

Image Dependent Log-likelihood Ratio Allocation for Repeat Accumulate Code based Decoding in Data Hiding Channels

Anindya Sarkar and B. S. Manjunath

Department of Electrical and Computer Engineering,
University of California, Santa Barbara, CA 93106

ABSTRACT

Error correction codes of suitable redundancy are used for ensuring perfect data recovery in noisy channels. For iterative decoding based methods, the decoder needs to be initialized with proper confidence values, called the log likelihood ratios (LLRs), for all the embedding locations. If these confidence values or LLRs are accurately initialized, the decoder converges at a lower redundancy factor, thus leading to a higher effective hiding rate. Here, we present an LLR allocation method based on the image statistics, the hiding parameters and the noisy channel characteristics. It is seen that this image-dependent LLR allocation scheme results in a higher data-rate, than using a constant LLR across all images. The data-hiding channel parameters are learned from the image histogram in the discrete cosine transform (DCT) domain using a linear regression framework. We also show how the effective data-rate can be increased by suitably increasing the erasure rate at the decoder.

Keywords: log likelihood ratio, repeat accumulate coding, data hiding channel, linear regression model

1. INTRODUCTION

While designing data hiding schemes for noisy channels, we encode the data bits using error correction codes of sufficient redundancy to ensure perfect data recovery, even after channel errors. An example of an end-to-end data hiding system is shown in Fig. 1. For exactly the same hiding setup, if the iterative decoding in the error correction framework can be made to converge at a lower redundancy factor, the effective hiding rate can be increased. *This can be done by proper initialization of the decoder confidence values (called log-likelihood ratios (LLRs), explained in Sec. 2) at the embedding locations.* In this paper, we propose methods for the accurate initialization of the LLR values.

Our previous hiding schemes^{1,2} have used quantization index modulation (QIM)³ for embedding in quantized discrete cosine transform (DCT) coefficients. For perceptual transparency, we do not modify coefficients that lie in the range $[-0.5, 0.5]$.¹ These coefficients are mapped to zero and are regarded as erasures (denoted by ‘e’ in Fig. 1). Repeat accumulate (RA) codes⁴ are well suited for such high erasure channels¹ - RA codes with a redundancy factor of q are used in the example in Fig. 1. The effective hiding channel in Fig. 1 includes both the image and the attack channel and is characterized by a 2×3 transition probability matrix A (mapping R to Z' in Fig. 1). As shown in Fig. 1, R is the binary codeword obtained after using RA-coding with redundancy q for a message M of N bits. Z' is a ternary sequence (elements in $Z \in \{0, 1, e\}$) obtained from the quantized DCT coefficients corresponding to the Nq embedding locations in the noisy received image. A is expressed as $\begin{bmatrix} p_{00} & p_{01} & p_{0e} \\ p_{10} & p_{11} & p_{1e} \end{bmatrix}$. Assuming a symmetric channel, the error probability p_e equals p_{01} (and p_{10}) and the erasure probability p_{er} equals p_{0e} (and p_{1e}).

Further author information: (Send correspondence to Anindya Sarkar)
Anindya Sarkar: E-mail: anindya@ece.ucsb.edu, Telephone: 1-805-893-5682

