IMPROVEMENTS ON DATA HIDING FOR LOSSY COMPRESSION

Husrev T. Sencar[1], Ali N. Akansu[1], Mahalingam Ramkumar[2]

[1] New Jersey Institute of Technology
Electrical and Computer Engineering Department
07102 Newark, New Jersey
Email: {*taha.sencar, ali*}@*njit.edu*
[2] IDT Corp. / AVWAY.COM Inc.
07102 Newark, New Jersey
Email: *ramkumar@avway.com*

ABSTRACT

Compression is the most common application that all forms of multimedia data undergo. Lossy nature of the compression due to the use of quantizers should be taken into account by the watermarking technique employed. In this paper, we present a data hiding scheme that incorporates the embedding with the quantization of lossy compression. We show that embedder-detector sets making use of compression scheme's quantization characteristics have better payload and lower compression bit rates than independent embedding and compression. We also optimized the system parameters that maximize the hiding rate at different compression levels.

1. INTRODUCTION

Data compression is the most common application that any multimedia content will undergo. Generally speaking, content is distributed in compressed formats chosen by the content creators. Therefore, optimal design of a watermarking method for the given compression is a very practical requirement.

It is common that quantization is performed in the transform domain for lossy compression. Knowing the quantization tables utilized by the compression scheme gives information about the distortion due to lossy compression. Compression may be considered as an attack where embedder has freedom to minimize the disturbing effect of quantization noise.

Gel'fand and Pinsker, [1], derive the capacity of a discrete memoryless channel in the presence of side information known only to the decoder. Their work has become a cornerstone for oblivious data hiding applications where the message extractor has no access to host signal. Later research gained a considerable momentum by reinterpreting side information as the multimedia content that carries hidden information. Costa, [2] , was the first researcher, to present an information-theoretic analysis of a channel with side information. He evaluated channel capacity and proposed encoder-decoder structures that achieve this capacity. Ref. [3, 4] give complementary insights into the information-theoretic analysis of the problem and highlight the design criteria for practical systems.

In this paper, we present an embedder structure which makes use of the compression information. We modify the embedder described in [5, 6] by incorporating it with the quantization table utilized by the specific compression technique that follows the embedder. Results show that payload is improved and better compression is possible. We evaluate the hiding performance under JPEG compression, however, the proposed methodology is trivially applicable to any lossy compression scheme. Embedder-detector parameters are optimized by averaging the values over 40 test images.

2. DATA HIDING MODEL

The model for joint optimization of data hiding and compression may be considered as a discrete memoryless channel with an input alphabet $\mathcal{X}$ and an output alphabet $\mathcal{Y}$, both of which depend on a given side information from a finite set $\mathcal{S}$ where $\mathcal{X}, \mathcal{Y}, \mathcal{S}, \in \Re^n$. Channel capacity is expressed with the addition of an auxiliary random variable $U \in \mathcal{U}$, $\mathcal{U}$ being a finite alphabet in $\Re^n$, for the conditional joint probability density $p(u,x|s)$, $X \in \mathcal{X}$, and $S \in \mathcal{S}$ is, as in Ref. [1],

$$R = \max_{p(u,x|s)} \{I(U,Y) - I(U,S)\}. \quad (1)$$

where $I(.,.)$ is the mutual information between two random variables and R is the maximum rate of communication.

Designing $U = X + \alpha S$, under the input power constraint $\frac{1}{n}\sum_{i=1}^{i=n} X_i^2 \leq P$, Costa derived the communication rate for $Z \sim \mathcal{N}(0,\sigma_n^2 I)$, $S \sim \mathcal{N}(0,\sigma_s^2 I)$, $X \sim \mathcal{N}(0,PI)$ ($\mathcal{N}(0,1)$ is a zero mean Gaussian random variable with variance one and I is the identity matrix), where X, S, Z are independent, and proved that channel capacity is same whether the side information is known to the decoder or not.

