Joint Security and Robustness Enhancement for Quantization Based Data Embedding

Min Wu, *Member, IEEE*

***Abstract*—This paper studies joint security and robustness enhancement of quantization-based data embedding for multimedia authentication applications. We present analysis showing that through a lookup table (LUT) of nontrivial run that maps quantized multimedia features randomly to binary data, the probability of detection error can be considerably smaller than the traditional quantization embedding. We quantify the security strength of LUT embedding and enhance its robustness through distortion compensation. Introducing a joint security and capacity measure, we show that the proposed distortion-compensated LUT embedding provides joint enhancement of security and robustness over the traditional quantization embedding.**

***Index Terms*—Data hiding, digital watermarking, distortion compensation, joint security and robustness enhancement, lookup table (LUT) embedding.**

I. Introduction

DATA HIDING in multimedia signals has been an active research area in recent years. One potential application is to use the embedded data to verify whether or not a multimedia host signal has been tampered with [1], [2]. The data-embedding mechanism for these authentication applications should be secure enough to prevent an adversary from forging the embedded data at his/her will [3]. In addition, semi-fragileness is often preferred to allow for distinguishing content changes versus noncontent changes. Robustness against moderate compression is desirable as the multimedia data with authentication watermark embedded in may inevitably go through lossy compression, such as in the emerging application of building trustworthy digital cameras [4]–[7]. In this paper, we focus on jointly enhancing the robustness and security of core embedding mechanisms that can be used as building blocks for authentication.

While spread-spectrum techniques have been widely used to embed a small number of bits robustly in multimedia signals [8], quantization-based embedding is more common for such high-rate data-hiding applications as authentication. A popular technique, often known as odd–even embedding [9] or dithered modulation [10], is to choose a quantization step size q and round a feature, which can be a sample or a coefficient of the host signal, to the closest even multiples of q to embed a "0" and to odd multiples to embed a "1". Motivated by Costa's information theoretical result [11], distortion compensation has been proposed to be incorporated into quantization-based embedding [10], [12]–[14], where the quantization embedding result is combined linearly with the host signal to form a watermarked signal. Using the optimal compensation factor that is a function of watermark-to-noise ratio (WNR), distortion compensated version of odd–even embedding can reach higher payload than the odd–even embedding alone.

One of the main problems of quantization-based embedding is security. An adversary who knows the embedding algorithm can change the embedded data at his/her will, which presents concerns of counterfeiting attacks on authentication [3]. There are three directions in which to alleviate this security problem. The first is to encrypt the data to be embedded using a secure cipher such as AES and RSA [15]. The second approach is to provide security to feature extraction, such as deriving features through projecting a set of samples/coefficients along a direction specified by a key [16], [17]. The third approach is to add security to the embedding mechanism itself to make it difficult for an adversary to embed a specific bit at his/her will. Since the first and second approaches involve multiple samples or coefficients, they cannot always allow the localization of tampered regions to fine scale, which is a desirable feature for authentication [2], [4]. In this paper, we concentrate on the third approach. More specifically, we propose new enhancement strategies for quantization-based embedding, which leads to joint improvement of security and robustness. It can also be combined with the other two approaches to further enhance the security strength.

Our proposed approach is built on top of a general embedding technique known as look-up table (LUT) embedding. A pixel-domain LUT embedding scheme was proposed by Yeung and Mintzer [2], and was extended to quantization-based embedding in a transform domain in our earlier work [4]. The proprietary LUT can be generated from a cryptographic key and add security to embedding. With the same quantization step size, the LUT embedding generally introduces larger distortion than the traditional odd–even embedding, making it less popular. In this paper, however, we present analysis showing that at the same WNR, the probability of detection error for LUT embedding can be smaller than the odd–even embedding. We further quantify the security strength of LUT embedding and analyze the effect of distortion compensation on it. As will be seen, our proposed distortion compensated LUT embedding provides joint enhancement of security and robustness over the traditional quantization embedding.

The paper is organized as the follows. We begin with a general formulation of LUT embedding in Section II. The security and robustness of LUT embedding are analyzed in Section III and

Manuscript received December 23, 2002; revised May 19, 2003. This research was supported in part by research grants from the U.S. National Science Foundation CCR-0133704 (CAREER) and the Minta Martin Foundation.

The author is with the Department of Electrical and Computer Engineering, University of Maryland, College Park, MD 20742, USA (e-mail: minwu@eng.umd.edu).

Digital Object Identifier 10.1109/TCSVT.2003.815951

Section IV, respectively. We then propose and analyze distortion compensated LUT embedding in Section V and demonstrate its capability of joint enhancement of security and robustness. Section VI presents experimental results on images. Finally, conclusions are drawn in Section VII.

II. LUT Embedding

We focus on quantization-based embedding in scalar features and use uniform quantizers in this paper. A proprietary LUT $T(\cdot)$ is generated beforehand. The table maps every possible quantized feature value randomly to "1" or "0" with a constraint that the runs of "1" and "0" are limited in length. To embed a "1" in a feature, the feature is simply replaced by its quantized version if the entry of the table corresponding to that feature is also a "1". If the entry of the table is a "0", then the feature is changed to its nearest neighboring values for which the entry is "1". The embedding of a "0" is similar. For example, we consider a uniform quantizer[1] with quantization step size $q = 10$ and a look-up table $\{\ldots, T(7) = 0, T(8) = 0, T(9) = 1, T(10) = 0, T(11) = 1, \ldots\}$. To embed a "1" to a coefficient "84", we round it to the nearest multiple of ten such that the multiple is mapped to "1" by the LUT. In this case, we found that "90" satisfies this requirement and use "90" as the watermarked pixel value. Similarly, to embed a "0" in this pixel, we round it to "80".

This embedding process can be abstracted into the following formula, where X_0 is the original feature, Y is the marked one, b is a bit to be embedded in, and $Quant(\cdot)$ is the quantization operation

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

Here, $\delta \triangleq \min_{|d|}\{d = Quant(x) - X_0 \text{ s.t. } T(Quant(x)/q) = b\}$. The extraction of the embedded data is by looking up the table

$$\hat{b} = T\left(\frac{\mathrm{Quant}(Y)}{q}\right) \tag{2}$$

where $\hat{b}$ is the extracted bit.

III. Quantifying the Security of LUT Embedding

During the process of LUT embedding by (1), when $T(Quant(X_0)/q)$ does not match the bit to be embedded (b), we need to find a nearby entry in LUT that is mapped to b. As such, the run of "1" and "0" entries of an LUT need to be constrained to avoid excessive modification on the feature. We denote the maximum allowable run of "1" and "0" as r. To analyze security as a function of r, we start with the case of $r = 1$, which leads to only two possible tables

$$T(i) = \begin{cases} 0, & \text{(if i is even),} \\ 1, & \text{(if i is odd),} \end{cases} \quad \text{or} \quad T(i) = \begin{cases} 1, & \text{(if i is even)} \\ 0, & \text{(if i is odd).} \end{cases}$$

[1]For a uniform quantizer with quantization step size q considered in this paper, the quantization operation $Quant(x)$ is to round x to the nearest integer multiples of q.

This is essentially the odd–even embedding [9] or the dithered modulation embedding [10]. Since there is little uncertainty in the table, unauthorized persons can easily manipulate the embedded data, and/or change some feature values while retaining the embedded values. As we discussed earlier in this paper, the odd–even embedding, or equivalently the choice of $r = 1$, is not appropriate for authentication applications if no other security measures, such as a careful design of what data to embed, are taken.

When r is greater than 1, the number of LUTs satisfying the run constraint can be computed from the recursive relation presented in the following theorem.

Theorem 1: Let $F_k^{(m,r)}$ be the number of m-ary LUTs that have a total of k entries and runs no greater than r. Then, for $k \geq r$

$$F_{k+1}^{(m,r)} = (m-1)\sum_{i=0}^{r-1} F_{k-i}^{(m,r)}. \tag{3}$$

Proof: See the Appendix.

