Arjun Nichal, Dr. Shraddha Deshpande / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue 4, June-July 2012, pp.751-755

A High Capacity Data Hiding Method for JPEG2000 Compression System

Arjun Nichal*, Dr. Shraddha Deshpande**
*(Department of Electronics, Walchand College of Engineering, Sangli, Maharashtra 416415, India
** (Department of Electronics, Walchand College of Engineering, Sangli, Maharashtra 416415, India

ABSTRACT

Data hiding is an important branch of information security. Imperceptibility and Hiding Capacity are very important aspects for efficient secret communication. It is necessary to increase hiding capacity for JPEG2000 baseline system because available redundancy is very limited. In this paper Redundancy Evaluation method is used for increasing hiding capacity. This method determines embedding depth adaptively for increasing hiding capacity. Large quantity of data is embedded into bitplanes, but at the cost of slightly change in Peak Signal to Noise Ratio (PSNR). This method easily implemented in JPEG2000 compression encoder and produced stego stream decoded normally at decoder. Simulation result shows that this method is secure and increases hiding capacity.

Keywords - Secret communication, JPEG2000, Data hiding, Information security, PSNR.

INTRODUCTION

Information hiding in digital images has drawn much attention in recent years. Secret message encrypted and embedded in digital cover media. The redundancy of digital media as well as characteristics of human visual system makes it possible to hide secret messages. Two competing aspects are considered while designing information hiding scheme 1) Hiding capacity and 2) Imperceptibility. Hiding capacity means maximum payload. Imperceptibility means keeping undetectable [1].

A least significant bits (LSB) substitution method is widely used for hiding data in digital images. This method widely used because of large capacity and easy implementation. This kind of secret data embedding approach carried out in image pixel and quantized discrete cosine transform (DCT) [2]-[3]. In JPEG compression system secure data hiding scheme achieved by modifying quantized DCT coefficients. A DCT domain data hiding scheme can be applied in JPEG very conveniently. A JPEG2000 international coding standard is based on discrete wavelet transform. Some data hiding schemes cannot fitted to JPEG2000 compression system directly. All secret data will be destroyed because of truncating operation if it is embedded into lowest bitplanes [4]. For JPEG2000 compression standard limited redundancy and bitstream truncation makes it difficult to hide information. To overcome these two problems redundancy evaluation method is used [5]-[6]. Redundancy evaluation method determines embedding depth adaptively for increasing hiding capacity. A candidate embedding point will be removed if evaluated quantization redundancy is less than two. For security purpose secret message is encrypted by using encryption key. At decoder side exact inverse procedure is used for extraction of secret message.

I. SECRET MESSAGE EMBEDDING ALGORITHM

This message embedding algorithm uses redundancy evaluation method for increasing hiding capacity. Quantized secret message embedded wavelet coefficients compressed by using JPEG2000 compression baseline system. Secret message is encrypted by using secret encryption key. Same secret encryption key is used at decoder side for extraction of secret message

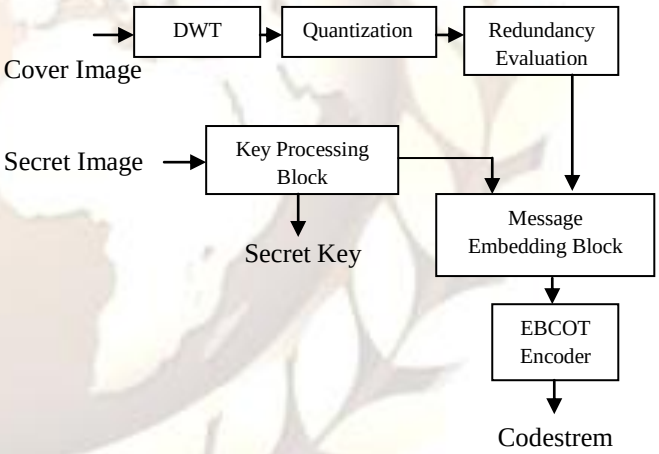

Fig. 1 Secret message embedding block diagram

1.1 Discrete Wavelet Transform

Cover image is decomposed by using discrete wavelet transform up to certain level.

