A Steganography method for JPEG2000 Baseline System

P.Ramakrishna Rao M.Tech.,*[CSE], Teaching Associate, Department of Computer Science, Dr.B.R.Ambedkar University, Etcherla – Srikaulam, 532 410.*

Abstract—Hiding capacity is very important for efficient covert communications. For JPEG2000 compressed images, it is necessary to enlarge the hiding capacity because the available redundancy is very limited. In addition, the bitstream truncation makes it difficult to hide information. In this paper, a high-capacity steganography scheme is proposed for the JPEG2000 baseline system, which uses bit-plane encoding procedure twice to solve the problem due to bitstream truncation. Moreover, embedding points and their intensity are determined in a well defined quantitative manner via redundancy evaluation to increase hiding capacity. The redundancy is measured by bit, which is different from conventional methods which adjust the embedding intensity by multiplying a visual masking factor. High volumetric data is embedded into bit-planes as low as possible to keep message integrality, but at the cost of an extra bit-plane encoding procedure and slightly changed compression ratio. The proposed method can be easily integrated into the JPEG2000 image coder, and the produced stego-bitstream can be decoded normally. Simulation shows that the proposed method is feasible, effective, and secure.

1. INTRODUCTION

MODERN information hiding technology is an important branch of information security. The redundancy of digital media, as well as the characteristic of human visual system, makes it possible to hide messages. Information hiding technology used in covert communication is named as steganography. Steganography has obvious difference with encryption because encryption hides information contents whereas steganography hides information existence. Three competing aspects, including capacity, security, and robustness, are usually considered in the designing of information hiding schemes. Security means invisibility and keeping undetectable. Capacity refers to the maximal secure payload. Robustness relates to the amount of modification the stego-object can withstand before an adversary can destroy the hidden information. Generally speaking, robustness is often emphasized in applications of digital watermarking rather than steganography. Security and enough hiding capacity should be needed for desired steganography algorithms. On the one hand, sufficient secret message bits can be embedded into cover objects, so as to ensure the effectiveness of communications. On the other hand, observable changes of cover objects ought to be avoided after information embedding, so as to ensure the security of communications.

The least significant bits (LSB) method is widely used to hide data into digital images because of its large capacity and easy implementation. In this kind of approach, messages are embedded into least significant bits of image pixels, palette indices, or quantized discrete cosine transform (DCT) coefficients. There have been many steganographic techniques utilizing LSB method, such as EZ-Stego, J-Steg, JPHide-Seek, and Out-Guess.

In JPEG coding system, quantized DCT coefficients are entropy encoded without distortion to get the final compressed bitstream. Secure information hiding can be achieved simply by modification on the quantized DCT coefficients. A DCT domain hiding scheme can be applied in JPEG very conveniently. There have been many kinds of DCT domain information hiding schemes developed for JPEG standard, such as the above-mentioned J-Steg, JPHide-Seek, and OutGuess. However, the situation is quite different for JPEG2000. As the latest still image coding international standard, JPEG2000 is based on discrete wavelet transform (DWT) and embedded block coding and optimized truncation (EBCOT) algorithms. It offers superior compression performance to JPEG, and puts emphasis on scalable compressed representations. In JPEG2000 coding system, bitstream is rate-distortion optimizing truncated after bit-plane encoding. The secret message will be destroyed by the truncating operation if it is embedded directly into the lowest bit-plane of quantized wavelet coefficients. Although there exist many kinds of DWT domain hiding schemes, most of them can not be fitted into JPEG2000 directly.

Spread spectrum hiding techniques can be applied in JPEG2000 directly, without consideration on bitstream truncation. The receiver extracts the hidden information by correlation detection. It is not necessary to keep all the embedded messages available in correlation detection. However, spread spectrum preprocessing will decrease hiding capacity significantly. Therefore, spread spectrum technology is often used in digital watermarking applications rather than covert communications.