Corollary 1: Construct a binary LUT as follows: 1) equiprobably initialize each of the first two entries to 0 or 1 and 2) generate the remaining entries with maximum allowable run of 2. Let the number of k-entry LUTs that satisfy the above conditions be F_k. Then, F_k is equals to twice the Fibonacci series $F_{k+1} = F_k + F_{k-1}$ for $k \geq 2$, and $F_0 = 2$, $F_1 = 2$, $F_2 = 4$.

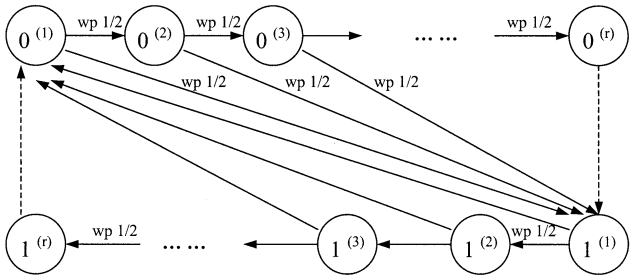
As an example of this corollary, we look at binary LUT with a length of 256 and maximum run of 2. The total number of such LUTs is on the order of 10^{53}, which is a significant increase from only two possible tables for run 1.

We further quantify the uncertainty of LUT embedding by identifying the generation process of binary LUT as a $2r$-state Markov chain illustrated in Fig. 1(a). Defining a state vector as $[0^{(1)}, 0^{(2)}, \ldots 0^{(r)}, 1^{(1)}, 1^{(2)}, \ldots, 1^{(r)}]$, the state transition matrix of this Markov chain is

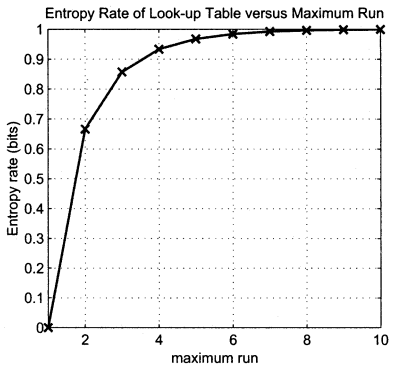
$$P = \left[\begin{array}{cccccc|cccccc} 0 & \frac{1}{2} & 0 & \ldots & \ldots & 0 & \frac{1}{2} & 0 & \ldots & \ldots & \ldots & 0 \\ 0 & 0 & \frac{1}{2} & 0 & \ldots & 0 & \frac{1}{2} & 0 & \ldots & \ldots & \ldots & 0 \\ \vdots & & & & & & \vdots & & & & & \\ 0 & \ldots & \ldots & \ldots & 0 & \frac{1}{2} & \frac{1}{2} & 0 & \ldots & \ldots & \ldots & 0 \\ 0 & \ldots & \ldots & \ldots & \ldots & 0 & 1 & 0 & \ldots & \ldots & \ldots & 0 \\ \hline \frac{1}{2} & 0 & \ldots & \ldots & \ldots & \ldots & 0 & \frac{1}{2} & 0 & \ldots & \ldots & 0 \\ \frac{1}{2} & 0 & \ldots & \ldots & \ldots & \ldots & \ldots & 0 & \frac{1}{2} & 0 & \ldots & 0 \\ \vdots & & & & & & \vdots & & & & & \\ \frac{1}{2} & 0 & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & 0 & \frac{1}{2} \\ 1 & 0 & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & 0 \end{array}\right] \tag{4}$$

We can show that the stationary probability of both $0^{(i)}$ and $1^{(i)}$ states is

$$\pi\left(0^{(i)}\right) = \pi\left(1^{(i)}\right) = \frac{2^{r-i-1}}{2^r - 1} \tag{5}$$



(a)



(b)

Fig. 1. Quantifying the uncertainty in LUT table generation. (a) A Markov chain model for LUT table generation, where the transition probability is 1/2 for solid arrow lines and 1 for dash arrow lines. (b) The entropy rate of LUT table as a function of the maximum allowable run r.

for $i = 1, \ldots, r$, and the entropy rate of the stationary process $\{Z_1, Z_2, \ldots\}$ is [18]

$$\lim_{n\to\infty} \frac{1}{n} H(Z_1, \ldots, Z_n) = \lim_{n\to\infty} H(Z_n | Z_{n-1}) = 1 - \frac{1}{2^r - 1} \text{ bit}. \tag{6}$$

For example, in the case of maximum allowable run $r = 2$, the LUT generation process is a 4-state Markov chain with transition matrix

$$P = \begin{bmatrix} 0 & \frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 1 & 0 \\ \frac{1}{2} & 0 & 0 & \frac{1}{2} \\ 1 & 0 & 0 & 0 \end{bmatrix}. \tag{7}$$

The stationary probability is $\pi = [1/3, 1/6, 1/3, 1/6]$, and the entropy rate is 2/3 bit. In contrast, the entropy rate with maximum run of 1 (or equivalently, the odd-even embedding) is 0 bit. We plot the entropy rate as a function of r in Fig. 1(b), which indicates that the uncertainty of LUT has increased significantly with a slight increase of the maximum allowable run.

It is important to note that the security quantified in this section measures how difficult an adversary can manipulate the data embedded in a watermarked feature with the knowledge of only this feature. We are interested in how much uncertainty a basic embedding mechanism can offer to each individual feature. Zooming into an LUT embedding mechanism that is already sufficiently secure at the individual feature level, another security aspect addresses how feasible it is for an adversary to derive the LUT from a number of watermarked features. Such a threat can be alleviated by introducing location dependency so that effectively different LUTs are used for different features [3]. Interested readers can refer to [3] for details.

IV. Robustness Analysis on LUT Embedding

Though bringing higher security, the increase in the allowable run r will inevitably lead to larger embedding distortion when a feature value of the host signal is not mapped by LUT to the bit to be embedded. In this section, we analyze the mean squared distortion introduced by LUT embedding and its probability of detection error under additive white Gaussian noise.

A. Distortion Incurred by Embedding

The mean squared distortion incurred by LUT embedding with binary LUT and maximum allowable run $r = 2$ is derived as the follows. First, we consider the error incurred purely by quantization, i.e., rounding an original feature in the range of $\mathcal{A} \triangleq [(k-1/2)q, (k+1/2)q)$ to kq. We assume that the original feature distributed (approximately) uniformly over this range $\mathcal{A}$, leading to a mean-squared distortion of

$$\text{MSE}(\text{quantize to } kq)|_{\mathcal{A}} = \frac{q^2}{12}. \tag{8}$$

This is the case when the LUT entry corresponding to the quantized version of the original feature equals to the bit to be embedded. We then consider the case that kq does not map to the desired bit value by LUT. In this situation, we have to shift the watermarked feature to $(k-1)q$ or $(k+1)q$ in order to embed the desired bit. For a half interval $\mathcal{A}_1 \triangleq [(k-1/2)q, kq)$ of an original feature, $(k-1)q$ maps to the desired bit by LUT and is output as watermarked feature with probability of $P(T(k) \neq T(k-1))$. On the other hand, with probability of $P(T(k) = T(k-1))$, $(k-1)q$ maps to the same value as kq does, and that value does not equal to the desired bit. According to the run constraint, $(k+1)q$ must be mapped to the desired bit value and should be output as the watermarked feature. By symmetry, the other half interval $\mathcal{A}_2 \triangleq [kq, (k+1/2)q)$ of an original feature can be analyzed in the same way. The mean squared distortion when kq does not match to the desired bit value is thus

$$\begin{aligned} &\text{MSE}\left(\text{quantize to } (k \pm 1)q\right)|_{\mathcal{A}} \\ &= q^2 \Big\{ \frac{7}{24} \Big[\left(P\left(T(k) \neq T(k-1)\right)\right. \\ &\qquad \left. + P\left(T(k) \neq T(k+1)\right) \Big] \\ &\qquad + \frac{19}{24} \Big[\left(P\left(T(k) = T(k-1)\right)\right. \\ &\qquad \left. + P\left(T(k) = T(k+1)\right) \Big] \Big\}. \end{aligned} \tag{9}$$

