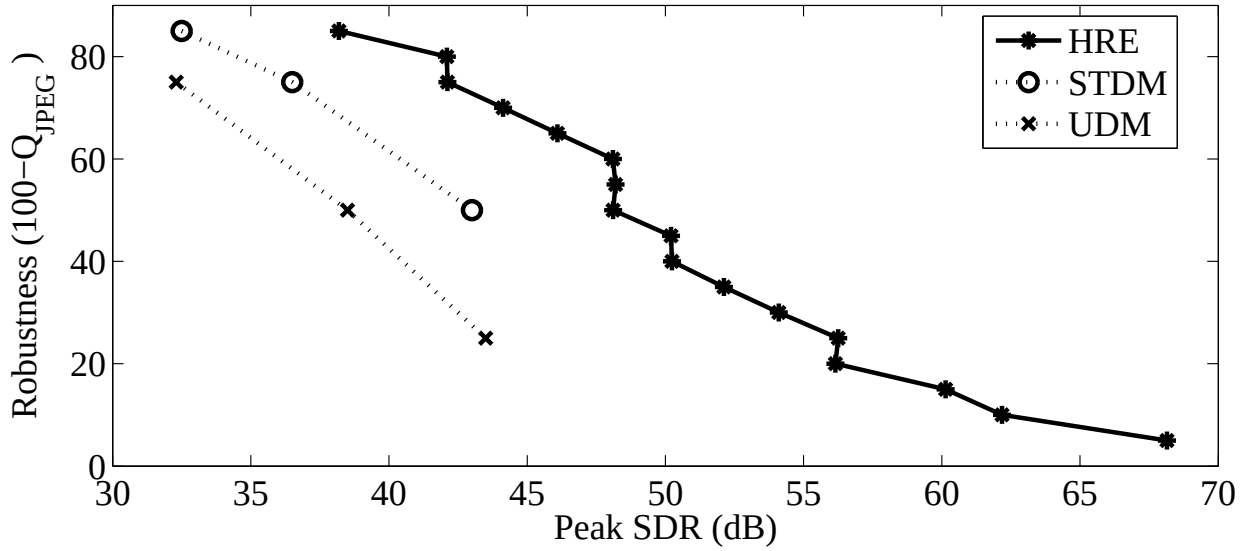

Fig. 14. **Robustness comparison between UDM,STDM and HRE against JPEG compression.** $R_m = 1/320$**. The bit-error rate is less than** 5×10^{-6}**.**

distortion. The proposed HRE algorithm provides joint security and robustness improvement over the traditional quantization based embedding scheme and LUT algorithm.

We then apply the HRE algorithm in the DCT domain and model both the embedding induced noise and quantization error due to JPEG compression (the attacking noise) as additive uniform noise. The expression of the bit error rate, P_e, is then derived based on the *pdf* of the attacked stego-signal. The optimal distortion compensation factor $\alpha^*_{HRE-JPEG}$ is then obtained by minimizing P_e over α. The optimal solution for quantizer based embedding against JPEG compression attack is achieved by applying $\alpha^*_{HRE-JPEG}$ in the proposed HRE algorithm.

Experimental results showed that the proposed scheme achieves the same embedding capacity as SCS against AWGN attack, while the security of the system is enhanced by 0.17 over the run $r \leq 2$ LUT based embedding scheme in terms of entropy rate. On the other hand, the HRE_{JPEG} algorithm causes 7 dB less distortion than STDM at fixed embedding rate and robustness against JPEG compression attack.

References

[1] E. Lin, A. Eskicioglu, R. Lagendijk, and E. Delp, "Advances in digital video content protection," in *Proceedings of the IEEE*, vol. 93, no. 1, Jan. 2005.

[2] I. Cox and M. Miller, "The first 50 years of electronic watermarking," *EURASIP Journal on Applied Signal Processing*, vol. 2002, no. 2, pp. 126–132, Feb. 2002.

[3] F. Mintzer, G. Braudaway, and M. M. Yeung, "Effective and ineffective digitalwatermarks," in *Proc. IEEE International Conference on Image Processing (ICIP'97)*, 1997.

[4] C. Lu, H.-Y. Liao, and M. Kutter, "Denoising and copy attacks resilient watermarking by exploiting prior knowledge at detector," *IEEE Transactions on Image Processing*, vol. 11, no. 3, pp. 280–292, Mar. 2002.

[5] P. Wong and N. Memon, "Secret and public key image watermarking schemes for image authentication and ownership verification," *IEEE Transactions on Image Processing*, vol. 10, no. 10, pp. 1593–1601, Oct. 2001.

[6] B. Macq, J. Dittmann, and E. Delp, "Benchmarking of image watermarking algorithms for digital rights management," in *Proceedings of the IEEE*, vol. 92, no. 6, June 2004, pp. 971–984.