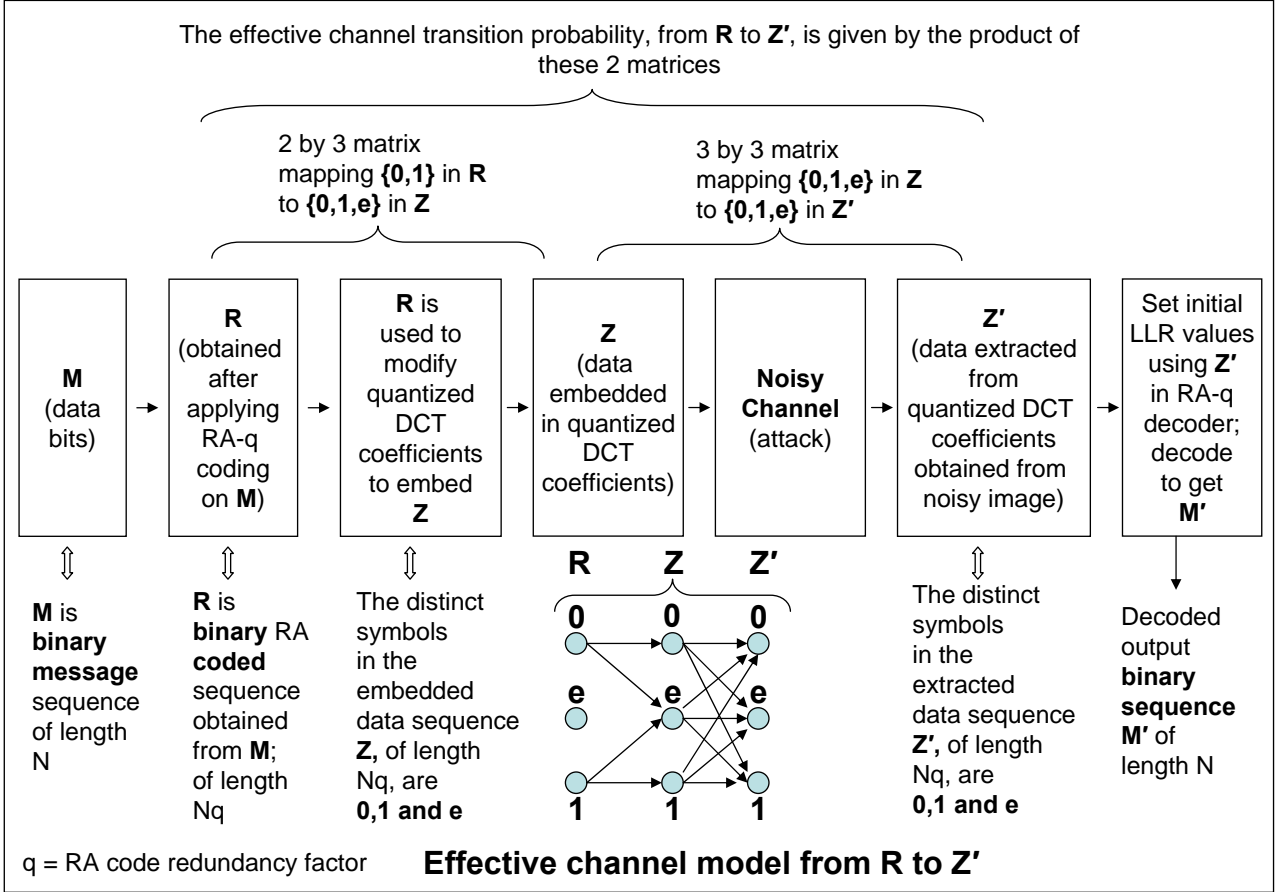


Figure 1. Embedding is done in the DCT domain using quantization index modulation (QIM) and error robustness is provided using a repeat accumulate (RA) coding framework.

2. COMPUTING THE LOG LIKELIHOOD RATIO

Let a certain image coefficient be equal to y and the corresponding embedded bit be b . The LLR value $LLR(y)$ denotes the logarithm of the ratio of the likelihood that a 0 was transmitted through that coefficient ($Pr(b = 0|y)$) to the likelihood that a 1 was transmitted ($Pr(b = 1|y)$).

$$LLR(y) = \log \left(\frac{Pr(b = 0|y)}{Pr(b = 1|y)} \right) \quad (1)$$

In our experiments, Δ , the quantization interval used by the QIM framework, equals 1 and the embedding logic used is that the coefficient is changed to the nearest even/odd integer when 0/1 is the bit to be embedded. Let x denote a DCT coefficient which gets quantized to $Q(x)$ after QIM-based embedding. Due to channel noise n , this modified coefficient is further changed to y ; assuming an additive noise model, $n = y - Q(x)$. Since consecutive quantization levels corresponding to 0 (or 1) are spaced at a distance of 2 ($\Delta = 1$) apart, the error probability p_e is expressed as follows:

$$p_e = \sum_{a=1}^{\infty} Pr(n > (2a - 1)\Delta/2, n < (2a + 1)\Delta/2) + \sum_{a=1}^{\infty} Pr(n < -(2a - 1)\Delta/2, n > -(2a + 1)\Delta/2)$$

The noise distribution falls off sharply on either side of 0. Assuming the noise to be concentrated mainly in

$[-\Delta, \Delta]$,

$$\sum_{a=1}^{\infty} Pr(n > (2a-1)\Delta/2, n < (2a+1)\Delta/2) \approx Pr(n > \Delta/2).$$

Under this assumption, $p_e \approx Pr(n > \Delta/2) + Pr(n < -\Delta/2)$,
therefore $(1 - p_e) \approx Pr(|n| \leq \Delta/2)$.