For JPEG2000 compressed images, limited redundancy and bitstream truncation makes it difficult to hide information. After analyzing the challenge of covert communication in JPEG2000 image codec, Su and Kuo presented a steganography scheme to hide high volumetric data into JPEG2000 bitstream. In order to avoid affection of bitstream truncation, their method was not designed for the standard baseline system of JPEG2000. It was limited to the simplified version of JPEG2000, named as "lazy" mode, in which the entropy coding procedure was completely bypassed. High-capacity hiding techniques for JPEG2000 standard baseline system should be further studied. Security is another important property of a desired hiding scheme. As the counterpart of steganography, steganalysis is the art of detecting steganography. The steganographic method is assumed to be publicly known with the exception of a secret key. If there exists an algorithm that can guess whether or not a given image contains a secret message with a success rate better than random guessing, the steganographic system is considered broken. Excellent work has been done to discover the existence of hidden information. The RS algorithm and the PoVs steganalysis work well for detecting LSB embedding. Stegdetect is a famous tool that can analyze JPEG images to detect secret messages hidden by JSteg, JPHide, and Outguess. Farid developed a universal blind detection scheme that can be applied to any steganographic schemes after proper training on databases of original and cover-images. In his work, a high-dimensional feature vector was constructed from higher order statistics of wavelet coefficients and their linear prediction errors. However, it is undesirable to use too many features in terms of classification performance due to the curse of dimensionality.

Compared with spatial or DCT domain steganalysis methods, wavelet domain universal steganalysis methods ought to be more sensitive to wavelet domain steganography, because the features are extracted from wavelet domain adopted to verify the security of our hiding scheme.

In this study, a high-capacity steganography scheme is proposed for the commonly used baseline mode of JPEG2000. This method uses bit-plane encoding procedure twice to solve the problem due to bitstream truncation. Moreover, the embedding points and their intensity are adjusted image adaptively based on redundancy evaluation to increase hiding capacity.

2. JPEG2000 BASELINE CODING SYSTEM

The quantized subband is divided into codeblocks that are units of bitplane encoding, with typical dimensions of 16×16 or 32×32 or 64×64. Bit-plane encoding is operated bit-plane by bit-plane, from high to low, to produce independent bitstream for each block. Each bit-plane is encoded in a sequence of three fractional bitplane coding passes. Then, an adaptive arithmetic coding strategy, known as the MQ coder, is employed to encode the bitstream. This MQ coder is bypassed in the lazy mode of JPEG2000. The EBCOT algorithm produces a finely embedded bitstream with many useful truncation points. The bitstream can be truncated at the end of any coding passes to get desired compression ratio. The truncation point of every codeblock is determined by rate-distortion optimization.

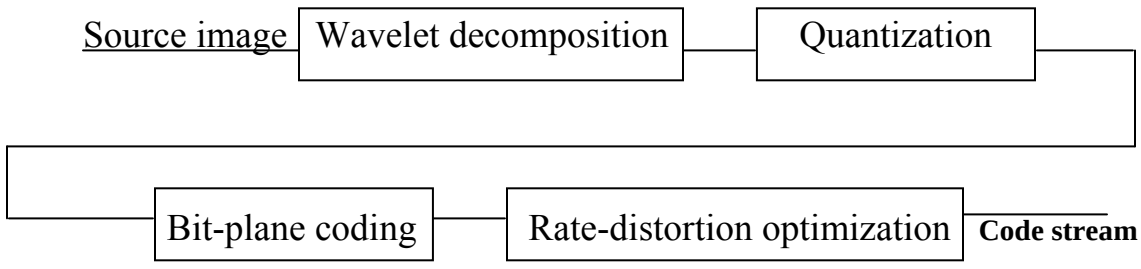

Figure1: JPEG2000 baseline encoder

JPEG2000 uses uniform scalar quantizers with enlarged "deadzones." Truncating the embedded bitstream associated with any given codeblock has the effect of quantizing the wavelet coefficients in that codeblock more coarsely. That is to say, there still exists a lossy procedure after entropy encoding. Su and Kuo have pointed out this problem. It is necessary to take some measures to keep embedded messages available.

3. STEGANOGRAPHY BASED ON TWICE BIT-PLANE ENCODING

The coding procedure of the proposed method is shown in Figure2.

