Distortion Compensated Lookup-Table Embedding: Joint Security and Robustness Enhancement for Quantization Based Data Hiding

Min Wu

ECE Department, University of Maryland, College Park, U.S.A.

ABSTRACT

Data embedding mechanism used for authentication applications should be secure in order to prevent an adversary from forging the embedded data at his/her will. Meanwhile, semi-fragileness is often preferred to allow for distinguishing content changes versus non-content changes. In this paper, we focus on jointly enhancing the robustness and security of the embedding mechanism, which can be used as a building block for authentication. The paper presents analysis showing that embedding through a look-up table (LUT) of non-trivial run that maps quantized multimedia features randomly to binary data offers a probability of detection error considerably smaller than that of the traditional quantization embedding. We quantify the security strength of LUT embedding and enhance its robustness through distortion compensation. We introduce a combined security and capacity measure and show that the proposed distortion compensated LUT embedding provides joint enhancement of security and robustness over the traditional quantization embedding.

Keywords: D ata hiding, digital watermarking, look-up table (LUT) embedding, distortion compensation, joint security and robustness enhancement.

1. INTRODUCTION

Tampering detection is one of the promising application areas of multimedia data hiding [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]. Meanwhile, semi-fragileness is often preferred to allow for distinguishing content changes versus non-content changes. Robustness against moderate compression is desirable since the multimedia data embedded with authentication watermarks may inevitably go through lossy compression, as in the emerging application of building trustworthy digital cameras [4–6]. In this paper, we focus on jointly enhancing the robustness and security of embedding mechanism, which can be used as a building block for authentication.

Among various embedding mechanisms, quantization based embedding is common for authentication purposes owing to its high embedding rate under blind detection, which is commonly needed in such applications. A popular technique, often known as odd-even embedding [7] or dithered modulation [8], 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 [9], distortion compensation has been proposed to be incorporated into quantization-based embedding and has substantially improved the tradeoff between payload and robustness [8, 10, 11].

Security is a major problem of quantization based embedding when used for authentication applications. An adversary who knows the embedding algorithm can change the embedded data at his/her will, which raises concerns of counterfeiting attacks on authentication [3]. There are several directions to alleviate this security problem: some involves adding uncertainty to the embedding mechanism, some generates features with randomness such as projecting a set of media components onto proprietary directions [12, 13], and some focuses on making the data to be embedded more tamper-proof and forge-proof such as via encryption. In this paper, we concentrate on adding security to the core embedding mechanism to make it difficult for an adversary to embed a specific bit at his/her will. More specifically, we propose new enhancement strategies for quantization based embedding, which leads to joint improvement of security and robustness. Unlike the other two types of approaches discussed above, the security enhancement through core embedding mechanism is not necessarily tied

The author can be contacted via email at minwu@eng.umd.edu .

with multiple samples or coefficients. As such, it is compatible to system designs that can localize the tampered regions, which is a desirable feature for authentication applications [2,4]. It can also be combined with the other approaches to further enhance the security strength.

The 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 [4], whereby the proprietary look-up table can be generated from a cryptographic key. We may constrain the maximum allowable run of 0 and/or 1 entries when generating LUTs. With the same quantization step size, the LUT embedding with increased run generally introduces larger distortion than the traditional odd-even embedding or dithered modulation (equivalent to imposing run constraint of one), making it less popular in the literature. In this paper, however, we present analysis showing that the probability of detection error for LUT embedding can be smaller than the odd-even embedding over a wide range of watermark-to-noise ratio (WNR). The intuition behind is that with larger run in LUT, stronger noise dragging a watermarked feature out of the enforced interval does not necessarily lead to errors in detection. 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, and analyze the security and robustness of LUT embedding in Section 2 and Section 3, respectively. We then propose and analyze distortion compensated LUT embedding in Section 4 and demonstrate its capability of joint enhancement of security and robustness. Section 5 presents experimental results on images, and Section 6 concludes the paper.

2. LOOK-UP TABLE (LUT) EMBEDDING AND ITS SECURITY

We focus on quantization based embedding in scalar features and use uniform quantizers in this paper. A proprietary look-up table (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 [*] with quantization step size $q = 10$ and a look-up table $\{..., T(7) = 0, T(8) = 0, T(9) = 1, T(10) = 0, T(11) = 1, ...\}$. To embed a “1” to a coefficient “84”, we round it to the nearest multiples of 10 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:

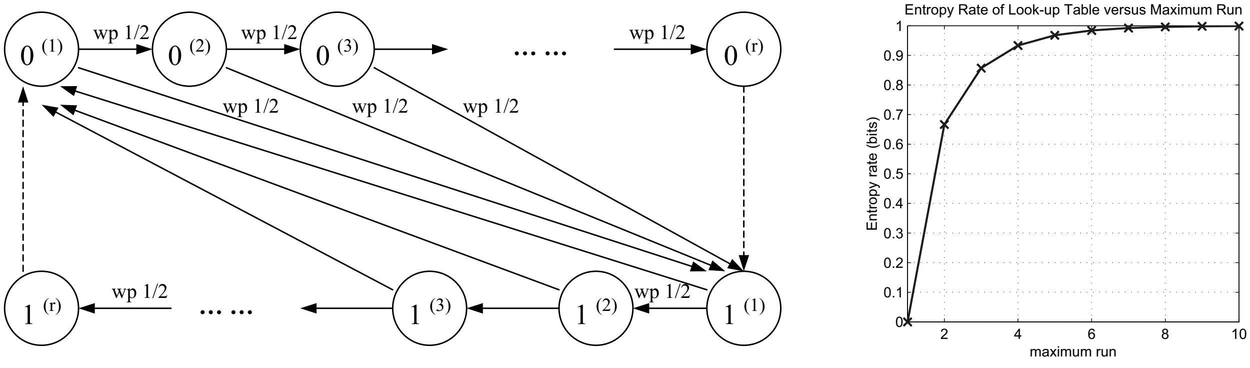
$$Y = \begin{cases} Quant(X_0) & \text{if } T(Quant(X_0)/q) = b \ , \\ X_0 + \delta & \text{otherwise} \ . \end{cases} \tag{1}$$

Here, $\delta \triangleq \arg\min d(x)$, where $d(x) = Quant(x) - X_0$ s.t. $T(Quant(x)/q) = b$. The extraction of the embedded data is by looking up the table, i.e., $\hat{b} = T(Quant(Y)/q)$, where $\hat{b}$ is the extracted bit.

During the process of LUT embedding by Eq. 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:

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

[*] 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.



(a) (b)

Figure 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.

This is essentially the odd-even embedding [7] or the dithered modulation embedding [8]. 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 are taken, such as a careful design of what data to embed.

When r is greater than 1, the number of LUTs satisfying the run constraint grows dramatically. For example, the total number of binary LUTs with length 256 and maximum run of 2 is on the order of 10^{53}. We quantify such uncertainty inherent in 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 $[0^{(1)}, 0^{(2)}, ...0^{(r)}, 1^{(1)}, 1^{(2)}, ..., 1^{(r)}]$, the state transition matrix of this Markov chain is

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

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

$$\pi(0^{(i)}) = \pi(1^{(i)}) = \frac{2^{r-i-1}}{2^r - 1} \tag{3}$$

for $i = 1, ..., r$, and the entropy rate of the stationary process $\{Z_1, Z_2, ...\}$ is [14]

$$\lim_{n\to\infty} \frac{1}{n} H(Z_1, ..., Z_n) = \lim_{n\to\infty} H(Z_n|Z_{n-1}) = 1 - \frac{1}{2^r - 1} \quad \text{bit.} \tag{4}$$

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

$$P = \left[\begin{array}{cccc} 0 & \frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 1 & 0 \\ \frac{1}{2} & 0 & 0 & \frac{1}{2} \\ 1 & 0 & 0 & 0 \end{array} \right]. \tag{5}$$

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].

3. 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.

3.1. 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 mean squared distortion of $\text{MSE(quantize to } kq\text{)}|_{\mathcal{A}} = q^2/12$. 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. When an original feature falls in the half interval $\mathcal{A}_1 \triangleq [(k-1/2)q, kq)$, with probability of $P(T(k) \neq T(k-1))$, $(k-1)q$ maps to the desired bit by LUT and is output as watermarked feature. 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

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

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 2. 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

$$\left\{ \begin{array}{rcl} P(T(k) = T(k-1)) & = & 1/3, \\ P(T(k) \neq T(k-1)) & = & 2/3. \end{array} \right. \tag{6}$$

Since with probability of 1/2 the table lookup value of kq matches the desired bit, the overall MSE of the embedding is $\text{MSE}|_{\mathcal{A}} = q^2/2$.

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 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.

3.2. 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 $T(Quant(Y)/q) \neq T(k')$.