The probability terms $P(T(k) = T(k-1))$ and $P(T(k) \neq T(k-1))$ can be computed from the Markovian model presented in Section III. If the Markov chain is initialized with the stationary probability $\pi = [1/3, 1/6, 1/3, 1/6]$ (or equivalently, the initial status of the LUT generation is set to this probability), we have

$$\begin{cases} P\left(T(k) = T(k-1)\right) = \frac{1}{3} \\ P\left(T(k) \neq T(k-1)\right) = \frac{2}{3}. \end{cases} \tag{10}$$

Therefore

$$\text{MSE}\left(\text{quantize to } (k \pm 1)q\right)|_{\mathcal{A}} = \frac{11}{12} q^2. \tag{11}$$

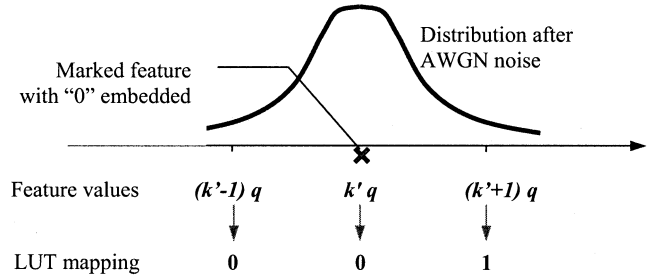


Fig. 2. Illustration of reduced detection errors of LUT embedding as the maximum allowable run r increases.

Since with probability of 1/2 the table lookup value of kq matches the desired bit, the overall MSE of the embedding is

$$\text{MSE}|_{\mathcal{A}} = \frac{1}{2}\cdot\frac{q^2}{12} + \frac{1}{2}\cdot\frac{11}{12}q^2 = \frac{q^2}{2}. \tag{12}$$

We can see that using the quantization step size q, LUT embedding with maximum run of 2 introduces MSE distortion of $q^2/2$, which is larger than the MSE distortion of $q^2/3$ by the odd-even embedding (or equivalently, LUT embedding with run 1). However, with larger run in LUT, stronger noise dragging a watermarked feature out of the enforced interval does not necessarily lead to errors in detection. An example is shown in Fig. 2. When noise drags a watermarked feature $k'q$ away to $(k'-1)q$, the extracted bit will have different value from the embedded bit in the case of odd-even embedding (run 1). Such a detection error may not happen when the allowable run of LUT increases since with some probability $(k'-1)q$ and $k'q$ are now mapped to the same bit value, as shown in Fig. 2. The probability of detection error can therefore be reduced. Next, we present analytic and experimental results on this issue.

B. Probability of Detection Error Under Additive White Gaussian Noise

To quantify the robustness in terms of the probability of detection error, we assume that the watermarked feature is at $k'q$ and that the additive noise follows i.i.d. Gaussian distribution $\mathcal{N}(0,\sigma^2)$ with zero mean and variance σ^2. The probability of noise pushing a feature to other intervals that are far away from $k'q$ is small due to the fast decay of the tails of Gaussian distribution, so the probability of detection error can be approximated by considering only the nearby intervals around $k'q$. When noise drags the watermarked feature away from $k'q$ to Y, we will encounter detection error only when $T(Quant(Y)/q) \neq T(k')$. For LUT embedding with a maximum allowable run of 2, there are three cases for the LUT entries of $k'-1$, k', and $k'+1$:

- $\{T(k') \neq T(k'-1), T(k') \neq T(k'+1)\}$;
- $\{T(k') = T(k'-1), T(k') \neq T(k'+1)\}$;
- $\{T(k') \neq T(k'-1), T(k') = T(k'+1)\}$.

Applying the Markovian property of LUT to computing the joint probability

$$P(Z_{k-1}, Z_k, Z_{k+1}) = P(Z_{k-1})P(Z_k|Z_{k-1})P(Z_{k+1}|Z_k)$$

where $Z_k \triangleq T(k)$, we find the probability of the first case as

$$\begin{aligned} &P(Z_{k'-1} \neq Z_{k'}, Z_{k'} \neq Z_{k'+1}) \\ &= P\left(Z_{k'-1} = 0^{(1)}\right)P\left(1^{(1)}|0^{(1)}\right)P\left(0^{(1)}|1^{(1)}\right) \\ &\quad + P\left(Z_{k'-1} = 0^{(2)}\right)P\left(1^{(1)}|0^{(2)}\right)P\left(0^{(1)}|1^{(1)}\right) \\ &\quad + P\left(Z_{k'-1} = 1^{(1)}\right)P\left(0^{(1)}|1^{(1)}\right)P\left(1^{(1)}|0^{(1)}\right) \\ &\quad + P\left(Z_{k'-1} = 1^{(2)}\right)P\left(0^{(1)}|1^{(2)}\right)P\left(1^{(1)}|0^{(1)}\right) \quad (13) \\ &= \frac{1}{3}. \quad (14) \end{aligned}$$

Note that (14) is based on the stationary probability of the Markov chain, which is valid either when the Markov chain is initialized with the stationary probability, or when k approaches infinity. Similarly, we obtain the probability of the other two cases as

$$P(Z_{k'-1} = Z_{k'}, Z_{k'} \neq Z_{k'+1}) = \frac{1}{3} \tag{15}$$

$$P(Z_{k'-1} \neq Z_{k'}, Z_{k'} = Z_{k'+1}) = \frac{1}{3}. \tag{16}$$

Thus, the probability of detection error under Gaussian noise can be approximated by

$$\begin{aligned} P_e \approx\ &P(Z_{k'-1} \neq Z_{k'}, Z_{k'} \neq Z_{k'+1})\cdot 2\cdot \mathcal{Q}\left(\frac{q}{2\sigma}\right) \\ &+ P(Z_{k'-1} = Z_{k'}, Z_{k'} \neq Z_{k'+1})\cdot \mathcal{Q}\left(\frac{q}{2\sigma}\right) \\ &+ P(Z_{k'-1} \neq Z_{k'}, Z_{k'} = Z_{k'+1})\cdot \mathcal{Q}\left(\frac{q}{2\sigma}\right) \quad (17) \\ =\ &\frac{4}{3}\cdot\mathcal{Q}\left(\frac{q}{2\sigma}\right) \quad (18) \end{aligned}$$

where the Q-function $\mathcal{Q}(x)$ is the tail probability of a Gaussian random variable $\mathcal{N}(0,1)$. Defining the watermark-to-noise ratio (WNR) γ as the ratio of MSE distortion introduced by watermark embedding to that by additional noise, we have $\gamma = q^2/2\sigma^2$ for the LUT embedding with maximum allowable run $r = 2$ according to (12). The probability of detection error of (18) in terms of WNR becomes

$$P_e^{(r=2)} \approx \frac{4}{3}\cdot\mathcal{Q}\left(\sqrt{\frac{\gamma}{2}}\right). \tag{19}$$

This analytic approximation of the probability of detection error vs. WNR is compared with the simulation result for maximum allowable run $r = 2$. We can see from Fig. 3 that the analytic approximation and simulation conform very well.

In contrast, for LUT with a maximum run of 1 (or equivalently, the odd-even embedding), detection error occurs as soon as the noise is strong enough to drag the watermarked feature to the quantization intervals next to the $k'q$ interval. The probability of detection errors for this embedding is

$$P_e^{(r=1)} \approx 2\times\left[\mathcal{Q}\left(\frac{q}{2\sigma}\right) - \mathcal{Q}\left(\frac{3q}{2\sigma}\right) + \mathcal{Q}\left(\frac{5q}{2\sigma}\right)\right] \tag{20}$$

$$= 2\times\left[\mathcal{Q}\left(\frac{\sqrt{3\gamma}}{2}\right) - \mathcal{Q}\left(\frac{3\sqrt{3\gamma}}{2}\right) + \mathcal{Q}\left(\frac{5\sqrt{3\gamma}}{2}\right)\right] \tag{21}$$

where the WNR $\gamma = q^2/3\sigma^2$.