Imposing restrictions on the distortions introduced by the information hider and attacker, such that these distortions have much less power than the cover signal S ($\frac{1}{n}\sum_{i=1}^{i=n} S_i^2 \gg P$ and $\frac{1}{n}\sum_{i=1}^{i=n} S_i^2 \gg \frac{1}{n}\sum_{i=1}^{i=n} Z_i^2$), will keep the original content more or less intact and simplify the problem. $U = X + \alpha S$ should be designed for the information hiding scheme under the best attack assumption. Moulin and O'Sullivan, [3], discuss that for oblivious information hiding assuming a memoryless embedding scheme where cover data, S, is *iid* Gaussian distributed, Gaussian attack is the optimal one. In the communication model for data hiding all intrusions of the attacker to watermarked signal will be represented by additive white Gaussian noise. However, it will not be the optimal attack for all cases. In our analysis, embedding and attack powers are represented by mean squared error distance.

The overall information hiding system is outlined below where $m \in \mathcal{M}$ is the message to be hidden, S is the original content data, X is the distortion introduced by the hider, Q is the quantization noise and Z is the intrusion of the attacker as

$$\begin{aligned} \mathcal{W} &: \quad m \longrightarrow W, \\ \hat{S} &= \mathcal{E}(S,W) = S + X, \\ Y &= \mathcal{E}(S,W) + Q + Z = S + X + Q + Z, \\ \hat{W} &= \mathcal{D}(Y), \\ \mathcal{W}^{-1} &: \quad \hat{W} \longrightarrow \hat{m}. \end{aligned} \tag{2}$$

A message indexed by m, from an alphabet $\mathcal{M}$, $1 \leq m \leq M$ is mapped out to a sequence $W \in \Re^n$. Sequence W must be embedded into the original content without any perceptual distortion. The mapping $\mathcal{W}$ from m to W is a one-to-one mapping in $\mathcal{R}^n$. The embedder, $\mathcal{E}$, and detector, $\mathcal{D}$, are nonlinear and not necessarily invertible functions $(\mathcal{D}(\mathcal{E}(S,W)) \neq W)$. The auxiliary random variable U is derived from the codebook used by the embedder-detector.

Reordering the terms in Eq. (1) for $U = X + \alpha S$ and $Y = S + X + Q + Z$, the hiding rate for the communication model in which embedder has knowledge of the quantization process, Q, we obtain the rate as

$$\begin{aligned} R(\alpha) = \max_{p(u,x|s)} & (H(X) + H(X + S + Q + Z) \\ & -H(X + S + Q + Z, X + \alpha S)). \end{aligned} \tag{3}$$

3. EMBEDDING

In order to attain higher information-hiding rates information hider has two degrees of freedom. These are of choosing the codebook and codeword. In applications, embedder-detector set is a function of α. In order to maximize the rate, information hider should maximize the distortion. Similarly, attacker distorts the watermarked content to remove all tracks of the embedded message. Communication rate is a tradeoff between the distortions of the information hider and attacker. Communication rate achieves the capacity when the ideal codebook, corresponding to the design of $U = X + \alpha S$, is generated where α is some function of channel noise statistics (e. g. for additive white Gaussian noise attack $\alpha = \frac{P}{P+\sigma_n^2}$, [2]). The codebook design for $U = X, \alpha = 0$, suffers from dramatically low hiding rates. Because, $U = X$ corresponds to a non-optimal codebook design which assumes S as an extra noise and tries to cancel it.

The choice of codebook structure for $U = X + \alpha S$ is easily realizable when $\alpha = 1$, by the use of special quantizers whose input is uncorrelated with the quantization error. These quantizers take S and W as the input and generate $X + S$ as the output where X and S are uncorrelated. References [7] and [5] employ embedder-detector sets using this type of quantizers. The drawback of choosing $U = X + S, \alpha = 1$, in an oblivious information hiding system is that the system performs better only if $\frac{P}{\sigma_n^2} \gg 1$ since communication rate can achieve the capacity only when there is no attack.

3.1. Embedder

Ramkumar, [5], proposed a practical scheme that improves the hiding rate by removing invertibility condition on the set $\mathcal{E}, \mathcal{D}$. This embedder improves channel communication for $P \leq \sigma_n^2$ using the codebook $U = X + S$, i. e. $\alpha = 1$, with a degradation in hiding rate for $\frac{P}{\sigma_n^2} > 1$.