Let ‘0’ be embedded in x and it is converted to $\mathcal{Q}(x)$, the nearest even integer c ; where $c = 2t, t \in \mathbb{Z}$. Due to noise n , the received coefficient $y = n + c$. If the channel noise is small enough so that y still rounds off to c (the nearest integral value of y is called $\text{round}(y)$), the embedded bit (0) is correctly decoded. From the peaky nature of the noise n around 0, we assume that the possible quantization levels that can get mapped to c , after noise addition and rounding, are $(c \pm 1)$ - this assumes $n \in [-\Delta, \Delta]$. Thus, when the received coefficient y rounds off to c , ‘1’ could have been embedded if the noise exceeds $\Delta/2$ (or is less than $-\Delta/2$) and the coefficient after QIM-based mapping $\mathcal{Q}(x)$ is $(c-1)$ (or $(c+1)$).

$$\begin{aligned} \text{Assuming } c \text{ is even, } Pr(b=0, \text{round}(y)=c) &= Pr(\mathcal{Q}(x)=c) \times Pr(\text{round}(c+n)=c) = \\ &Pr((c-1) < x < (c+1)) \times Pr(b=0) \times Pr(|n| < 0.5) = \\ &Pr((c-1) < x < (c+1))/2 \times Pr(|n| < 0.5), \\ &\text{under the assumption that } Pr(b=0) = 1/2. \end{aligned}$$

$$\begin{aligned} \text{Assuming } c \text{ is even, } Pr(b=1, \text{round}(y)=c) &= \\ Pr(\mathcal{Q}(x)=(c-1)) \times Pr(\text{round}(c-1+n)=c) &+ Pr(\mathcal{Q}(x)=(c+1)) \times Pr(\text{round}(c+1+n)=c) = \\ \{Pr((c-2) < x < c)/2 \times Pr(n > 0.5) &+ Pr(c < x < (c+2))/2 \times Pr(n < -0.5)\}. \end{aligned}$$

$$\begin{aligned} \text{Assuming } N_c = Pr((c-0.5) \leq x < (c+0.5)), \\ Pr(\mathcal{Q}(x)=c) = Pr((c-1) < x < (c+1))/2, \Rightarrow Pr(\mathcal{Q}(x)=c) &= (N_c + N_{c-1}/2 + N_{c+1}/2)/2, \end{aligned}$$

where N_c denotes the fraction of embeddable DCT coefficients whose value changes to c on rounding. It also corresponds to the c^{th} bin in the normalized DCT histogram with integer-valued bin indices.

Using the above relations, we obtain

$$LLR(y|\text{round}(y)=c, c \neq 0) = \pm \log \left(\frac{(N_c + N_{c-1}/2 + N_{c+1}/2)(1 - p_e)}{(N_c + N_{c-1} + N_{c+1} + N_{c-2}/2 + N_{c+2}/2)p_e/2} \right), \quad (2)$$

where the \pm signs are for $c = \text{even/odd}$, respectively, and $LLR(y)$ is kept at 0 when $\text{round}(y) = 0$.

The distribution of the AC DCT coefficients has been approximated as Laplacian.^{5,6} Always, $N_{c-1} > N_c > N_{c+1}$ holds, for $c \geq 1$, and $N_c \approx N_{-c}$, by symmetry. If we assume $N_c \approx (N_{c-1} + N_{c+1})/2$, then $LLR(y)$ reduces to:

$$LLR(y|\text{round}(y)=c, c \neq 0) = \pm \log \left(\frac{1}{p_e} - 1 \right) \quad (3)$$

It is experimentally observed that the LLR allocation methods using (2) and (3) result in similar embedding rates. Hence, in subsequent experiments, the image-dependent LLR is computed using the relatively simpler expression (3). The next issue is computing p_e for a given image and noise channel.