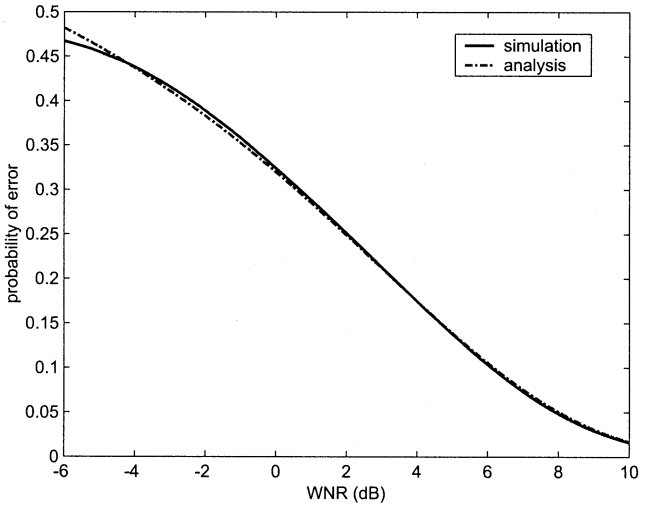


Fig. 3. Analytic and simulation result of detection error probability under white Gaussian noise for LUT embedding with maximum allowable LUT run of 2.

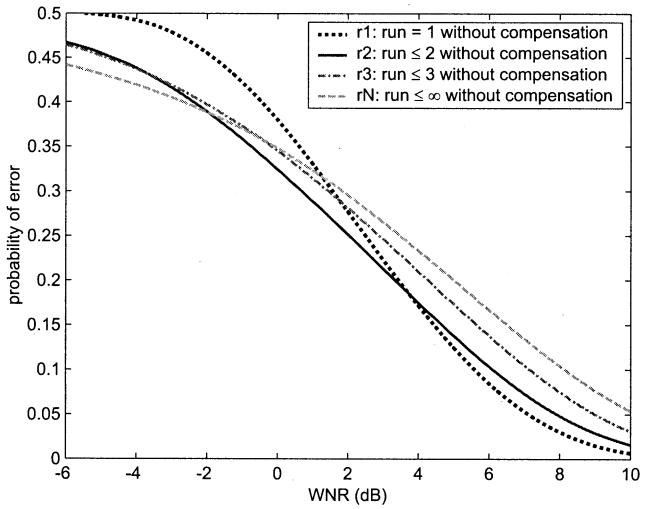


Fig. 4. Detection error probability under white Gaussian noise for LUT embedding with different maximum allowable LUT runs.

Using a total of 500 000 simulation points at each WNR ranging from -6 dB to $+10$ dB, we compare the probability of detection error versus WNR for maximum allowable run r of 1, 2, 3, and infinity, respectively. As can be seen from Fig. 4, P_e of a maximum run of 2 (solid line) is significantly smaller than a run of 1 (dot line) for up to 4-dB advantage at low and medium WNR, and is slightly higher at high WNR. In addition, the further increase of LUT's run (dotted-dashed line and dashed line) gives only a small amount of reduction of P_e at low WNR and much larger P_e at medium and high WNR. This indicates that LUT embedding with maximum allowable run of 2 can potentially provide higher robustness, as well as higher security than the commonly used quantization embedding with equivalent run 1. In the next section, we explore techniques that further improve the robustness and capacity of LUT embedding.

V. Distortion-Compensated LUT Embedding

Motivated by Costa's information theoretical result [11], distortion compensation has been proposed and incorporated into quantization-based embedding [10], [12]–[14], where the LUT enforced feature is combined linearly with the original feature value to form a watermarked feature. Using an optimal scaling factor that is a function of WNR, distortion compensated version of odd-even embedding provides higher capacity than without compensation [10]. The basic idea behind such improvement is to render more separation between the watermarked feature values while keeping the mean square distortion introduced by the embedding process unchanged. In this section, we propose to apply distortion compensation to LUT embedding and study the impact of distortion compensation on the reliability of LUT embedding.

A. Analysis of Probability of Detection Error

Let X_0 be the original unmarked feature, X_1 the output from LUT embedding alone (with maximum allowable LUT run $r = 2$), and Y be the finally watermarked feature after distortion compensation. We use a quantization step size of q/α to produce X_1 in the LUT embedding step, where $\alpha \in (0, 1]$ is also used as a weighting factor in distortion compensation

$$Y = \alpha X_1 + (1 - \alpha) X_0. \tag{22}$$

When α equals 1, this is reduced to the LUT embedding with quantization step size q and without distortion compensation. The overall mean squared distortion introduced by this distortion compensated embedding is

$$E\left(|Y - X_0|^2\right) = E\left(\alpha^2 |X_1 - X_0|^2\right) = \frac{q^2}{2}. \tag{23}$$

In other words, the mean squared distortion by embedding remains the same as in the noncompensated version that uses a quantization step size of q.

One criterion for selecting of α is to maximize the following "SNR":

$$\mathrm{SNR}^{(r=2)} = \frac{2 \cdot \left(\frac{q}{\alpha}\right)^2}{(1-\alpha)^2 \frac{\left(\frac{q}{\alpha}\right)^2}{2} + \sigma_n^2}. \tag{24}$$

Here, the "signal" power in the numerator is the mean squared distance between two neighboring, perfectly enforced feature values representing "1" and "0", and the "noise" power in the denominator is the mean squared deviation away from a perfectly enforced feature, where the deviation is introduced by both distortion compensation and additional noise of variance σ_n^2. The α value that maximizes the above SNR can be found as

$$\alpha_{opt}^{(r=2)} = \frac{1}{1 + \frac{2\sigma_n^2}{q^2}} = \frac{1}{1 + \frac{1}{WNR}}. \tag{25}$$

We can see that in terms of a function of WNR, this optimum compensation factor is identical to the distortion compensation case studied by Chen–Wornell [10] where the equivalent run is 1. We also note that a watermarking system under study usually targets at optimizing the embedding capacity at a specific noise

level. This will give a specific targeted WNR, and lead to an optimal α corresponding to this noise level. When the targeted noise level changes, so does the corresponding optimal α.

To analyze the probability of detection error, we focus on the scenario when X_0 is in the interval of $[(k-1/2)q/\alpha, kq/\alpha)$ for some k, and study three cases of X_1, namely (1) $X_1 = kq/\alpha$, (2) $X_1 = (k-1)q/\alpha$, and (3) $X_1 = (k+1)q/\alpha$, respectively. As analyzed in the previous section, the conditional probability of each of these three cases is 1/2, 1/3, and 1/6, respectively. In the first case of $X_1 = kq/\alpha$, the watermarked feature

$$Y = kq + (1-\alpha)X_0 = (1-\alpha)\Delta X_0 + \frac{kq}{\alpha}$$

where $\Delta X_0 \triangleq X_0 - kq/\alpha$. Under white Gaussian noise $\mathcal{N}(0,\sigma^2)$, the conditional probability of error can be further broken down into three substantial terms that reflect different combinations of the $(k-1)^{th}$, k^{th}, and $(k+1)^{th}$ entries in the LUT table. This analysis approach is similar to the one used in Section IV-B. Thus, the conditional probability of error for this case becomes