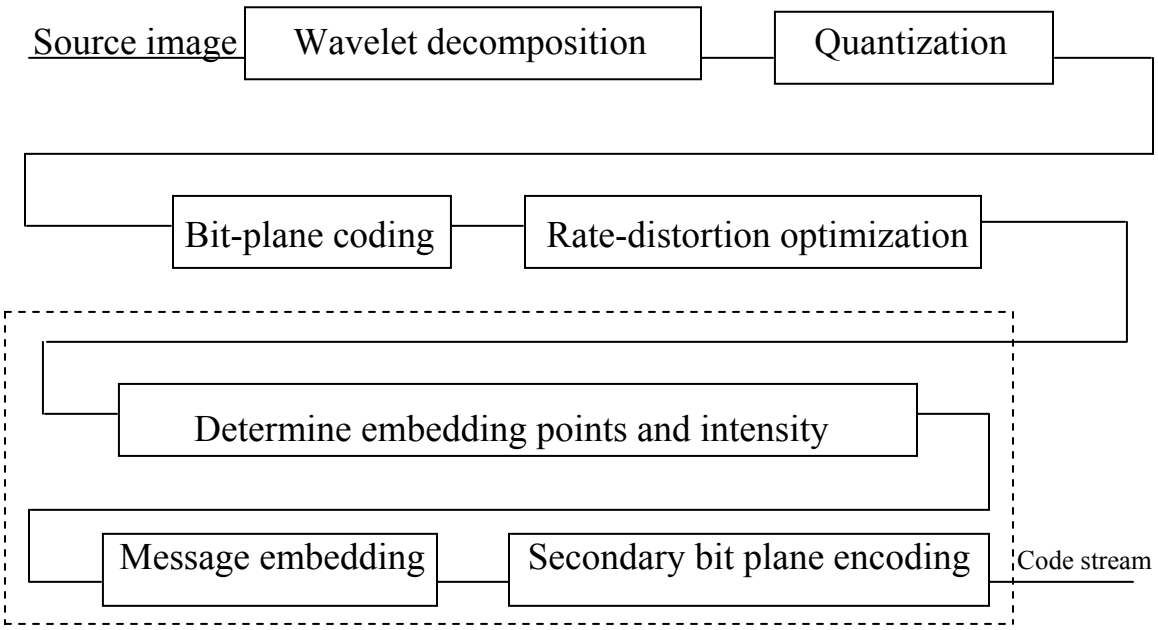

Figure2: Information hiding based on twice bit-plane encoding

Detailed descriptions of the three additional steps are:

1. There are three sub-steps involved in the determination of embedding points and embedding intensity for a codeblock as follows:
   • The wavelet coefficients greater than a given threshold are chosen as candidate embedding points.
   • According to the rate distortion optimization, the lowest bit-plane which keeps unabridged after bitstream truncation is determined as the lowest embed allowed bitplane of the codeblock.
   • The embedding points and embedding intensity are adjusted adaptively on the basis of redundancy evaluation.
2. Scrambled synchronization information and secret messages are embedded into the selected embedding points from the lowest embed-allowed bit-plane to higher ones.
3. Secondary bit-plane encoding is operated after information embedding.

After embedding, we organize the bitstream according to the previous result of rate-distortion optimization. By doing this, messages are embedded into bit-planes that would not be truncated by rate-distortion optimization. The integrality of the embedded message is ensured at the cost of increased computational complexity and slightly changed compression ratio. The twice bit-plane encoding procedure is explained to execute the bit-plane encoding twice, whereas the rest parts, such as wavelet transform, quantization, rate-distortion optimization, bitstream organization, are executed only once. Information extraction is illustrated in Figure3. First, the lowest bit-plane with complete information of all its three coding passes can be determined easily in the procedure of entropy decoding. Then the embedding points and their intensity are determined by the method similar to the encoder. Finally, both synchronization information and secret messages are extracted.