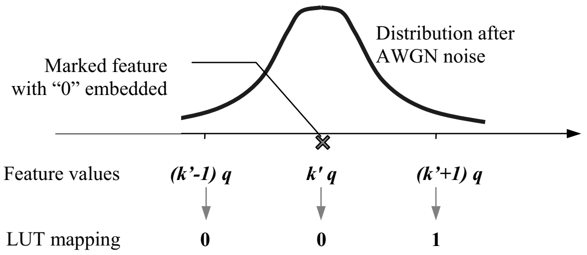

Distribution after AWGN noise
Marked feature with “0” embedded
Feature values
(k’-1) q
k' q
(k’+1) q
LUT mapping
0
0
1

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

For LUT embedding with maximum allowable run of 2, there are three cases for the LUT entries of $k'-1$, k', and $k'+1$, namely, $\{T(k') \neq T(k'-1), T(k') \neq T(k'+1)\}$, $\{T(k') = T(k'-1), T(k') \neq T(k'+1)\}$, and $\{T(k') \neq T(k'-1), T(k') = T(k'+1)\}$. 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 obtain the probabilities of the three cases [15]

$$P(Z_{k'-1} \neq Z_{k'}, Z_{k'} \neq Z_{k'+1}) = P(Z_{k'-1} = Z_{k'}, Z_{k'} \neq Z_{k'+1}) = P(Z_{k'-1} \neq Z_{k'}, Z_{k'} = Z_{k'+1}) = \frac{1}{3}. \tag{7}$$

Thus the probability of detection error under Gaussian noise can be approximated by $P_e \approx 4\mathcal{Q}(q/2\sigma)/3$, 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 the discussions in Section 3.1. The probability of detection error in terms of WNR becomes $P_e^{(r=2)} \approx 4\mathcal{Q}(\sqrt{\gamma/2})/3$. This analytic approximation of the probability of detection error vs. WNR is compared with the simulation result for maximum allowable run $r=2$ in Fig. 3(a), where we can see that the analytic approximation and simulation conform with each other very well.

In contrast, for LUT with 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

$$P_e^{(r=1)} \approx 2 \times [\mathcal{Q}(q/2\sigma) - \mathcal{Q}(3q/2\sigma) + \mathcal{Q}(5q/2\sigma)] = 2 \times [\mathcal{Q}(\sqrt{3\gamma}/2) - \mathcal{Q}(3\sqrt{3\gamma}/2) + \mathcal{Q}(5\sqrt{3\gamma}/2)] \tag{8}$$

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

Using a total of 500,000 simulation points at each WNR ranging from -6dB to +10dB, we compare the probability of detection error vs. WNR for maximum allowable run r of 1, 2, 3, and infinity, respectively. As can be seen from Fig. 3(b), P_e of maximum run of 2 (solid line) is significantly smaller than run of 1 (dot line) for up to $4dB$-advantage at low and medium WNR, and is slightly higher at high WNR. In addition, the further increase of LUT's run (dot-dash line and dash 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

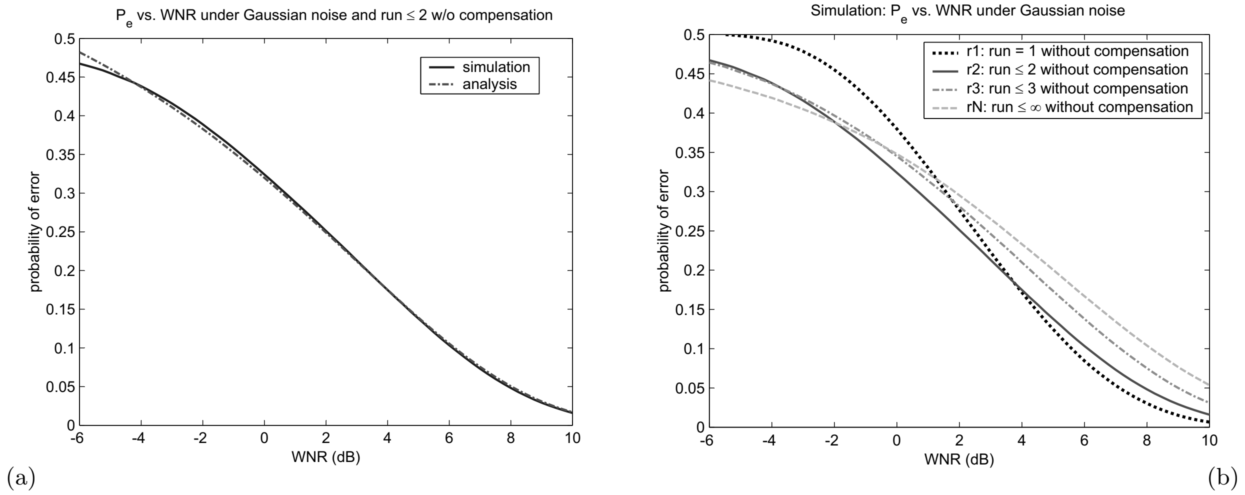


Figure 3. Detection error probability under white Gaussian noise for LUT embedding: (a) analytic and simulation results for maximum allowable LUT run of 2; (b) simulation results for different maximum allowable LUT runs.

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.