$$\begin{aligned} P_e^{(1)}(\Delta X_0) \approx & \frac{1}{3}\left[\mathcal{Q}\left(\frac{Y-\left(k-\frac{1}{2}\right)\frac{q}{\alpha}}{\sigma_n}\right)+\mathcal{Q}\left(\frac{\left(k+\frac{1}{2}\right)\frac{q}{\alpha}-Y}{\sigma_n}\right)\right. \\ & +\mathcal{Q}\left(\frac{Y-\left(k-\frac{3}{2}\right)\frac{q}{\alpha}}{\sigma_n}\right)+\mathcal{Q}\left(\frac{\left(k+\frac{1}{2}\right)\frac{q}{\alpha}-Y}{\sigma_n}\right) \\ & \left.+\mathcal{Q}\left(\frac{Y-\left(k-\frac{1}{2}\right)\frac{q}{\alpha}}{\sigma_n}\right)+\mathcal{Q}\left(\frac{\left(k+\frac{3}{2}\right)\frac{q}{\alpha}-Y}{\sigma_n}\right)\right] \quad (26) \\ = & \frac{2}{3}\left[\mathcal{Q}\left(\frac{(1-\alpha)\Delta X_0+\frac{q}{2\alpha}}{\sigma_n}\right)\right. \\ & \left.+\mathcal{Q}\left(\frac{\frac{q}{2\alpha}-(1-\alpha)\Delta X_0}{\sigma_n}\right)\right] \\ & +\frac{1}{3}\left[\mathcal{Q}\left(\frac{(1-\alpha)\Delta X_0+\frac{3q}{2\alpha}}{\sigma_n}\right)\right. \\ & \left.+\mathcal{Q}\left(\frac{\frac{3q}{2\alpha}-(1-\alpha)\Delta X_0}{\sigma_n}\right)\right]. \quad (27) \end{aligned}$$

Similarly, the conditional probability of error for the other two cases are given as follows:

$$\begin{aligned} P_e^{(2)}(\Delta X_0) \approx & \mathcal{Q}\left(\frac{q-\frac{q}{2\alpha}-(1-\alpha)\Delta X_0}{\sigma_n}\right) \\ & +\frac{2}{3}\mathcal{Q}\left(\frac{(1-\alpha)\Delta X_0+\frac{3q}{2\alpha}-q}{\sigma_n}\right) \\ & +\frac{1}{3}\mathcal{Q}\left(\frac{(1-\alpha)\Delta X_0+\frac{5q}{2\alpha}-q}{\sigma_n}\right) \quad (28) \\ P_e^{(3)}(\Delta X_0) \approx & \mathcal{Q}\left(\frac{(1-\alpha)\Delta X_0+q-\frac{q}{2\alpha}}{\sigma_n}\right) \\ & +\frac{2}{3}\mathcal{Q}\left(\frac{\frac{3q}{2\alpha}-q-(1-\alpha)\Delta X_0}{\sigma_n}\right) \\ & +\frac{1}{3}\mathcal{Q}\left(\frac{\frac{5q}{2\alpha}-q-(1-\alpha)\Delta X_0}{\sigma_n}\right). \quad (29) \end{aligned}$$

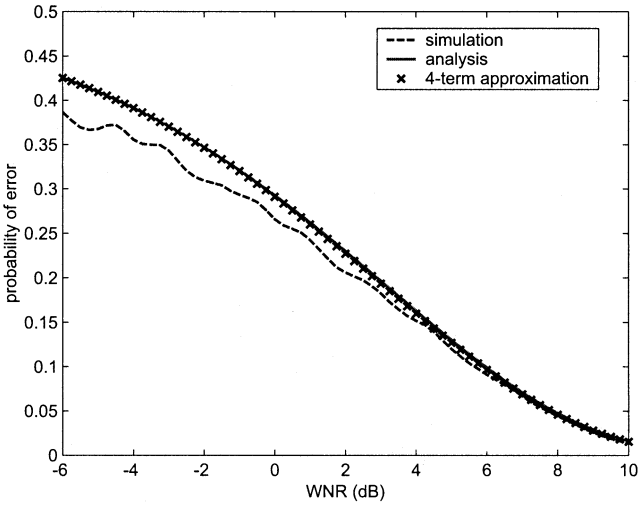


Fig. 5. Analytic and simulation result of detection error probability under white Gaussian noise for distortion compensated LUT embedding with maximum allowable run of 2.

The result of $X_0 \in [kq/\alpha, (k+1/2)q/\alpha]$ can be obtained by symmetry. Therefore, we arrive at the overall probability of detection error as

$$\begin{aligned} P_e = & \frac{2}{\frac{q}{\alpha}}\int_{-\frac{q}{2\alpha}}^{0}\left[\frac{1}{2}P_e^{(1)}(\Delta X_0)+\frac{1}{3}P_e^{(2)}(\Delta X_0)\right. \\ & \left.+\frac{1}{6}P_e^{(3)}(\Delta X_0)\right]d(\Delta X_0) \quad (30) \\ = & \alpha\sqrt{\frac{2}{\gamma}}\int_{-\frac{\sqrt{\frac{\gamma}{2}}}{\alpha}}^{0}\left[\frac{1}{2}P_e^{(1)}(t)+\frac{1}{3}P_e^{(2)}(t)+\frac{1}{6}P_e^{(3)}(t)\right]dt. \quad (31) \end{aligned}$$

where $t = \Delta X_0/\sigma_n$, and $\gamma = q^2/2\sigma^2$ is the WNR. Because of the fast decay of $\mathcal{Q}(x)$ as x increases, we can further approximate P_e into four terms

$$\begin{aligned} P_e = & \alpha\sqrt{\frac{2}{\gamma}}\int_{-\frac{\sqrt{\frac{\gamma}{2}}}{\alpha}}^{0}\left\{\frac{1}{6}\mathcal{Q}\left(\sqrt{2\gamma}\left(1-\frac{1}{2\alpha}\right)+(1-\alpha)t\right)\right. \\ & +\frac{1}{3}\left[\mathcal{Q}\left(\frac{\sqrt{2\gamma}}{2\alpha}+(1-\alpha)t\right)\right. \\ & +\mathcal{Q}\left(\frac{\sqrt{2\gamma}}{2\alpha}-(1-\alpha)t\right) \\ & \left.\left.+\ \mathcal{Q}\left(\sqrt{2\gamma}\left(1-\frac{1}{2\alpha}\right)\right.\right. \\ & \left.\left.-\ (1-\alpha)t\right)\right]\right\}dt. \quad (32) \end{aligned}$$

Fig. 5 plots the probability of error P_e versus the WNR γ for distortion compensated LUT embedding with maximum allowable run of 2. Solid line represents the numerical evaluation of (31), cross marks are approximations of (32), and the dashed line comes from our simulation of a total of 500 000 data points at each WNR setting. We can see that the analytic approximations of (31) and (32) agree very well with the simulation results especially at high WNR, while there is a small gap between them at lower WNR. Including more LUT entries around k in

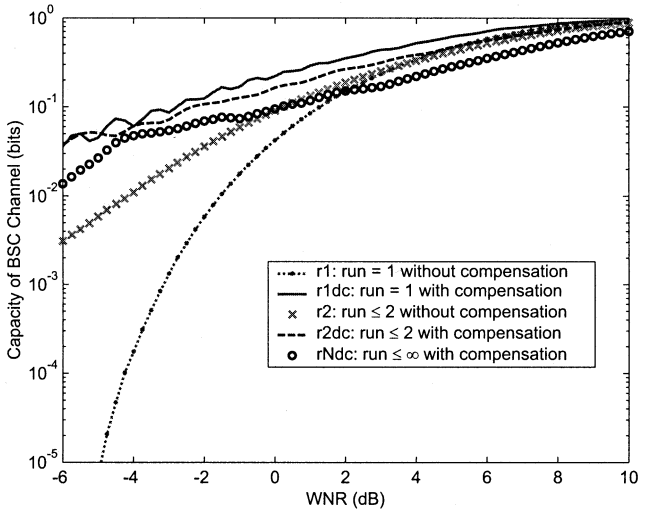


Fig. 6. BSC embedding capacity under different maximum allowable LUT runs and different compensation settings.