3. OBTAINING THE CHANNEL PARAMETERS FROM THE IMAGE DCT HISTOGRAM

In our data hiding setup, the effective channel also includes the host image and hence, the channel characteristics are image dependent. We have experimented with the normalized histogram in the DCT domain as an image feature that affects the channel properties. We use a linear regression model to determine the error and erasure rates for a given image and known hiding parameters. These rates are empirically obtained for the training images. The normalized histogram of all the coefficients in the hiding band is computed and a window of $(2m+1)$ histogram bins is considered, centered at the 0^{th} bin - the bins are denoted by $\{N_{-m}, \dots, N_{-1}, N_0, N_1, \dots, N_m\}$.

$$p_e = \sum_{i=-m}^m w_{e,i} N_i, \quad p_{er} = \sum_{i=-m}^m w_{er,i} N_i \quad (4)$$

where the $\{w_{e,i}\}$ and $\{w_{er,i}\}$ terms are determined based on a Minimum Mean Squared Error (MMSE) criterion using the empirically computed p_e and p_{er} , for the training images.

The experimental setup is as follows: out of a set of 1000 images, half are used for training and the rest for testing. Data embedding is performed using Yet Another Steganographic Scheme (YASS),² our recently proposed JPEG steganographic framework. Here, a 8×8 block is chosen randomly to hide data out of a $B \times B$ big-block ($B > 8$); we have used $B = 9$ in the experiments. The design quality factor used for hiding is called QF_h and a certain number ($num = 10$) of top AC DCT coefficients, encountered during zigzag scan for a 8×8 DCT-domain block, is used as the embedding band. After hiding, the images are JPEG compressed at an output quality factor QF_a of 75. These parameters (B, QF_h, num, QF_a) are kept the same for the training and testing sets. With respect to Fig. 1, YASS just provides a method to select the “ N_q ” image coefficients to be used for hiding - any other method which uses QIM based hiding and RA code based error correction can also be used.

We plot the normalized estimation error for p_e (or p_{er}), in Fig. 2 (or Fig. 3) which equals the average estimation error in p_e (or p_{er}), divided by the average value of p_e (or p_{er}). It is seen that the normalized estimation error decreases significantly upto $m = 5$.

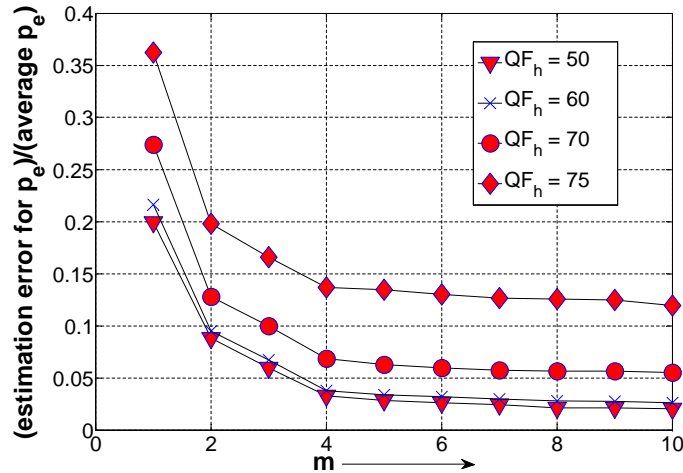


Figure 2. Variation in the normalized estimation error for p_e with m , where $(2m+1)$ weights are used to estimate p_e

4. EFFECTIVENESS OF IMAGE DEPENDENT LLR ALLOCATION SCHEME

By definition (1), $LLR(y)$ is positive/negative when 0/1 is the more likely bit and equals zero for an erasure. If the absolute value of y were less than 0.5, $LLR(y) = 0$ (erasure); else, depending on whether the received coefficient were close to an even or odd integer, $LLR(y)$ is set to α or $-\alpha$ (as used in^{1,2}), where the scaling factor α reflects the decoder’s confidence in the accuracy of the decoded bit values. In our proposed approach, the scaling factor of α has to be adjusted depending on the hiding channel characteristics.