Embedder is a quantizer characterized by two parameters, period Δ and threshold β where $0 < \beta \leq \Delta$. The form of quantizer used for implementation is a periodic continuous triangular function. Watermark signal to be embedded is limited by the peak values of the periodic function. Embedding is a translation of the input coefficient values by introducing distortions thresholded to $\pm\frac{\beta}{2}$ such that the mapping of embedded coefficient over the periodic function has a minimum Euclidean distance to the watermark signal. The period Δ and threshold β of the quantizer are dictated by the permitted embedding distortion to the content. Similarly, detection of the watermark signal is realized by mapping the watermarked signal over the periodic function with the same Δ as the embedder does and the fixed threshold $\beta = \Delta$, which adds non-invertibility to the $\mathcal{E}, \mathcal{D}$ set. Figure 1 represents embedding of two different watermark signal coefficients, x_0 and x_1, to signal coefficient s. Embedding x_0 into s generates the watermarked signal $\hat{s}_0$. Whereas, embedding x_1 into s generates $\hat{s}_\beta$ rather than $\hat{s}_1$ due to thresholding by $\pm\frac{\beta}{2}$.

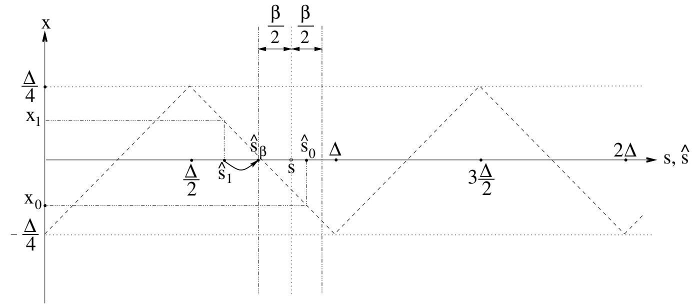


Fig. 1. Representation for embedding watermark signal to an input signal.

As $\Delta \to \infty$, for some finite β, the data hiding model assumes the use of codebook $U = X,\ \alpha = 0$. When $\Delta = \beta$ is chosen, it corresponds to use of codebook $U = X + S,\ \alpha = 1$. For all other fractions of $\frac{\beta}{\Delta}$, system performance is optimal under different attack powers.

A formal analysis of this approach was given by Sencar *et al.*, [6]. The embedder imposes power constraints by limiting the distortion level for each coefficient. As a result, distortion X corresponding to message m is replaced by X_n. Embedder derives X_n from X and imposes the input power constraint on X_n rather than on X. Since decoder is not aware of this change, $X_d = X_n - X$ can be considered as another source of noise. This may also be interpreted as a dependency between the total channel noise, $Z + X_d$, and hider's distortion, X, to the content.

Hiding rate for this embedder may be calculated by assuming $X_d \in \mathcal{X}$, being a deterministic function of X, with a nonzero correlation $E[X, X_d] = \rho_{XX_d}$, that is known to the embedder but not to the detector. Correlation, ρ_{XX_d}, is inversely proportional to a change in β such that for the two extremes $\beta = \Delta$, and $\beta = 0$ correlations are $\rho_{XX_d} = 0$ and $\rho_{XX_d} = 1$, respectively. For independent X, S and Z, X_d is also independent from S and Z. The codeword X corresponding to the message m for the content S is modified to $X_n = X + X_d$ due to the uninvertible thresholding at the embedder where detector is blind to this operation. The power constraint is also imposed on X_n rather than the codeword X, $\frac{1}{n}\sum_{i=1}^{i=n} X_{n_i}^2 \leq P$.

Recalling Eq. (1) for auxiliary random variable $U = X + S$ and reordering the terms, rate R for this data hiding scheme is derived as

$$R(\alpha = 1) = H(X) + H(X_n + S + Z) - H(X_d + Z, X + S). \tag{4}$$

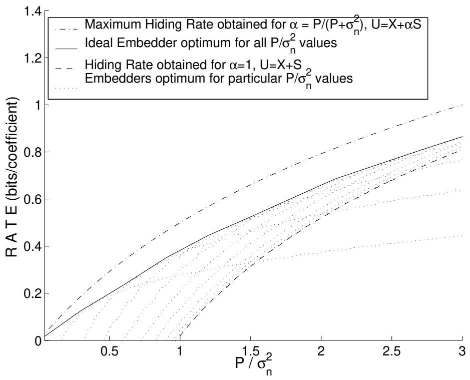


Fig. 2. Hiding rates for ideal embedding.