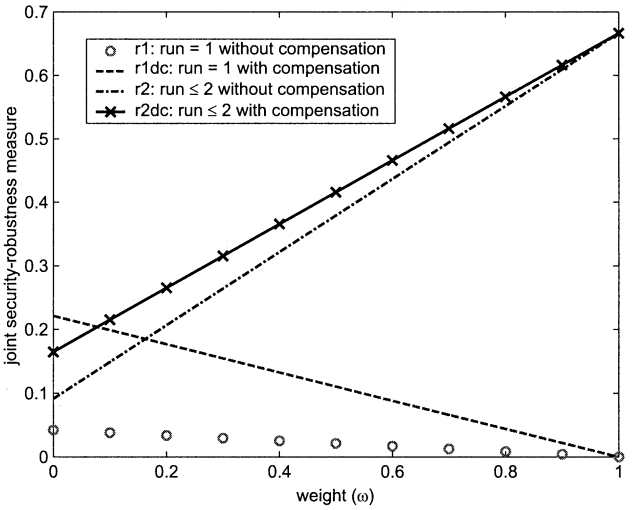


Fig. 7. Linear joint security and capacity measure of LUT embedding as a function of weight ω at a WNR of 0 dB.

our analysis will improve the approximation accuracy and reduce this gap at low WNR.

Next, we jointly evaluate the robustness and security of the proposed distortion compensated LUT embedding with maximum allowable run of 2 and of other embedding settings.

B. Joint Evaluation of Robustness and Security

We quantify the robustness of different embedding settings through their embedding capacities at a wide range of WNRs. For simplicity, the channel between embedding and detection is modeled as a simple, binary symmetric channel (BSC) [18] with cross-over probability being the probability of error P_e studied above. That is

$$\begin{aligned} C_{\mathrm{LUT}} &= 1 - h(P_e) \\ &= 1 + P_e \log(P_e) + (1 - P_e)\log(1 - P_e). \end{aligned} \quad (33)$$

We compare the BSC embedding capacity of five cases in Fig. 6, namely, the maximum allowable run of 2 with and without distortion compensation, constant run of 1 (traditional odd-even embedding) with and without compensation, and maximum allowable run of infinity (i.e., no run constraint) with compensation. From the cross-marked line to the dashed line, we see that when the maximum allowable run is 2, the embedding capacity increases significantly for up to 4-dB advantage in WNR after applying distortion compensation. We also observe that when keeping all other conditions identical and only varying the maximum allowable run of LUT, the increase in allowable run gives higher embedding capacity in low WNR when no compensation is used (the dotted line to the cross marked line), and a moderately smaller capacity when distortion compensation is applied (the solid line to the dash line to the circle line). For example, at comparable capacity, distortion compensated LUT embedding with maximum run of 2 requires about 1 dB more in WNR than the compensated case with run of 1. The intuition behind is as follows: the run constraint of 1 with distortion compensation, or equivalently the scalar Costa's embedding [14], gives near-optimal embedding capacity supported by information theoretical study [10], which concerns maximizing the capacity under a specific WNR without other considerations such as the security inherent in the embedding mechanism in Section III. On the other hand, the case of run constraints of 2 provides extra uncertainty in the embedding. As an expense, the error rate at the same WNR level is slightly higher, or equivalently, the embedding capacity is lower than the run-1 case. This shows a tradeoff between capacity and security, but the above embedding capacity comparison alone, however, concerns mainly the robustness and does not include information about security.

To take into account both security and robustness issues, we define a joint measure $J(H, C)$ as a function of the entropy rate H of the embedding mapping and the embedding capacity C. One simple choice of $J(\cdot,\cdot)$ is a linear combination of the entropy rate and the embedding capacity under BSC assumption for additive noise. That is

$$J = \omega H_{\mathrm{LUT}} + (1 - \omega) \cdot C_{\mathrm{LUT}} \quad (34)$$

where H_{LUT} is the entropy rate of LUT table given by (6), C_{LUT} is the BSC embedding capacity given by (33), and $\omega \in [0, 1]$ is a weight factor to provide desirable emphasis to security and robustness issues. We plot this joint measure at 0 dB WNR for maximum LUT run of 1 and 2, respectively, with different weight ω and different compensation settings. We can see from Fig. 7 that distortion compensated embedding with run constraint of 2 (cross-marked line) gives the highest J over a wide range of weight values. It holds until the weight ω going below 0.15 or security is not much concerned, where the joint measure for the traditional odd-even embedding with distortion compensation (dash line) becomes higher. The figure suggests that as long as some level of security is desired, by slightly increasing the allowable LUT run from 1 to 2 and by applying distortion compensation, we can provide joint improvement of security and robustness to quantization-based embedding.

C. Discussions

Variations of Distortion Compensation: We explore a few variations of distortion compensation and compare their perfor-

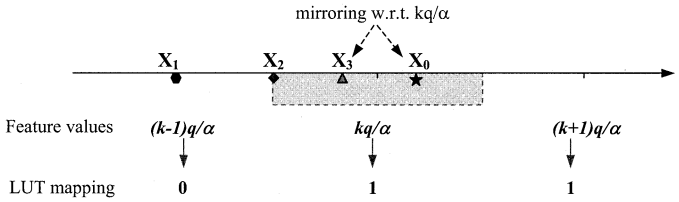


Fig. 8. Illustration of different distortion-compensation strategies.

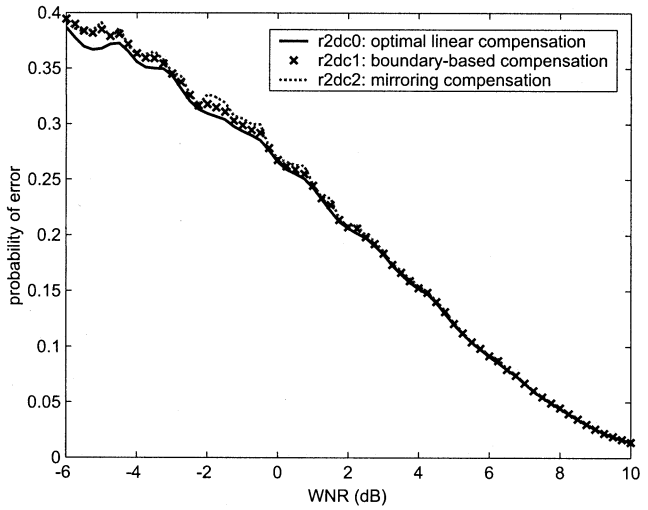


Fig. 9. Comparison of probability of error of three compensation techniques for LUT embedding with maximum allowable run of 2.

mance with the linear compensation in (22). We shall focus on the case of maximum allowable run of 2. As illustrated in Fig. 8, to embed a bit b, the linear compensation technique interpolates between the enforced point X_1 (highlighted by a hexagonal icon) and the original feature point X_0 (five-star icon). To prevent the compensation step from introducing large deviation from the enforced point X_1 when $T(k) \neq b$, we propose two alternatives to X_0. One is a boundary point X_2 (diamond icon), and the other is a mirroring point X_3 (triangle icon).

Shown in Fig. 9 are the performances of boundary-point-based compensation (cross marks), mirroring-based compensation (dot line), and the optimal linear compensation (solid line). The probabilities of detection error are comparable for these three compensation cases. The underlying reason is because the larger distortion introduced by embedding, such as in the optimal linear compensation can also bring larger guard zone hence resist stronger distortion. This leads to nearly identical robustness of the above three compensation approaches when normalized in terms of WNR.