[7] J. Fridrich, "Applications of data hiding in digital images," in *Proceedings of the Fifth International Symposium on Signal Processing and Its Applications (ISSPA '99)*, Aug. 1999.

[8] M. Maes, T. Kalker, J.-P. Linnartz, J. Talstra, F. Depovere, and J. Haitsma, "Digital watermarking for dvd video copy protection," *IEEE Signal Processing Magazine*, vol. 17, no. 5, pp. 45–60, Sept. 2000.

[9] M. Utku-Celik, G. Sharma, E. Saber, and A. Murat-Tekalp, "Hierarchical watermarking for secure image authentication with localization," *IEEE Transactions on Image Processing*, vol. 11, no. 6, pp. 585–595, June 2002.

[10] D. Kundur, "Multiresolution digital watermarking: Algorithms and implications for multimedia signals," Ph.D. dissertation, University of Toronto, Toronto, ON, Canada, 1999.

[11] M. Ramkumar, "Data hiding in multimedia-theory and applications," Ph.D. dissertation, New Jersey Institute of Technology, Newark, NJ, 2000.

[12] C.-Y. Lin, "Watermarking and digital signature techniques for multimedia authentication and copyright protection," Ph.D. dissertation, Columbia University, New York, NY, 2000.

[13] R. Venkatesan and M. H. Jakubowski, "Image watermarking with better resilience," in *Proceedings. 2000 International Conference on Image Processing*, vol. 1, no. 10-13, Sept. 2000, pp. 403–406.

[14] A. C. K. L. C. Haiping Lu, Yun Q. Shi, "Binary image watermarking through blurring and biased binarization," *International Journal of Image and Graphics*, vol. 5, no. 1, pp. 1–21, 2005.

[15] S. Kay and E. Izquierdo, "Improving watermark robustness by combining spatial and frequency domain strategies," in *Proc. 9th Int. Conference on Telecommunication Systems, Modeling and Analysis*, Mar. 2001.

[16] Z. Du, Y. Zou, and P. Lu, "An optimized spatial data hiding scheme combined with convolutional codes and hilbert scan," in *Proceedings of the Third IEEE Pacific Rim Conference on Multimedia: Advances in Multimedia Information Processing*, 2002, pp. 97–104.

[17] C.-Y. Lin and S.-F. Chang, "Watermarking capacity of digital images based on domain-specific masking effects zero-error information hiding capacity for digital image," in *IEEE International Conference On Information Technology: Coding and Computing*, Las Vegas, Apr. 2001.

[18] C.-T. Hsu and J.-L. Wu, "A DWT-DFT composite watermarking scheme robust to both affine transform and jpeg compression," *IEEE Transactions on Circuits System and Video Technology*, 2003.

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

[20] J. Eggers, R. Bäuml, R. Tzschoppe, and B. Girod, "Scalar costa scheme for information embedding," *IEEE Transactions on Signal Processing*, vol. 51, pp. 1003 –1019, 2003.

[21] F. Perez-Gonzalez, F. Balado, and J. Martin, "Performance analysis of existing and new methods for data hiding with known-host information in additive channels," *IEEE Transactions on Signal Processing*, vol. 51, no. 4, pp. 960 –980, 2003.

[22] N. Liu and K. P. Subbalakshmi, "Vector quantization based scheme for data hiding for images," in *Proc. SPIE International Conference on Electronic Images'04*, San Jose, CA, Jan. 2004.

[23] ——, "Non-uniform quantizer design for image data hiding," in *IEEE International Conference on Image Processing*, Singapore, Oct. 2004.

[24] W. Bender, D. Gruhl, and N. Morimoto, "Techniques for data hiding," in *Proc. SPIE*, vol. 2420, 1995.

[25] I. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Transactions on Image Processing*, vol. 6, pp. 1673–1687, Dec. 1997.

[26] D. F. HS Malvar, "Improved spread spectrum: a new modulation technique for robust watermarking," *IEEE Transactions on Signal Processing*, 2003.

[27] A. K. Goteti and P. Moulin, "QIM watermarking games," in *Proc. IEEE International Conference on Image Processing (ICIP'04)*, Singapore, Oct. 2004.

[28] R. Tzschoppe, R. Bauml, R. Fischer, J. Huber, and A. Kaup, "Additive non-gaussian noise attacks on the scalar costa scheme (scs)," in *Proc. SPIE International Conference on Electronic Images'05*, vol. 5681, San Jose, CA, Jan. 2005.

[29] J. Vila-Forcen, S. Voloshynovskiy, O. Koval, F. Perez-Gonzalez, and T. Pun, "Worst case additive attack against quantization-based data-hiding methods," in *Proc. SPIE International Conference on Electronic Images'05*, vol. 5681, San Jose, CA, Jan. 2005.

[30] P. Moulin and A. Briassouli, "A stochastic QIM algorithm for robust, undetectable image watermarking," in *Proc. IEEE International Conference on Image Processing (ICIP'04)*, Singapore, Oct. 2004, pp. 1173–1176.