Reevaluating the rate given in Eq. (3) for $\alpha = 1$, Eq. (5) is obtained.

$$R(\alpha = 1) = H(X) + H(X + S + Z) - H(Z) - H(X + S) \tag{5}$$

Fig. 2 displays the maximum hiding rate (payload) obtained for the optimum α value, $\alpha = \frac{P}{P+\sigma_n^2}$, the rate for $\alpha = 1$ as in Eq. (5) and the rate for $\alpha = 1$ with the uninvertible embedder-detector for various ρ_{XX_d} values as in Eq. (4). Given the prior channel noise information, σ_n^2, ideal hiding rates for this embedding scheme can be evaluated. Otherwise, embedding performance will be optimal for a particular ρ_{XX_d} or P/σ_n^2 value.

Data hider has the freedom to pick the best among values of Δ and β for embedding. This may be interpreted as maximization of the data hiding rate by adapting the codebook to the channel noise. For the two extremes where $\frac{P}{\sigma_n^2}$ is low and high, the performance of the scheme is equivalent to the use of designs $U = X$ and $U = X + S$, respectively.

3.2. Joint embedding and compression

The idea of modifying the embedder with respect to compression characteristics relies on the fact that content creator, as the distributor, has the control over both watermarking and compression. Under this circumstance, an optimal system is the one that handles watermarking and compression jointly rather than considering them independent.

Quantization involved in compression will round watermarked signals to discrete quanta values. The difference between the mappings of the watermarked signal and the quantized watermarked signal over the embedding function is another source of distortion that decreases the hiding rate. However, knowing the quantization characteristics in advance, embedder can adjust its embedding power to lessen this type of distortion. This requires embedder to be modified in order to make comparisons between watermarked signal and its quantized version to decide on the proper embedding power. Also, using the *a priori* information on the compression, embedder chooses among the $(\Delta,\ \beta)$ parameter pair that maximizes data hiding rate.

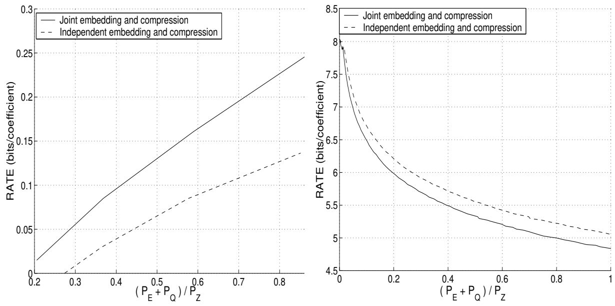
A more formal approach for the modified detector is based on the previous analysis with the addition of the quantization noise term, Q. Since compression is interrelated to embedding, resulting quantization noise is not independent from the embedding distortion, X_n. Reordering Eq. (1) for the codebook $U = X + S$, $\alpha = 1$, with the additional noise figure as

$$\begin{aligned} R(\alpha = 1) = H(X) + H(X_n + S + Q + Z) \\ -H(X_d + Z + Q, X + S). \end{aligned} \tag{6}$$

The mutual information between U and Y in Eqs. (4) and (6) varies due to existence of the quantization noise, Q. Since embedder interrelates X, X_n and Q during embedding process, these terms have a nonzero correlation with each other. At the same attack power where distortion due to quantization is a part of it, the rate calculated by Eq. (6) for the modified embedder is greater than the rate given in Eq. (4) due to additional correlation between X and Q.