Robustness Against Uniformly Distributed Noise: Primarily introduced by quantizing the watermarked signals, uniformly distributed noise is common in data-hiding applications. Due to the bounded nature of uniform noise, detection is error free until the range of noise exceeds half of the quantization step size. The probability of detection error under uniform noise for the odd-even embedding was analyzed in our previous work [19]. For embedding with larger LUT runs and distortion compensation, the robustness analysis against uniformly distributed additive noise is similar to that for Gaussian noise presented earlier in this paper and will not be elaborated here. We present the

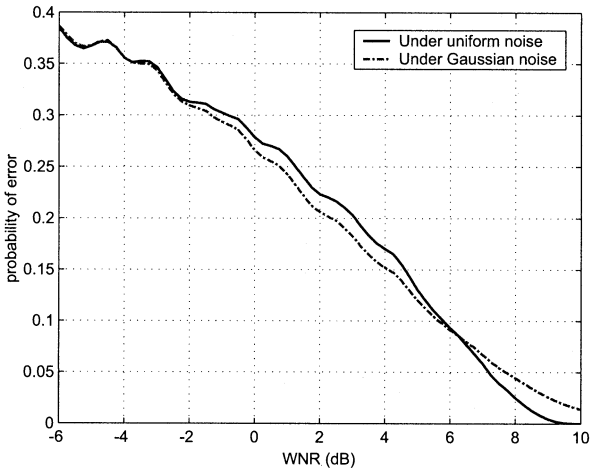


Fig. 10. Comparison of the probability of detection error under uniform versus white Gaussian noise for LUT embedding with maximum allowable run of 2 and linear distortion compensation.

robustness comparison of LUT embedding against uniform noise versus white Gaussian noise in Fig. 10, where the LUT embedding uses maximum allowable run of 2 and linear distortion compensation. We see that the LUT embedding has similar robustness against uniform and Gaussian noise. The quantization nature of LUT embedding, along with the bounded property of uniform noise, gives a zero-error region at very high WNR; and the slightly higher error rate in medium WNR under uniform noise can be reduced by soft detection [19].

VI. Experimental Results With Images

As a proof-of-concept, we apply our proposed distortion compensated LUT embedding with run constraint of 2 to the 512 $\times$ 512 Lenna image. One bit is embedded in each pixel, and the embedded raw data forms a 512 $\times$ 512 pattern shown in Fig. 11(c). For comparison, we have also implemented a embedding scheme using the same LUT but without compensation,[2] as well as the popular odd-even embedding with and without compensation. The base quantization step q is 3 and the PSNRs of watermarked images are about 42 dB. Fig. 11(b) shows a zoomed-in version of watermarked Lenna by the proposed embedding with LUT run constraint of 2 and linear distortion compensation.

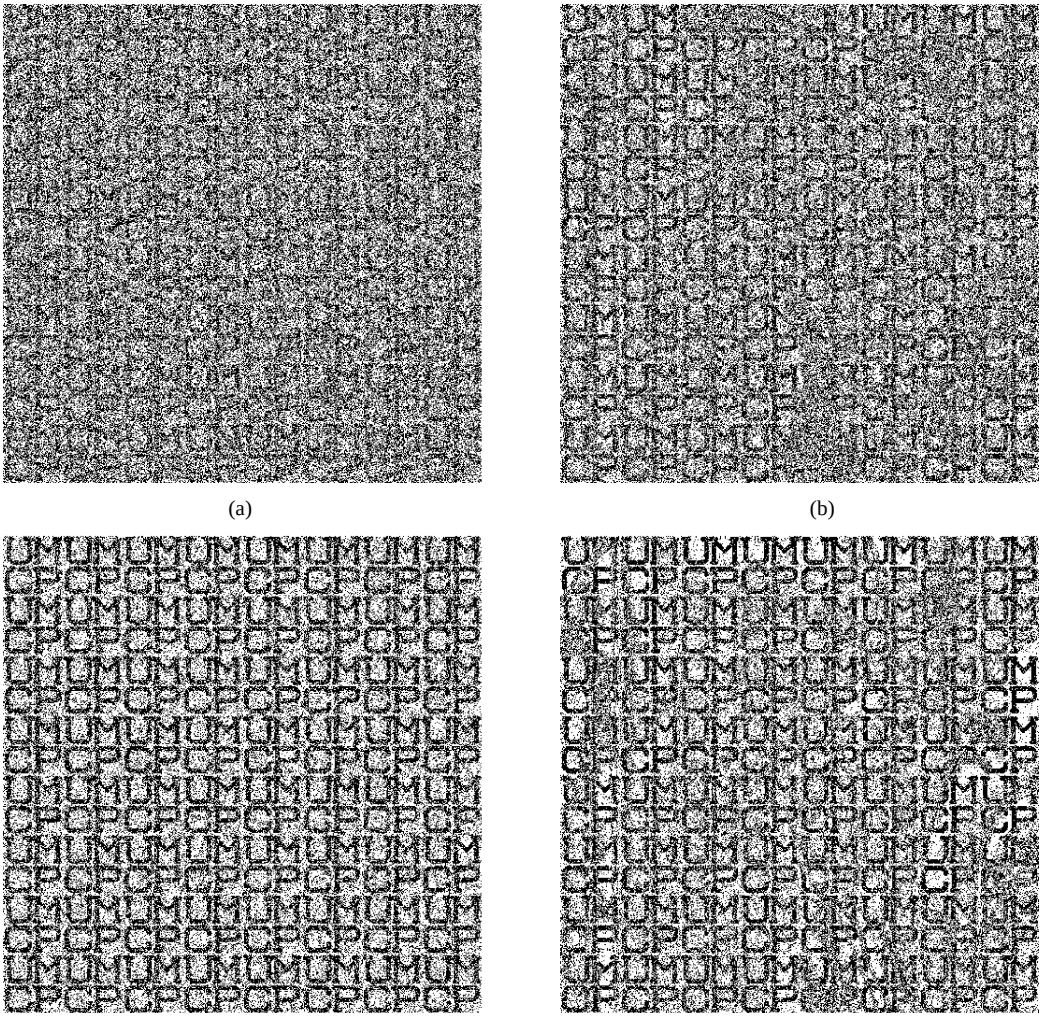
Next, we add white Gaussian noise to watermarked images and tailor its strength to give a WNR of 0 dB in all tests. The detection errors on 512 $\times$ 512-bit raw data are visualized in Fig. 12, from which we can see an improvement by distortion compensation [Fig. 12(c) and (d)] on reducing the raw bit error rate by 10%. We also note that when distortion compensation is applied, the error rate for run constraint of 1 [Fig. 12(c)] is slightly lower than that for run constraint of 2 [Fig. 12(d)]. These all confirm our analysis presented in Fig. 6 of Section V.

To overcome the bit errors in data extraction, channel coding can be applied to provide reliable communication at targeted WNRs. Here, we visualize the effect of simple repetition coding

[2]This noncompensated scheme is similar to [2] but applied in quantized pixels. For simplicity, we omit an error diffusion step that can further improve the perceptual quality of watermarked images.

(a) (b) (c)

Fig. 11. A zoomed-in view of the (a) original Lenna image and (b) the watermarked version using distortion-compensated LUT embedding with run constraint of 2, along with (c) a 512×512-bit pattern embedded in the Lenna image. The base quantization step is 3 and the PSNRs of the watermarked images are 42 dB.



(a) (b) (c) (d)

Fig. 12. Visualization of raw error pattern by LUT embedding with different settings under $\mathrm{WNR} = 0$dB. (a) Run $= 1$, no compensation, error 38.8%. (b) Run ≤ 2, no compensation, error 35.1%. (c) Run $= 1$, with compensation, error 23.6%. (b) Run ≤ 2, with compensation, error 26.0%.

followed by majority voting in decoding. As can be seen from Fig. 13, the 16-time repetition coding of a 128×128-bit pattern can allow most bits extracted correctly, and the 64-time repetition will deliver a 64×64-bit pattern free of error. The result under uniform noise at WNR 0 dB, shown in Fig. 13(c), is similar to that under white Gaussian noise. This is expected based on our study in Section V-C.