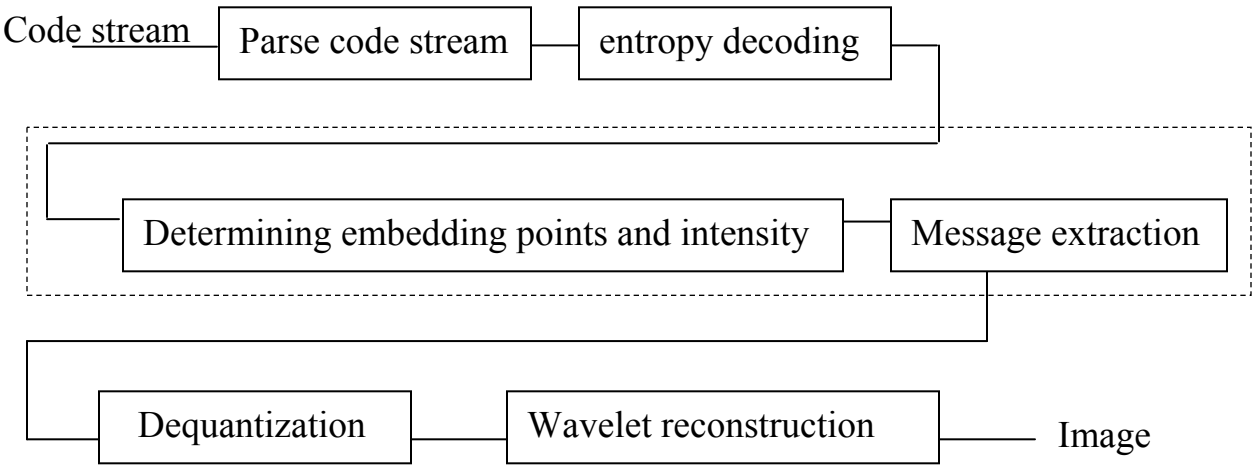

Figure3: Procedures of message extraction

IV. REDUNDANCY EVALUATION

The redundancy of uniform quantization is evaluated according to the visual masking effect and brightness sensitivity of human visual system. In this section, wavelet coefficients are processed to do redundancy evaluation, but not to be encoded. The calculation on self-contrast effect and neighborhood masking effect has been specified in the extended system of JPEG2000 for realizing nonuniform quantization. The extended part of JPEG2000 standard is consulted to select parameter values in the first two steps:

1) Self-contrast masking effect is taken in to consideration

$$y_i = sign\ (\bar{x}_i)\ |\bar{x}_i \cdot \Delta_i|^{\alpha} \qquad (1)$$

where $\bar{x}_i$ the quantized wavelet coefficient with the bits is lower than the highest no-zero bit are replaced by zeros. By clearing the lower bits, we can get identical result in both encoder and decoder. The parameter Δ_i is the quantization step of the wavelet coefficient. The parameter assumes a value between 0 and 1. The result of the first step is y_i.

2) the neighborhood masking effect is exploited to process the wavelet Coefficients as the following:

$$z_i = \frac{y_i}{1 + (\alpha \sum_{k \in neighborhood} |x_k|^{\beta}) / |\emptyset_i|} \qquad (2)$$

The neighborhood contains wavelet coefficients within a window of N×N, centered at the current position. The parameter $|\emptyset_i|$ is the total number of wavelet coefficients in the neighborhood. The parameter assumes a value between 0 and 1, together with $|\emptyset_i|$, is used to control the strength of embedding intensity adjustment due to neighborhood masking. The parameter α is a normalization factor with a constant value of $(10000/2^{d-1})^{\beta}$, and d denotes the bit depth of the image component. A small value of β suppresses the contribution of a few large wavelet coefficients around sharp edges. The parameter β is set to 0.2 in our experiments. The symbol denotes the neighboring wavelet coefficients greater than or equal to 16, and all its bits lower than the highest no-zero bit are set to be zeros. The result of the second step is z_i.

3) a weighting factor about brightness sensitivity is used in the processing. The symbol I^{θ}_{l} denotes the subband at resolution level $l \epsilon \{0,1,\ldots k\}$ and with orientation $\theta \epsilon \{LL,LH,HL,HH\}$.The symbol $I^{\theta}_{l}(i,j)$ denotes the wavelet coefficient located at (i,j) in subband I^{θ}_{l}. The level of discrete wavelet decomposition is k. Level k is the lowest resolution level, and level 0 is the highest resolution level. Because human eyes are less sensitive to noise in bright or dark image regions, the local brightness weighting factor $\Lambda(l,i,j)$ can be calculated as follows:

$$\Lambda(l,i,j) = \begin{Bmatrix} 2 - L(l,i,j): & if\ L(l,i,j) < 1 \\ L(l,i,j); & ther\ wire \end{Bmatrix} \quad (3)$$

$$L(l,i,j) = 1 + \frac{1}{128} I_0^k \left(1 + \left\lfloor \frac{i}{2^{k-l}} \right\rfloor . 1 + \left\lfloor \frac{j}{2^{k-l}} \right\rfloor \right) \quad (4)$$

Because the direct current (DC) level of the image signal has been shifted to zero before wavelet decomposition, the pixel value has a dynamic range of [-128, 127]. The local average brightness is normalized by dividing 128. Then the result of the third step, $\acute{z}_i$, is given by

$$Z_i^1 = \frac{z_i}{\Lambda\,(l,i,j)} \quad (5)$$

Quantization redundancy is calculated by the following equation:

$$\gamma_i = \frac{x_i}{z_i^1} \quad (6)$$

Uniform quantization is used in the JPEG2000 baseline system. The redundancy of the wavelet coefficient $x`_i$ can be measured by r_i. In order to reduce the image degradation, we only use the wavelet coefficients with r_i not less than 2 to carry message bits. The rule of adjustment on embedding points and intensity is as follows:

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

V. SYNCHRONIZATION INFORMATION AND SCRAMBLING MEASURE

The secret message must be divided into small fragments before it is embedded into number of codeblocks of a cover image. Some kind of predefined synchronization information is necessary for accurately extraction of the hidden message. The synchronization information can be simply structured, as shown in Figure 4.