1.2 Quantization

Uniform scalar quantizer is used for quantization purpose.

$$q_b[n] = sign(y_b[n]) \left\lfloor \frac{y_b[n]}{\Delta_b} \right\rfloor \quad (1)$$

Here $y_b[n]$ denotes the sample of subbands, while $q_b[n]$ denotes the quantization indices and Δ_b denotes the step size.

1.3 Redundancy Evaluation

The redundancy of uniform quantization is determined according to the visual masking effect and brightness sensitivity of human visual system. The calculation of self- contrast masking effect, neighborhood masking effect and local brightness weighting factor is calculated as follows. In the first step self-contrast masking effect is calculated,

$$y_i = sign(\overline{x_i})|\overline{x_i} \cdot \Delta_i|^{\alpha} \quad (2)$$

Where $\overline{x_i}$ is the quantized wavelet coefficient with bits lower than highest no-zero bit are replaced by zeros. Δ_i is quantization step. Parameter α takes value between 0 and 1. Result of first step is y_i. In second step neighborhood masking is calculated

$$z_i = \frac{y_i}{1+(a\sum_{k\in neighborhood}|\hat{x}_k|^{\beta})/|\phi_i|} \quad (3)$$

The symbol $\hat{x}_k$ denotes the neighboring wavelet coefficients greater than or equal to 16 and its bits lower than highest no-zero are replaced by zeros. Symbol $|\phi_i|$ is number of wavelet coefficient in neighborhood. Parameter β assumes value between 0 and 1. Parameter a is a normalization factor and having constant value $a = (10000/2^{d-1})^{\beta}$. d is a bit depth of image component. In third step weighting factor about brightness sensitivity is calculated.

$$\Lambda(l,i,j) = \begin{cases} 2 - L(l,i,j), & if\ L(l,i,j) < 1 \\ L(l,i,j), & Otherwise \end{cases} \quad (4)$$

$$L(l,I,J) = 1 + \frac{1}{128} I_0^k \left(1 + \left[\frac{i}{2^{k-1}}\right], 1 + \left[\frac{j}{2^{k-1}}\right]\right) \quad (5)$$

$\Lambda(l,i,j)$ is a local brightness weighting factor. The symbol I_l^{θ} denotes the sunband at resolution level $l \in \{0,1,\ldots..k\}$ and with orientation $\theta \in \{LL, LH, HL, HH\}$. The symbol $I_l^{\theta}(i,j)$ denotes the wavelet coefficient located at (i,j) in subband I_l^{θ}. The level of discrete wavelet decomposition is k. The result of next step is

$$z_i^{'} = \frac{z_i}{\Lambda(l,i,j)} \quad (6)$$

Final quantization redundancy is calculated by using following equation.

$$r_i = \frac{x_i}{z_i^{'}} \quad (7)$$

The redundancy of wavelet coefficient $\overline{x_i}$ can be measured by r_i , for avoiding degradation of image we use wavelet coefficients with r_i not less than 2 to carry message bits.The rules of adjusting embedding points and intensity is as follows.

1) If $r_i < 2$, then embedding point should be removed.
2) If $2^n \le r_i < 2^{n+1}$ then embedding capacity of this point is determined by n bits.

The final n_i is the adaptive embedding depth for each quantized wavelet coefficient $\overline{x_i}$.

1.4 Key Processing Block

In this step secret image is encrypted by using secret key. Encryption process hides the contents of the information whereas stegnography hides existence of the information. Suppose m_i is a secret data and n_i is a secret key, then final encrypted data will be,

$$Encrypted\ data = m_i \oplus n_i \quad (8)$$

1.5 Message Embedding Block

In this message embedding block message is embedded adaptively in quantized wavelet coefficient. First threshold assigned for embedding process. Wavelet coefficients greater than given threshold are chosen as candidate embedding point. Threshold calculated as follows.

$$Threshold = 2^n \quad where\ n = 4,5,6,7 \quad (9)$$

Next step is to calculate lowest embed allowed bitplane. This can be calculated by using following formula.

$$Lowest\ embed\ bitplane = \frac{\log(threshold)}{\log(2)} - 1 \quad (10)$$

Bitplanes lower than lowest embed allowed bitplanes are truncated during compression process.
Now suppose value of threshold is 16. Four wavelet coefficients A, B, C and D having values 33, 65, 9 and 128 respectively. Coefficient C cannot chosen for embedding process because its value is less than threshold. Lowest embed allowed bitplane is 3. Now after calculation of redundancy, result for wavelet coefficients A, B and D as follows.