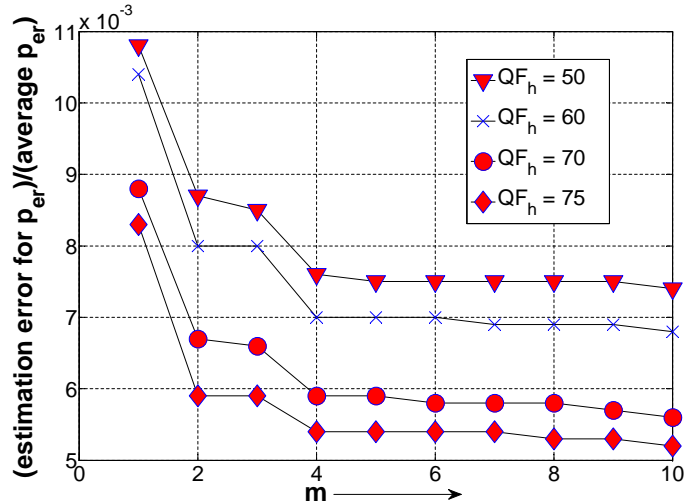


Figure 3. Variation in the normalized estimation error for p_{er} with m , where $(2m + 1)$ weights are used to estimate p_{er} .

In Table 1, the scaling factor α is varied and it is shown that the effective data-rate (that can be perfectly recovered) varies significantly depending on α . Here, the hiding rate is expressed in terms of bpnc (data-bits embedded per non-zero DCT coefficient). The bpnc is averaged over 250 images. The QIM-based hiding is incorporated in the YASS framework in these experiments. The parameters used are the same as in Sec. 3 for the estimation of p_e and p_{er} : $B = 9$, QF_h is varied from 50-75, $num = 10$ and $QF_a = 75$. The q factor in RA-q framework is gradually increased till the embedded data bits are perfectly recovered - the minimum q at which perfect recovery occurs is called q_{opt} .

It is also seen that the proper choice of α , α_{opt} (that α value which results in the highest hiding rate, i.e. the lowest value of q_{opt} , for a given set of hiding parameters $\{QF_h, QF_a, num, B\}$) decreases with increasing noise levels. The explanation is that as QF_h increases from 50 to 75, with QF_a being fixed at 75, the JPEG compression induced noise increases and hence, the confidence in the decoded bits decreases leading to a lower α_{opt} . The method that uses a constant α of α_{opt} for all the images under the same hiding conditions is called **Method 1 (M1)**. The image-dependent LLR allocation method that uses (3) is called **Method 2 (M2)**.

The results in Table 1 show the best-case results using a constant α - here, α is fixed based on the hiding conditions and does not vary per image. *It is seen that the average bpnc obtained using α_{opt} (M1) is less than that obtained using the image-dependent LLR allocation scheme (M2)*. The trend holds consistently for QF_h values in the range [50,75].

Table 1. The average bpnc for 250 images is tabulated for varying α and QF_h , using $B=9$, $QF_a=75$, $num=10$ (hiding band consists of top 10 AC DCT elements) in the YASS formulation. It is observed that $\alpha_{opt} = 9, 7, 4$ and 3 for $QF_h = 50, 60, 70$ and 75 , respectively. Since α_{opt} lies in $[1,6]$ for $QF_h = 70$ and 75 , the bpnc values for α in $[7,12]$ have not been shown.

$QF_h \backslash \alpha$	1	2	3	4	5	6	7	8	9	10	11	12	M2
50	0.0442	0.0854	0.1140	0.1316	0.1433	0.1476	0.1485	0.1498	0.1506	0.1498	0.1488	0.1468	0.1555
60	0.0491	0.0941	0.1234	0.1390	0.1395	0.1414	0.1426	0.1412	0.1402	0.1357	0.1276	0.1175	0.1537
70	0.0471	0.0891	0.1104	0.1109	0.1098	0.0986	-	-	-	-	-	-	0.1236
75	0.0418	0.0774	0.0859	0.0812	0.0635	0.0413	-	-	-	-	-	-	0.0985