4. DISTORTION COMPENSATED LUT EMBEDDING

Motivated by Costa's information theoretical result [9], distortion compensation has been proposed and incorporated into quantization-based embedding [8,10,11], 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 [8]. The basic idea behind such improvement is to render more separation between the watermarked feature values while keeping the mean squared 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.

4.1. 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 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:

$$Y = \alpha X_1 + (1 - \alpha) X_0. \tag{9}$$

When α equals to 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 $E(|Y - X_0|^2) = E(\alpha^2 |X_1 - X_0|^2) = q^2/2$. In other words, the mean squared distortion by embedding remains the same as in the non-compensated version that uses a quantization step size of q.

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

$$SNR^{(r=2)} = \frac{2 \cdot (q/\alpha)^2}{(1-\alpha)^2 \frac{(q/\alpha)^2}{2} + \sigma_n^2}. \tag{10}$$

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

$$\alpha_{opt}^{(r=2)} = \frac{1}{1+\frac{1}{q^2/2\sigma_n^2}} = \frac{1}{1+\frac{1}{WNR}}. \tag{11}$$

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 [8] 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. And 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 is the corresponding optimal α.

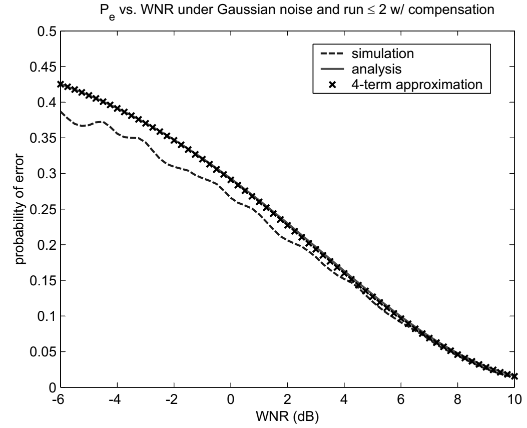


Figure 4. Detection error probability under white Gaussian noise for distortion compensated LUT embedding with maximum allowable run of 2.

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. Using the analysis from 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

$$Y = kq + (1-\alpha)X_0 = (1-\alpha)\Delta X_0 + kq/\alpha$$

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 3.2. Thus the conditional probability of error for each of the above three cases becomes

$$\begin{aligned} P_e^{(1)}(\Delta X_0) \quad &\approx \quad \frac{2}{3}\left[\mathcal{Q}\left(\frac{(1-\alpha)\Delta X_0 + q/2\alpha}{\sigma_n}\right) + \mathcal{Q}\left(\frac{q/2\alpha - (1-\alpha)\Delta X_0}{\sigma_n}\right)\right] + \\ &\quad\;\; \frac{1}{3}\left[\mathcal{Q}\left(\frac{(1-\alpha)\Delta X_0 + 3q/2\alpha}{\sigma_n}\right) + \mathcal{Q}\left(\frac{3q/2\alpha - (1-\alpha)\Delta X_0}{\sigma_n}\right)\right], \end{aligned}$$

$$P_e^{(2)}(\Delta X_0) \approx \mathcal{Q}\left(\frac{q - q/2\alpha - (1-\alpha)\Delta X_0}{\sigma_n}\right) + \frac{2}{3}\mathcal{Q}\left(\frac{(1-\alpha)\Delta X_0 + 3q/2\alpha - q}{\sigma_n}\right) + \frac{1}{3}\mathcal{Q}\left(\frac{(1-\alpha)\Delta X_0 + 5q/2\alpha - q}{\sigma_n}\right),$$

$$P_e^{(3)}(\Delta X_0) \approx \mathcal{Q}\left(\frac{(1-\alpha)\Delta X_0 + q - q/2\alpha}{\sigma_n}\right) + \frac{2}{3}\mathcal{Q}\left(\frac{3q/2\alpha - q - (1-\alpha)\Delta X_0}{\sigma_n}\right) + \frac{1}{3}\mathcal{Q}\left(\frac{5q/2\alpha - q - (1-\alpha)\Delta X_0}{\sigma_n}\right).$$

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

$$\begin{aligned} P_e \quad &= \quad \frac{2}{q/\alpha}\int_{-q/2\alpha}^{0}\left[\frac{1}{2}P_e^{(1)}(\Delta X_0) + \frac{1}{3}P_e^{(2)}(\Delta X_0) + \frac{1}{6}P_e^{(3)}(\Delta X_0)\right] d(\Delta X_0) \\ &= \quad \alpha\sqrt{2/\gamma}\int_{-\sqrt{\gamma/2}/\alpha}^{0}\left[\frac{1}{2}P_e^{(1)}(t) + \frac{1}{3}P_e^{(2)}(t) + \frac{1}{6}P_e^{(3)}(t)\right] dt. \end{aligned} \tag{12}$$