$r_A = 1.59$ $r_B = 2.60$ $r_D = 12.5$

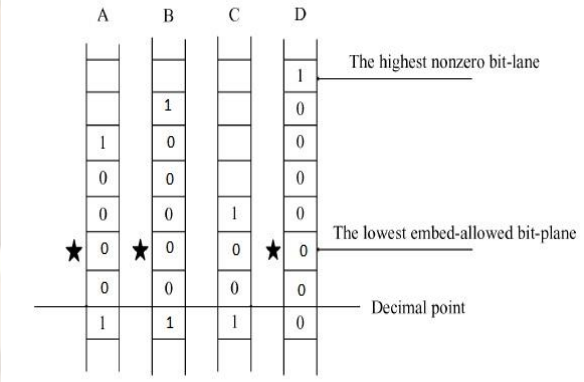

Fig. 2 Candidate Embedding Points

Value of r_A is less than 2 . Wavelet coefficient A cannot be used for embedding process.

Value of r_B is greater than 2. $2^1 < 2.60 < 2^2$ so the embedding capacity of coefficient B is 1 bit.

Value of r_D is greater than 2. $2^3 < 12.5 < 2^4$ so the embedding capacity of coefficient D is 3 bits.

In next step encrypted bits are embedded into selected wavelet coefficients adaptively.

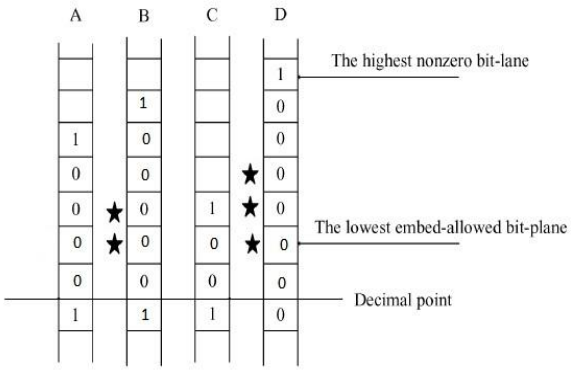

Fig. 3 Adjusted embedding points and intensity

1.6 Embedded Block Coding and Optimized Truncation (EBCOT) Encoder

After message embedding process message embedded quantized subbands are encoded by using Embedded Block coding and optimized truncation (EBCOT) encoder. EBCOT encoder is used in JPEG2000 baseline system for encoding purpose. Three coding passes are used in EBCOT encoder 1) Significance propagation pass 2) Magnitude refinement pass 3) Clean-up pass. These three coding passes are used for encoding purpose. Final output of this EBCOT encoder block is one dimensional codestream.

II. SECRET MESSAGE EXTRACTION ALGORITHM

Extraction process is simply inverse process to that of embedding process.

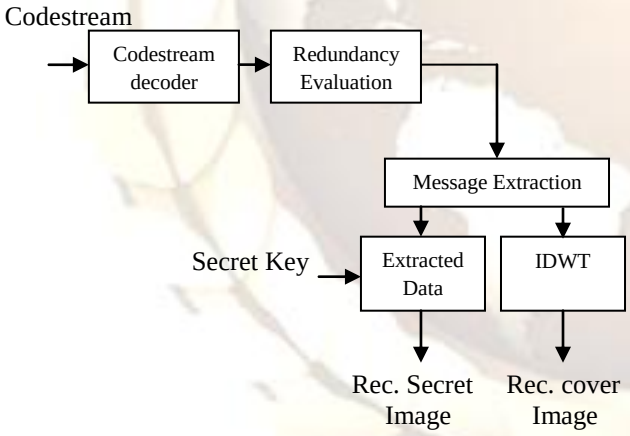

Fig. 4 Secret message extraction algorithm

Codestream is the input for secret message extraction algorithm. Output of the codestream decoder is a subbands. After codestream decoder redundancy is to be evaluated as described in secret message embedding algorithm. By using quantization redundancy matrix r_i embedded secret bits are extracted from subbands. Extracted secret bits are encrypted bits. So original secret image recovered by using following formula.