Furthermore, we examine the effects of attacks other than additive white noise. In particular, we are interested in the performance under the popular JPEG compression. We apply JPEG compression with quality factors 95% and 75%, respectively, to the watermarked image of Fig. 11. As shown in Fig. 14(a), the equivalent WNR of JPEG 95% quality is 0.5 dB and the raw error rate before error correction coding is 24.5%, both of which

(a) (b) (c)

Fig. 13. Visualization of extracted data after applying repetition coding and majority voting under $\mathrm{WNR} = 0$dB. The effective payloads are: (a) 64×64 bits and (b) and (c) 128×128 bits. (a) 64 repetitions, Gaussian noise. (b) 16 repetitions, Gaussian noise. (c) 16 repetitions, uniform noise. The noise distribution is (a) and (b) white Gaussian and (c) white uniform.

(a)

(b)

Fig. 14. Visualization of extracted data from the watermarked image of Fig. 11 after JPEG compression with two different quality factors: (a) JPEG 95% quality with equivalent WNR=0.5 dB and error rate before coding 24.5%. (b) JPEG 75% quality with equivalent WNR= -6.25 dB and error rate before coding 37.8%. 16-time repetition coding and majority voting is used, with an effective payload of 128×128 bits.

are comparable to the additive noise case shown in Fig. 12 and Fig. 13. When compression becomes stronger with respect to the watermark, as in Fig. 14(b), the error rate before coding is higher and requires more powerful coding to accurately extract the effective payload. For the same level of compression, one can increase the quantization step size and thus make the watermark stronger to reduce the raw error rate. This is a tradeoff between robustness, imperceptibility, and payload.

As a final note, the proposed LUT embedding with distortion compensation can be combined with advanced coding such as those in [13], [14] to improve the coding efficiency. It can also be applied in transform domains such as the DCT and the Wavelet domain for improved tradeoff between imperceptibility, payload, and robustness against common processing.

VII. Conclusions

In summary, this paper studies the joint enhancement of security and robustness for quantization-based data embedding. We start with a general embedding approach that employs a LUT mapping quantized multimedia features to binary data. We quantify the security strength of LUT embedding in terms of entropy rate and have shown that the security is improved significantly with a slight increase of the allowable LUT run from 1 to 2. We present analysis showing that LUT embedding with larger run constraints can have smaller probability of detection error for up to 4-dB advantage in WNR. We then explore distortion compensation on LUT embedding to further enhance its robustness and provide an additional advantage of up to 4 dB in WNR. Through a joint security and capacity measure, we have shown that our proposed distortion compensated LUT embedding with maximum allowable run of 2 offers joint enhancement of security and robustness over the traditional quantization embedding that has an equivalent run of 1. This joint enhancement makes the proposed embedding scheme an attractive building block for multimedia authentication applications.

Appendix

Proof of Theorem 1: The generation process of LUT table can be represented using an m-ary tree, and $F_{k+1}^{(m,r)}$ equals to the number of nodes in the $(k+1)^{th}$ level of this tree. Proving (3) is thus equivalent to count the nodes in Level-$(k+1)$. First, we mark all the nodes that have different values from their parent nodes. The number of nodes marked in this step is $(m-1)F_k^{(m,r)}$. Next, for $r \geq 2$, among the unmarked nodes of Level-$(k+1)$ that have the same value as their parent nodes, $(m-1)F_{k-1}^{(m,r)}$ of them have a grandparent node and a parent node that carry different values. Because the nodes' value changes from grandparent level to parent level, the run is reset

there so that the run from parent to the current level does not exceed the constraint r. We therefore mark these nodes, giving a total of $(m-1)[F_k^{m,r} + F_{k-1}^{m,r}]$ marked nodes. We continue this marking process for nodes that have continuous run of 3, $4, \ldots, r$ to mark all the nodes in Level-$(k+1)$, giving a total number of $(m-1)\sum_{i=0}^{r-1} F_{k-i}^{(m,r)}$. □

ACKNOWLEDGMENT

The author thanks Prof. B. Liu of Princeton University for insightful discussions during the early exploration of lookup table embedding, and anonymous reviewers for their constructive comments.

REFERENCES

[1] I. J. Cox, M. L. Miller, and J. A. Bloom, *Digital Watermarking*. New York: Morgan Kaufmann, 2001.

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

[3] M. Holliman and N. Memon, "Counterfeiting attacks on oblivious blockwise independent invisible watermarking schemes," *IEEE Trans. Image Processing*, vol. 9, pp. 432–441, Mar. 2000.

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

[5] D. Kundur and D. Hatzinakos, "Digital watermarking for telltale tamper-proofing and authentication," *Proc. IEEE*, vol. 87, pp. 1167–1180, July 1999.

[6] C.-Y. Lin and S.-F. Chang, "Semi-fragile watermarking for authenticating JPEG visual content," in *Proc. SPIE Int. Conf. Security and Watermarking of Multimedia Contents II (EI'00)*, vol. 3971, 2000.

[7] P. Yin and H. Yu, "Semi-fragile watermarking system for MPEG video authentication," in *Proc. Int. Conf. Acoustics, Speech and Signal Processing (ICASSP)*, Orlando, FL, May 2002, pp. 3461–3464.

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

[9] M. Wu and B. Liu, "Data hiding in image and video: part-I—fundamental issues and solutions," *IEEE Trans. Image Processing*, vol. 12, pp. 685–695, June 2003.

[10] B. Chen and G. W. Wornell, "Quantization index modulation: a class of provably good methods for digital watermarking and information embedding," *IEEE Trans. Inform. Theory*, vol. 47, pp. 1423–1443, May 2001.

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

[12] P. Moulin and J. A. O'Sullivan. Information—Theoretic Analysis of Information Hiding. Preprint, Sept. 1999, revised Dec. 2001. [Online] Available: http://www.ifp. uiuc.edu/~moulin/paper.html

[13] M. Kesal, M. K. Mihcak, R. Koetter, and P. Moulin, "Iteratively decodable codes for watermarking applications," in *Proc. 2nd Int. Symp. Turbo Codes and Related Topics*, Brest, France, Sept. 2000.

[14] J. J. Eggers, R. Bauml, R. Tzschoppe, and B. Girod, "Scalar Costa scheme for information embedding," *IEEE Trans. Signal Processing*, vol. 51, pp. 1003–1019, Apr. 2003.

[15] W. Trappe and L. C. Washington, *Introduction to Cryptography With Coding Theory*. Englewood Cliffs, NJ: Prentice-Hall, 2001.

[16] M. D. Swanson, B. Zhu, and A. H. Tewfik, "Robust data hiding for images," in *Proc. IEEE DSP Workshop*, Loen, Norway, 1996, pp. 37–40.

[17] M. Alghoniemy and A. H. Tewfik, "Self-synchronizing watermarking techniques," in *Proc. Symp. Content Security and Data Hiding in Digital Media*: NJ Center for Multimedia Research and IEEE, Sept. 1999.

[18] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. New York: Wiley, 1991.

[19] M. Wu and B. Liu, *Multimedia Data Hiding*. New York: Springer-Verlag, Oct. 2002.

Min Wu (S'95–M'01) received the B.E. degree in electrical engineering and the B.A. degree in economics from Tsinghua University, Beijing, China, in 1996 (both with the highest honors), and the M.A. and Ph.D. degrees in electrical engineering from Princeton University, Princeton, NJ, in 1998 and 2001, respectively.

She was with NEC Research Institute and Signafy, Inc. in 1998, and with Panasonic Information and Networking Laboratories in 1999. Since 2001, she has been an Assistant Professor of the Department of Electrical and Computer Engineering, Institute of Advanced Computer Studies, and the Institute of Systems Research, both at the University of Maryland, College Park. Her research interests include information security, multimedia signal processing, and multimedia communications. She is co-author of the book *Multimedia Data Hiding* (New York: Springer-Verlag, 2002) and holds three U.S. patents on multimedia data hiding.

Dr. Wu is a member of the IEEE Technical Committee on Multimedia Signal Processing, Publicity Chair of the 2003 IEEE International Conference on Multimedia and Expo (ICME'03, Baltimore), and a Guest Editor of a Special Issue on Multimedia Security and Rights Management of the *EURASIP Journal on Applied Signal Processing*. She received a CAREER award from the U.S. National Science Foundation in 2002.