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

$$\begin{aligned} P_e \quad &\approx \quad \alpha\sqrt{2/\gamma}\int_{-\sqrt{\gamma/2}/\alpha}^{0}\left\{\frac{1}{6}\mathcal{Q}\left(\sqrt{2\gamma}(1-1/2\alpha) + (1-\alpha)t\right) + \right. \\ &\left. \frac{1}{3}\left[\mathcal{Q}\left(\sqrt{2\gamma}/2\alpha + (1-\alpha)t\right) + \mathcal{Q}\left(\sqrt{2\gamma}/2\alpha - (1-\alpha)t\right) + \mathcal{Q}\left(\sqrt{2\gamma}(1-1/2\alpha) - (1-\alpha)t\right)\right]\right\} dt. \end{aligned} \tag{13}$$

Fig. 4 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 Eq. 12, cross marks are approximations of Eq. 13, and dash 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 Eq. 12 and Eq. 13 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 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.

4.2. 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 modelled as a simple, binary symmetric channel (BSC) [14] with cross-over probability being the probability of error P_e studied above. That is,

$$C_{LUT} = 1 - h(P_e) = 1 + P_e \log(P_e) + (1 - P_e) \log(1 - P_e). \tag{14}$$

We compare the BSC embedding capacity of five cases in Fig. 5, 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 dash line, we see that when the maximum allowable run is 2, the embedding capacity increases significantly for up to $4dB$-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 dot 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 $1dB$ 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 [11], gives near-optimal embedding capacity supported by information theoretical study [8], which concerns maximizing the capacity under a specific WNR without other considerations such as the security inherent in the embedding mechanism in Section 2. 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; however, the above embedding capacity comparison alone concerns mainly the robustness and does not include information about security.

To take into account both security and robustness issues, we define a combined 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 binary symmetric channel (BSC) assumption for additive noise. That is,

$$J = \omega H_{LUT} + (1 - \omega) \cdot C_{LUT}, \tag{15}$$

where H_{LUT} is the entropy rate of LUT table given by Eq. 4, C_{LUT} is the BSC embedding capacity given by Eq. 14, and $\omega \in [0, 1]$ is a weight factor to provide desirable emphasis to security and robustness issues. We plot this combined measure at $0dB$ WNR for maximum LUT run of 1 and 2, respectively, with different weight ω and different compensation settings. We can see from Fig. 5 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 combined 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.

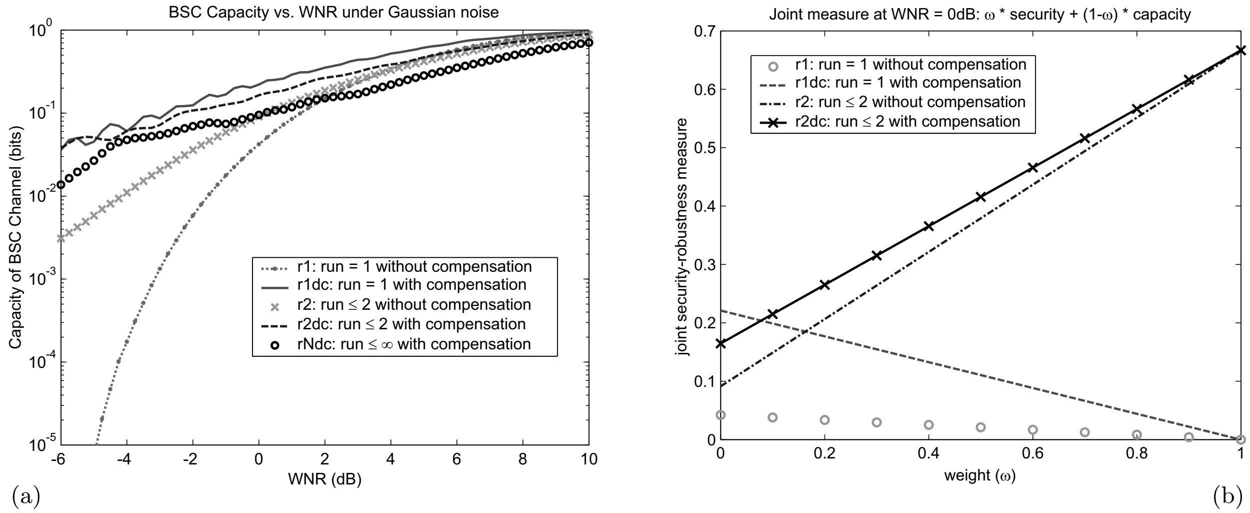


Figure 5. Joint evaluation of robustness and security for LUT embedding: (a) BSC embedding capacity under different maximum allowable LUT runs and different compensation settings; (b) the linear security-capacity combined measure of LUT embedding as a function of weight ω at a WNR of $0dB$.