[31] M. Swanson, B. Zhu, and A. Tewfik, "Multiresolution scene-based video watermarking using perceptual models," *IEEE journal on selected areas in communications*, vol. 16, pp. 540–550, May 1998.

[32] J. Chae, D. MukherJee, and B. Manjunath, "Color image embedding using multidimensional lattice structures," in *Proc. IEEE International Conference on Image Processing (ICIP'98)*, 1998.

[33] M. Wu, "Joint security and robustness enhancement for quantization based data embedding," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 831–841, Aug. 2003.

[34] M. M. Yeung and F. Mintzer, "An invisible watermarking technique for image verification," in *Proc. IEEE International Conference Image Processing (ICIP'97)*, vol. 2, Santa Barbara, CA, 1997, pp. 680–683.

[35] M. Wu and B. Liu, "Data hiding in image and video: part-i¡ªfundamental issues and solutions," *IEEE Transactions on Image Processing*, vol. 12, p. 685¨C695, June 2003.

[36] B. Chen and G. W. Wornell, "Quantization index modulation methods for digital watermarking and information embedding of multimedia," *Journal of VLSI Signal Processing*, vol. 27, pp. 7–33, 2001.

[37] M. Wu and B. Liu, "Watermarking for image authentication," in *Proc. IEEE International Conference on Image Processing (ICIP'98)*, Chicago, IL, 1998.

[38] R. L. Rivest, "The MD5 message digest algorithm, request for comments (RFC)1321," *Internet Activities Board, Internet PrivacZ Task Force*, vol. 3RIPEMD-1281, Apr. 1992.

[39] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, *Introduction To Algorithms 2nd Ed,.* Cambridge, MA: The MIT Press, 2001.

[40] W. B. Pennebaker and J. L. Mitchell, *JPEG : Still Image Data Compression Standard.* Norwell, MA: Kluwer Academic Publishers, Dec. 1992.

[41] J. Chae, D. MukherJee, and B. Manjunath, "A robust data hiding using the multidimensional lattice," in *Proc. IEEE International Conference of ADL (ADL'98)*, Santa Barbara, Apr. 1998, pp. 319–326.

[42] K. Solanki, N. Jacobsen, U. Madhow, B. S. Manjunath, and S. Chandrasekaran, "Robust image-adaptive data hiding using erasure and error correction," *IEEE Transactions on Image Processing*, vol. 13, no. 12, pp. 1627–1639, Dec. 2004.

[43] P. H. W. Wong and O. C. Au, "A capacity estimation technique for jpeg-to-jpeg image watermarking," *IEEE Transation on Circuits and Systems for Video Technology*, vol. 13, no. 8, pp. 746–752, Aug. 2003.

[44] K. Sayood, *Introduction to Data compression 2nd Ed.* San Francisco, CA: Morgan Kayfmann Publishers, 2000.

[45] M. Costa, "Writing on dirty paper," *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 439–441, 1983.

PLACE PHOTO HERE

Ning Liu received the B.E in Electrical Engineering from the Sichuan University, China in 1995, and the M.E in Signal Processing Engineering from the Tongji University, China in 2001. Since Fall 2002, He has been a Ph.D. student in the Department of Electrical and Computer Engineering, Stevens Institute of Technology, Hoboken, NJ, where he works in the MSyNC lab under the guidance of Prof. Subbalakshmi. His research interests include quantizer based steganography and stego-games, digital image/video watermarking, joint source channel coding.

PLACE PHOTO HERE

Palak Amin received the B.E. and the M.E. degree both in Computer Engineering from the Department of Electrical and Computer Engineering, Stevens Institute of Technology, Hoboken, NJ in 2003. He is currently working towards the Ph.D. degree in Computer Engineering at Stevens Institute of Technology, Hoboken, NJ. He was with the MedSW-West Lab, Siemens Medical Solutions at Iselin, NJ during 2001-2002. His research interests include multimedia security - digital image/video watermarking, statistical security, distributed source channel coding (DSCC), and multiple description coding (MDC).

PLACE PHOTO HERE

K. P. Subbalakshmi is an Assistant Professor in the Department of Electrical and Computer Engineering, Stevens Institute of Technology, Hoboken, NJ, where she co-directs the MSyNC: Multimedia Systems Networking and Communications Laboratory.

She is the Program Chair of the IEEE GLOBECOM 2006 Symposium on Information and Communication Security and a guest editor of the IEEE Journal on Selected Areas of Communication, Special Issue on Cross-Layer Wireless Multimedia Communications. She is the Chair of the Special Interest Group on Multimedia Security within the IEEE Multimedia Communication Technical Committee. Dr. Subbalakshmi leads research projects in information security, error resilient encryption , joint source-channel and distributed source-channel coding. She has been an active participant in several international conference program committees and organizations.