4.1 Increasing the Hiding Rate Using More Erasures

At the encoder side, the erasure cutoff δ_{enc} used is 0.5. Therefore, coefficients in the range $[-0.5,0.5]$ are erased. At the decoder side, we have further increased the erasure cutoff δ_{dec} ($\delta_{dec} \geq 0.5$). Therefore, at the decoder, LLR(y) is computed as shown in (5) and (6).

$$\text{if } |y| \leq \delta_{dec}, LLR(y) = 0, \text{ for both M1 and M2} \quad (5)$$

$$\text{else } LLR(y) = \begin{cases} \pm\alpha_{opt}, & \text{for M1, if round}(y) \text{ is even/odd} \\ \pm \log\left(\frac{1}{p_e} - 1\right), & \text{for M2, if round}(y) \text{ is even/odd} \end{cases} \quad (6)$$

If $\delta_{dec} > \delta_{enc}$, the decoder will have an increased erasure rate (p_{1e} increases) while p_{11} decreases. Also, the number of erasures wrongly mapped to ‘1’ (p_{e1}) decreases, while p_{ee} increases. In this changed setup, it is seen that the effective data-rate (bpnc) increases as δ_{dec} is increased from 0.5 and then decreases after a certain point, for both M1 and M2. *The bpnc for M2 is consistently higher than that using M1, as shown in Table 2.* For M1, we have used α_{opt} of 9, 7, 4 and 3 for for QF_h of 50, 60, 70 and 75, respectively. It is seen that the bpnc is maximum for δ_{dec} of 0.60, 0.60, 0.65 and 0.70 for QF_h of 50, 60, 70 and 75, respectively.

Table 2. The bpnc value varies depending on δ_{dec} , the cutoff value used at the decoder. The hiding parameters used for YASS are $B = 9$, $QF_a = 75$ and $num = 10$.

QF_h	$\delta_{dec} = 0.50$		$\delta_{dec} = 0.60$		$\delta_{dec} = 0.65$		$\delta_{dec} = 0.70$	
	M1	M2	M1	M2	M1	M2	M1	M2
50	0.1506	0.1555	0.1560	0.1592	0.1555	0.1580	0.1549	0.1570
60	0.1426	0.1537	0.1538	0.1597	0.1536	0.1586	0.1534	0.1576
70	0.1109	0.1236	0.1266	0.1329	0.1287	0.1339	0.1260	0.1330
75	0.0859	0.0985	0.1007	0.1072	0.1030	0.1080	0.1055	0.1086

5. CONCLUSIONS

We have presented an image-dependent LLR allocation method where the LLR values are computed based on both the DCT domain image histogram and the hiding channel. We have shown that the effective hiding rate can be significantly improved by assigning accurate LLR values for initializing the RA decoder. Though we have used RA codes in our experiments, the method used for LLR allocation is general enough to be used for other iterative decoding (turbo coding) schemes. Future work shall focus on extending this LLR computation framework for other hiding schemes (apart from QIM) which use iterative decoding based error correction.

ACKNOWLEDGMENTS

This research is supported in part by a grant from ONR # N00014-05-1-0816 and ONR # N00014-10-1-0141.

REFERENCES

1. K. Solanki, N. Jacobsen, U. Madhow, B. S. Manjunath, and S. Chandrasekaran, “Robust image-adaptive data hiding based on erasure and error correction,” *IEEE Trans. on Image Processing* **13**, pp. 1627–1639, Dec 2004.
2. K. Solanki, A. Sarkar, and B. S. Manjunath, “YASS: Yet Another Steganographic Scheme that resists blind steganalysis,” in *9th International Workshop on Information Hiding*, pp. 16–31, Jun 2007.
3. 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* **47**, pp. 1423–1443, May 2001.
4. D. Divsalar, H. Jin, and R. J. McEliece, “Coding theorems for turbo-like codes,” in *36th Allerton Conf. on Communications, Control, and Computing*, pp. 201–210, Sept. 1998.
5. F. Muller, “Distribution shape of two-dimensional DCT coefficients of natural images,” *Electronics Letters* **29**, pp. 1935–1936, Oct. 1993.
6. R. Reininger and J. Gibson, “Distributions of the two-dimensional DCT coefficients for images,” *Comm., IEEE Trans. on* **31**, pp. 835–839, Jun 1983.