What is not so readily obvious is that better compression of the watermarked signal is possible when embedding is coordinated by the compression. *As embedder tries to minimize quantization noise by changing the embedded signal value with respect to its reconstruction value at the output of the quantizer, entropy of the quantized watermark signal decreases.*

Fig. 3-a displays the hiding rates obtained for synthetically generated data using both joint and independent embedding-compression. The cover data, S, is assumed to be a vector with *iid* Gaussian distribution. Quantization step size at each point is chosen to be 6Δ. P_E, P_Q, and P_Z are distortions due to embedding, quantization and attack, respectively. Fig. 3-b displays the entropies for the watermarked signal after quantization for the same set of data. *Joint embedding and compression provides a better compression of the watermarked signal when compared with independent embedding and compression.*



(a) (b)

Fig. 3. **(a)** Hiding rates for joint and independent embedding-compression. **(b)** Entropy of the quantized embedded signals.

4. RESULTS

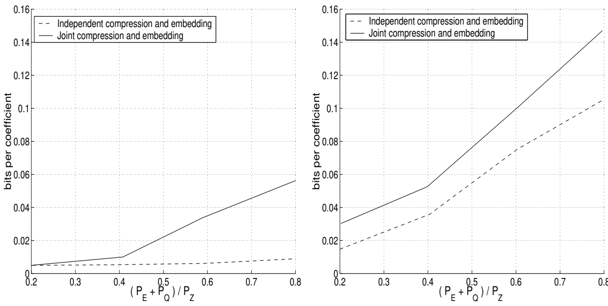
We implement a data hiding methodology on images where embedding is followed by JPEG compression scheme. Quality factor concept introduced to compression standard enables provider to compress at various bit rate values by scaling the built in quantization tables. We applied data hiding on 256x256 sized test images. Coefficients of transformed block are combined coherently into so called channels, first channel (00-channel) corresponding to DC coefficients and 63 channels corresponding to AC coefficients. We embedded the watermark signal into first 9 low frequency channels since the rest of the channels go through a coarser quantization which makes embedding extremely difficult. Watermark signal embedded into transformed image coefficients is an *iid* uniformly distributed vector of length 1024. This vector is embedded into the preselected low frequency channels by the modified embedder making use of the quantization table for a particular quality factor.

The attacker's intrusion is modeled by *iid* Gaussian noise vector of length 1024. Figure of merit for evaluating the results for the overall system is the normalized correlation between embedded watermark signal and the detected watermark signal at various ratios of total distortion due to embedding and quantization to distortion due to Gaussian noise, $FM = \frac{P_E+P_Q}{P_Z}$. We evaluate results for the range of $0.2 \leq \frac{P_E+P_Q}{P_Z} \leq 0.8$. Corresponding hiding rates are overestimated by calculating the statistics of the Gaussian noise additive to watermark signal vector so that the signal vector and the noised signal vector have the same normalized correlation.

Figures 4 a-b and 5 a-b display the hiding rates and correctly detected number of bits over the same range of $FM = \frac{P_E+P_Q}{P_Z}$ where embedding powers for JPEG-10 and JPEG-50 compression are restricted to be same. Entropies of the watermarked signals after quantization are displayed in figures 6 a-b. Modified embedder contributes less bits per pixel increase to the compression bit rate of the sample image. Tables 1 and 2 display the optimum Δ and β values for embedding to the 9 low frequency channels. They are obtained by averaging over the calculated Δ and β parameter values of the 40 test images.

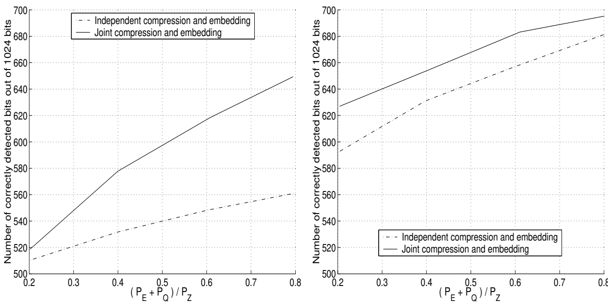
5. CONCLUSIONS

We propose a modification to the embedder described in [5] which handles embedding and compression jointly. Benefits of the proposed scheme are twofold. Based on the *a priori* information regarding compression, it becomes possible to achieve higher hiding rates by embedding at appropriate Δ and β values. It is shown that the proposed scheme improves payload for data hiding. Additionally, as embedder aims to minimize quantization noise, resultant embedded signal is more friendly to the quantization.