$$m_i = Encrypted\ data \oplus n_i \qquad (11)$$

Where m_i is a recovered secret image and n_i is encryption key. Encryption key used at embedding operation and extraction operation are same. Inverse discrete wavelet transform (IDWT) is used for recovering cover image

III. QUALITY PARAMETERS

For comparing With Redundancy Evaluation Method and Without Redundancy Evaluation Method we have considered various quality parameters such as Compression Ratio (CR), Peak Signal to Noise Ratio (PSNR) and Embedding Capacity (EC).

3.1 Compression Ratio (CR)

The compression ratio is calculated as the ratio of number of bits required to represent original image to the number of bits required to represent compressed codestream.

$$CR = \frac{\text{Number of bits required to represent original image}}{\text{Number of bits required to represent compressed codestream}} \qquad (12)$$

3.2 Peak-Signal to Noise Ratio (PSNR)

The PSNR is calculated by using following formula.

$$PSNR = 10log_{10}\left(\frac{MAX_I^2}{MSE}\right) \qquad (13)$$

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

Where MAX_I is maximum possible pixel value of image $I(i,j)$. MSE is a mean square error. $I(i,j)$ is a original cover image. $K(i,j)$ is a reconstructed cover image. m is number of rows and n is number of columns.

3.3 Embedding Capacity (EC)

Embedding capacity is calculated by using following formula.

$$EC = \sum_{i=1}^{n}\sum_{j=1}^{m} n(i,j)$$

$$if\ \bar{x}(i,j) > Threshold \qquad (14)$$

$\bar{x}(i,j)$ is a quantized wavelet coefficient matrix.

IV. EXPERIMENTAL RESULTS AND DISCUSSIONS

In this paper binary secret image is embedded into grayscale cover image. Image into image steganography scheme is to be carried out. Some standard grayscale images are used as a cover images. With Redundancy Evaluation Method and Without Redundancy Evaluation Method are compared on the basis of various performance parameters such as Compression Ratio (CR), Peak Signal to Noise Ratio (PSNR) and Embedding Capacity (EC).
Lena image having size 512*512 is used for processing.

(a) **(b)**

Fig. 5 (a) Original Lena Image, (b) Secret Image

Now with compression rate 0.5, Decomposition level 5 and threshold 32 determined embedding capacity of Lena image is 5575 bits. 5476 bits embedded in Cover image Lena with compression ratio 15.9959. At decoder side same parameters used for extraction of secret message. After decoding process value of PSNR is 34.2839db. Only the first, Second and third decomposition levels are used to embed secret messages. The forth and fifth decomposition level contains important low frequency components that cannot modified to hide secret messages.

(a)

(b)

Fig. 6 (a) Reconstructed Lena Image, (b) Retrieved Secret Image

Table 1: Results for Lena image with diff. compression rate and common threshold = 32

C. Rate	*With Redundancy Evaluation*			*Without Redundancy Evaluation*			*C. Ratio*
	EC	**NBE**	**PSNR**	**EC**	**NBE**	**PSNR**	
0.2	1482	1444	30.973	741	676	31.217	39.974
0.4	4092	3844	33.522	2045	1936	34.322	19.993
0.6	7129	7056	35.065	3564	3364	36.154	13.330
0.8	10094	10000	36.328	5049	4900	37.446	9.998
1	13021	12996	37.263	6515	6400	38.414	7.998

C. Rate is a compression rate, EC is a embedding Capacity, NBE is number of bits embedded, PSNR is Peak Signal to Noise Ratio and C. Ratio is a Compression Ratio.

Table 2: Results of Lena Image with diff. Thresholds and common compression rate = 0.5.

Threshold	*EC of With RE*	*EC of Without RE*
16	13452	6725
32	5574	2787
64	1915	957
128	420	210

EC of With RE means Embedding capacity With redundancy evaluation and EC of Without RE means Embedding Capacity of Without Redundancy Evaluation.