4.3. Discussions

Variations of Distortion Compensation We explore a few variations of distortion compensation and compare their performance with the linear compensation in Eq. 9. We shall focus on the case of maximum allowable run of 2. As illustrated in Fig. 6, 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. 7(a) are the performances of boundary point based compensation (cross marks), mirroring based compensation (dot line), and the optimal linear compensation (solid line). The probability 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.

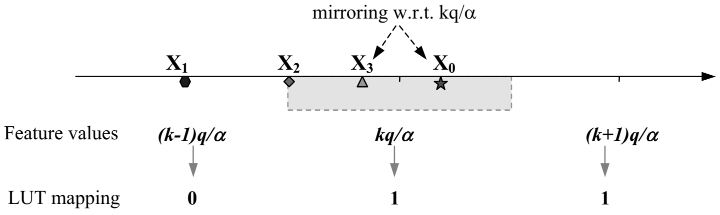
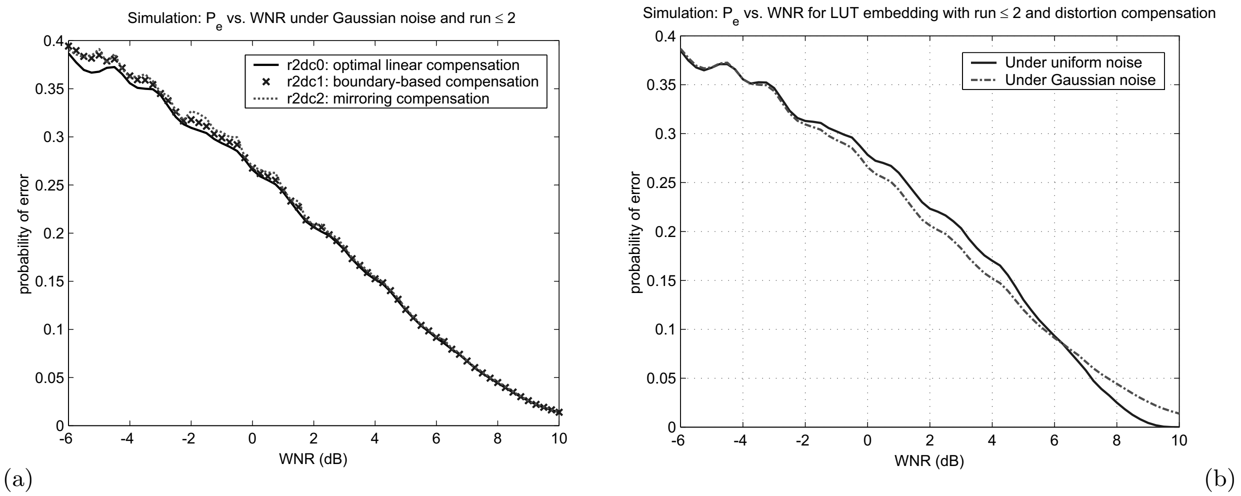


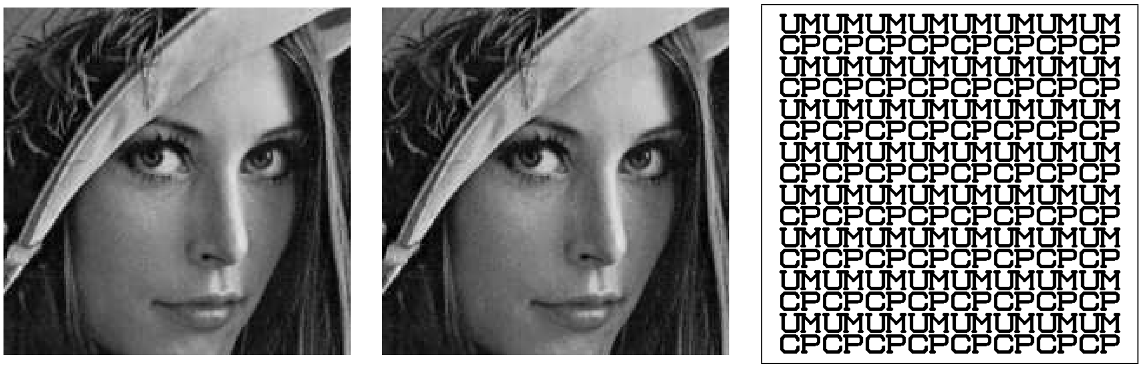
Figure 6. Illustration of different distortion compensation strategies.

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 [16]. 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 robustness comparison of LUT embedding against uniform noise versus white Gaussian noise in Fig. 7(b), 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 [16].