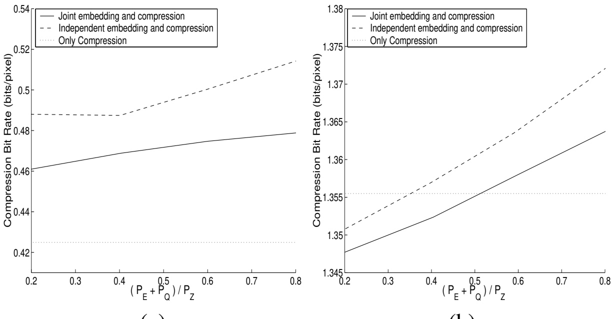
(a) (b)

Fig. 4. Hiding rates for 00-Channel with compression at quality factors ($P_E \approx [40, 170]$) **(a)** JPEG-10 and **(b)** JPEG-50.



(a) (b)

Fig. 5. Number of correctly detected bits out of 1024 hidden bits for ($P_E \approx [40, 170]$) **(a)** JPEG-10 and **(b)** JPEG-50.



(a) (b)

Fig. 6. Entropy rates after quantization corresponding to **(a)** JPEG-10 and **(b)** JPEG-50. **(b)**.

	$FM = 0.2$		$FM = 0.4$		$FM = 0.6$		$FM = 0.8$	
	Δ	β	Δ	β	Δ	β	Δ	β
Ch. 00	485	96	471	130	472	168	465	190
Ch. 01	257	64	199	67	174	69	169	76
Ch. 02	171	45	148	49	137	54	117	50
Ch. 10	253	59	210	67	200	80	171	77
Ch. 11	199	51	159	50	149	55	143	60
Ch. 12	217	60	185	62	175	67	168	72
Ch. 20	224	58	184	60	177	66	165	70
Ch. 21	195	56	171	58	160	60	152	63
Ch. 22	219	65	204	73	202	78	193	83

Table 1. Δ and β values of 9 low frequency channels optimized for JPEG-10.

	$FM = 0.2$		$FM = 0.4$		$FM = 0.6$		$FM = 0.8$	
	Δ	β	Δ	β	Δ	β	Δ	β
Channel 00	280	47	253	61	276	81	291	107
Channel 01	100	34	81	32	67	29	67	33
Channel 02	93	35	80	38	55	24	57	30
Channel 10	107	34	91	38	79	37	71	31
Channel 11	92	31	89	41	65	30	63	31
Channel 12	96	40	77	35	75	42	58	29
Channel 20	90	31	79	32	90	49	60	28
Channel 21	96	39	84	44	55	25	51	23
Channel 22	93	38	72	30	65	31	44	20

Table 2. Δ and β values of 9 low frequency channels optimized for JPEG-50.

6. REFERENCES

[1] S. I. Gelfand and Mark S. Pinsker, "Coding for channel with random parameters," *Problems of Control and Information Theory*, vol. 9, no. 1, pp. 19–31, 1980.

[2] Max Costa, "Writing on dirty paper," *IEEE Transactions on Information Theory*, vol. 29, pp. 429–441, 1983.

[3] Pierre Moulin and Joseph A. O'Sullivan, "Information-theoretic analysis of information hiding," preprint.

[4] Mahalingam Ramkumar and Ali N. Akansu, "Capacity estimates for data hiding in compressed images," *IEEE Transaction on Image Processing*, vol. 10, no. 8, pp. 1252–1263, Aug. 2001.

[5] Mahalingam Ramkumar and Ali N. Akansu, "Self-noise suppression schemes for blind image steganography," in *Proc SPIE Multimedia Systems and Applications*, 1999, vol. 3845.

[6] Husrev T. Sencar, Mahalingam Ramkumar, and Ali N. Akansu, "Efficient codebook structures for practical information hiding systems," in *Proc CISS*, Mar. 2001.

[7] Brian Chen and Gregory W. Wornell, "Provably robust digital watermarking," in *Proc SPIE Multimedia Systems and Applications*, 1999, vol. 3845, pp. 43–54.