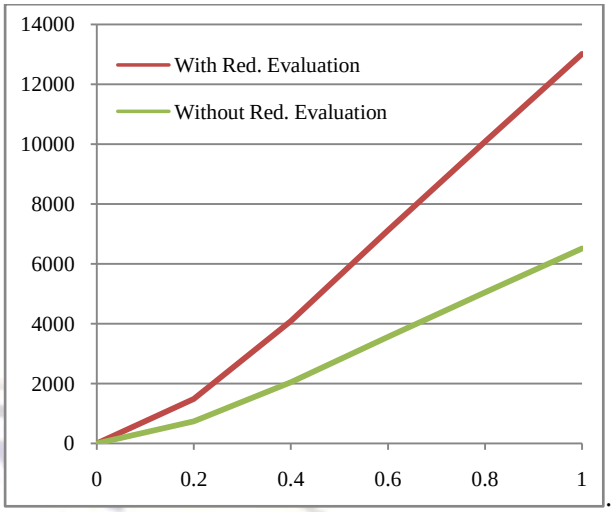

Fig. 7 Compression rate Vs Embedding Capacity

Compression rate Vs embedding capacity is plotted for both With and Without Redundancy Evaluation method.

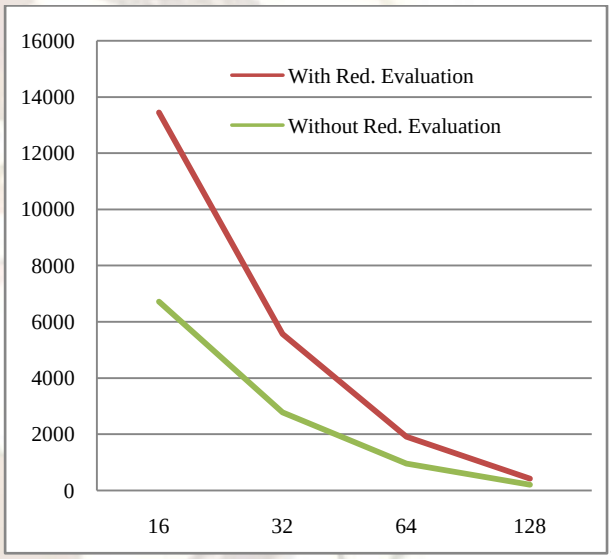

Fig. 7 Threshold Vs Embedding Capacity

Threshold Vs Embedding capacity (EC) plotted for both With as well as Without Redundancy Evaluation Method.

V. CONCLUSION

Results produced with With Redundancy Evaluation method yields in large embedding capacity than Without Redundancy Evaluation method. Without changing much image quality maximum secret data is to embedded.

Redundancy evaluation method increases Embedding capacity (EC) at the cost of slight change in Peak Signal to Noise Ratio (PSNR).

This effort gives comprehensive study of image steganography for JPEG2000 baseline system with variety of quality parameters.

REFERENCES

[1] N. Proves and P. Honeyman, "Hide and seek: An introduction to Steganography," IEEE Security and Privacy Mag., vol. 1, no. 3, pp. 32-44, 2003.

[2] H. C. Wu, N. I. Wu, C. S. Tsai, and M. S. Hwang, "Image steganographic scheme based on pixel-value differencing and LSB replacement methods," IEE Proc. Vis., Image , Signal Process., vol. 152, no.5, pp. 611–615, Oct. 2005.

[3] C. K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," Pattern Recognit., vol. 37, no. 3, pp. 469–474, 2004.

[4] JPEG2000 Part 1: Final Committee Draft Version 1.0, ISO/IEC. FCD 15444-1, 2000.

[5] P. C. Su and C. C. J. Kuo, "Steganography in JPEG2000 compressed images," IEEE Trans. Consum. Electron., vol. 49, no. 4, pp. 824–832, Apr. 2003.

[6] Liang Zhang, Haili Wang and Renbiao Wu, "A high capacity stegnography scheme for JPEG2000 baseline system," IEEE Transactions on Image Processing, vol. 18, no. 8, August 2009.