(a) (b)

Figure 7. Comparison of probability of error for distortion compensated LUT embedding with maximum allowable run of 2: (a) using three different compensation techniques; (b) under uniform versus white Gaussian noise for linear distortion compensation.



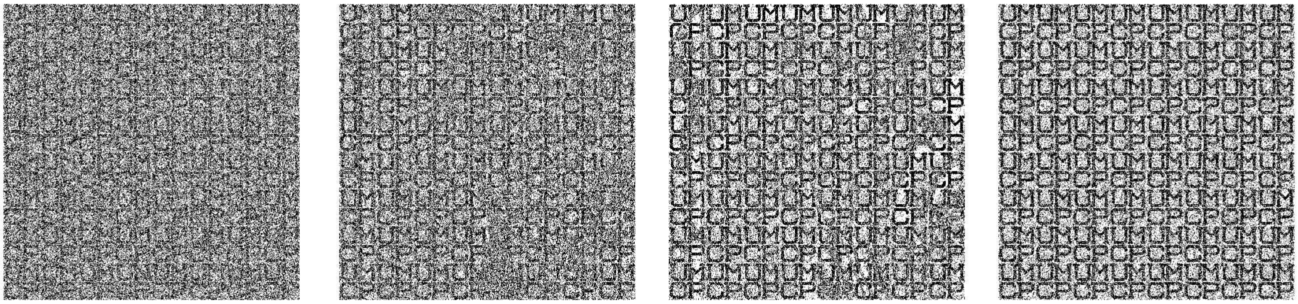
(a) (b) (c)

Figure 8. A zoomed-in view of the original Lenna image (a) and the watermarked version (b) using distortion compensated LUT embedding with run constraint of 2, along with a 512 × 512-bit pattern (c) embedded in the Lenna image.

5. EXPERIMENTAL RESULTS WITH IMAGES

As a proof-of-concept, we apply our proposed distortion compensated LUT embedding with run constraint of 2 to the 512×512 Lenna image. One bit is embedded in each pixel, and the embedded raw data forms a 512×512 pattern shown in Fig. 8(c). For comparison, we have also implemented a embedding scheme using the same LUT but without compensation [†], 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 $42dB$. Fig. 8(b) shows a zoomed-in version of watermarked Lenna by the proposed embedding with LUT run constraint of 2 and linear distortion compensation.

[†] This non-compensated 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) run=1, no compensation, error 38.8%

(b) run≤2, no compensation, error 35.1%

(c) run≤2, with compensation, error 26.0%

(d) run=1, with compensation, error 23.6%

Figure 9. Visualization of raw error pattern by LUT embedding with different settings under WNR = 0dB.

Next, we add white Gaussian noise to watermarked images and tailor its strength to give a WNR of $0dB$ in all tests. The detection errors on 512×512-bit raw data are visualized in Fig. 9, from which we can see an improvement by distortion compensation (Fig. 9(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. 9(d)) is slightly lower than that for run constraint of 2 (Fig.9(c)). These all confirm our analysis presented in Fig. 5(a) of Section 4.

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 followed by majority voting in decoding. As can be seen from Fig. 10(a)(b), 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 $0dB$, shown in Fig. 10(c), is similar to that under white Gaussian noise. This is expected based on our study in Section 4.3. Additional results on the effects of attacks other than additive white noise, such as the JPEG compression, can be found in [15].

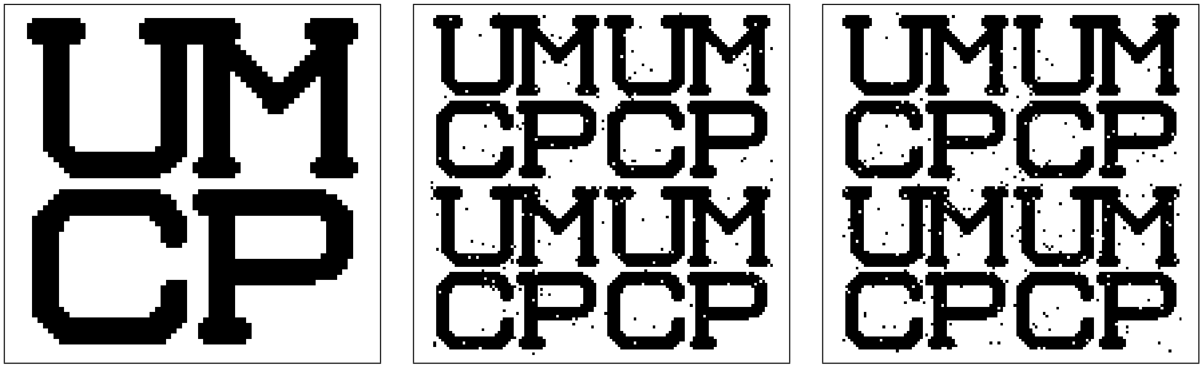
As a final note, the proposed LUT embedding with distortion compensation can be combined with advanced coding such as those in [11] to improve the coding efficiency. It can also be applied in transform domains such as the DCT and the Wavelet domain for improved tradeoffs between imperceptibility, payload, and robustness against common processing.

6. 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 look-up table mapping quantized multimedia features to binary data. The security strength of LUT embedding, quantified in terms of entropy rate, is shown to improve 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 $4dB$-advantage in WNR. We then explore distortion compensation on LUT embedding to further enhance its robustness and provide an additional advantage of up to $4dB$ in WNR. Finally, through a combined security and capacity measure, our proposed distortion compensated LUT embedding with maximum allowable run of 2 demonstrates 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.

ACKNOWLEDGMENTS

This research was supported in part by research grants from U.S. National Science Foundation CCR-0133704 (CAREER) and Minta Martin Foundation. The author thanks Prof. Bede Liu of Princeton University for insightful discussions during the early exploration of lookup table embedding.



(a) 64 repetitions, Gaussian noise **(b)** 16 repetitions, Gaussian noise **(c)** 16 repetitions, uniform noise

Figure 10. Visualization of extracted data after applying repetition coding and majority voting under WNR=0dB. The effective payloads are 64 × 64 bits for (a), and 128 × 128 bits for (b) and (c).

REFERENCES

1. I.J. Cox, M.L. Miller, and J.A. Bloom: *Digital Watermarking*, Morgan Kaufmann Publishers, 2001.
2. M. M. Yeung and F. Mintzer: "An Invisible Watermarking Technique for Image Verification", *IEEE International Conference on Image Processing (ICIP'97)*, 1997.
3. M. Holliman and N. Memon, "Counterfeiting Attacks on Oblivious Blockwise Independent Invisible Watermarking Schemes", *IEEE Trans. on Image Processing*, vol.9, no.3, pp.432-441, March 2000.
4. M. Wu and B. Liu: "Watermarking for Image Authentication", *IEEE International Conference on Image Processing (ICIP'98)*, Chicago, IL, 1998.
5. D. Kundur and D. Hatzinakos: "Digital Watermarking for Telltale Tamper-Proofing and Authentication," *Proceedings of the IEEE*, Special Issue on Identification and Protection of Multimedia Information, vol. 87, no. 7, pp.1167-1180, July 1999.
6. C-Y. Lin and S-F. Chang: "Semi-Fragile Watermarking for Authenticating JPEG Visual Content", *Proc. of SPIE Inter. Conf. on Security and Watermarking of Multimedia Contents II (EI'00)*, vol. 3971, 2000.
7. M. Wu and B. Liu: "Data Hiding in Image and Video: Part-I –Fundamental Issues and Solutions", *IEEE Trans. on Image Processing*, vol.12, no.6, pp.685-695, June 2003.
8. B. Chen and G.W. Wornell: "Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding", *IEEE Trans. on Info. Theory*, vol. 47, no. 4, pp. 1423-1443, May 2001.
9. M.H.M. Costa: "Writing on Dirty Paper", *IEEE Trans. on Info. Theory*, vol. IT-29, no. 3, May 1983.
10. P. Moulin and J. A. O'Sullivan: "Information-Theoretic Analysis of Information Hiding", *IEEE Trans. on Information Theory*, vol. 49, no. 3, pp.563-593, March 2003.
11. J.J. Eggers, R. Bauml, R. Tzschoppe, and B. Girod: "Scalar Costa Scheme for Information Embedding", IEEE Trans. on Signal Processing, vol. 51, no. 4, pp.1003-1019, April 2003.
12. M. D. Swanson, B. Zhu, A. H. Tewfik: "Robust Data Hiding for Images", *Proc. of IEEE DSP Workshop*, pp.37-40, Loen, Norway, Sept. 1996.
13. M. Alghoniemy and A.H. Tewfik: "Self-synchronizing Watermarking Techniques", *Proc. of Symposium on Content Security and Data Hiding in Digital Media*, NJ Center for Multimedia Research and IEEE, 1999.
14. T.M. Cover and J.A. Thomas: *Elements of Information Theory*, 2nd Ed., John-Wiley & Sons, 1991.
15. M. Wu: "Joint Security and Robustness Enhancement for Quantization Based Embedding," *IEEE Trans. on Circuits and Systems for Video Technology*, Special Issue on Authentication, Copyright Protection, and Information Hiding, vol. 13, no. 8, pp.831-841, August 2003.
16. M. Wu and B. Liu: *Multimedia Data Hiding*, Springer Verlag, October 2002.