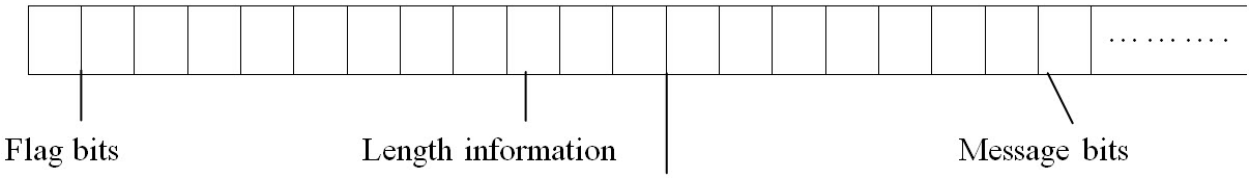

Figure4: First structure of the Synchronization information

Synchronization information is embedded into every code block before the secret message. The first part of the synchronization information is a 2-bit flag that indicates whether a certain code block contains secret message. The flag can be set to “11” or “00,” that means “accept” or “reject,” respectively. Only double zeros are to be embedded into a codeblock when it has too small hiding capacity to hold the synchronization information. The decoder will be informed by the flag to give up extracting from this code block. The second part of the synchronization information is a 12-bit fragment that indicates the length of the secret message embedded in this codeblock.

A more complex structure, depicted in Figure5, can be defined for synchronizing to provide better performance. After the flag, the follow-up twenty bits indicate where this message fragment localizes in the whole secret message. The third part of the synchronization information is a 12-bit fragment that indicates the length of the secret message embedded in this codeblock. For example, if the message fragment for a certain codeblock is from the n^{th} bit to the m^{th} bit of the secret message, then the 20-bit fragment should take value of n, and the 12-bit fragment should take value of (m-n+1). By adding the fragment of localization information, we give error resilience capability to the steganography scheme. For simplification, both the synchronization information bits and the secret message bits are all called message bits in the following discussion.

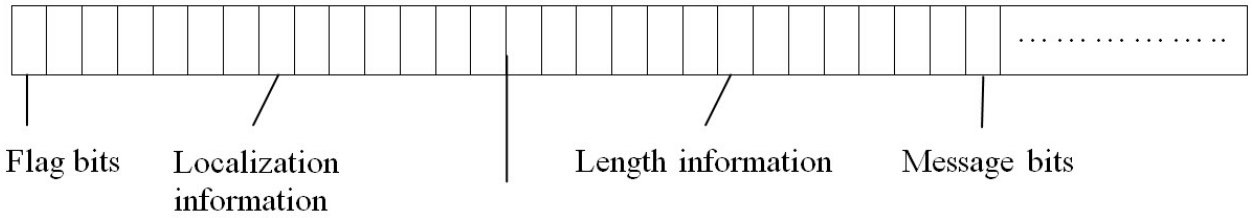

Figure5: Second structure of the synchronization information

A 64-bit secret key is used as a seed to generate a sequence of pseudo random binary numbers, which is used to scramble the message bits

$$S_i = m_i \oplus n_i \; ; \quad i = 1,2, \ldots\ldots\ldots\ldots\ldots N \qquad (7)$$

where N is the total number of message bits. The symbol m_i denotes the i^{th} message bit, and n_i the i^{th} binary number of the pseudo random sequence. The operator Θ denotes binary addition. The scrambled message bits, denoted as s_i, are to be embedded into selected wavelet coefficients. The same pseudo random sequence, controlled by the secret key, is generated and used at the decode side to retrieve m_i simply by an operation of binary addition.

VI. SIMULATION

The source image is Lena, a grayscale image of 512×512, shown in Figure6. Each pixel has eight bits. The secret message to be embedded is the logo of Civil Aviation University of China, which is shown in Figure6. It is

Figure6: (a) Original image used as cover media (b) the binary logo image used as secret message

a 80×80 binary image with a pixel depth of just one bit. Therefore, there are 6400 bits of secret message in total. In the following procedure, the source image is compressed at a ratio of 16, and information hiding is conducted simultaneously.

The source image is decomposed using five-level DWT. The forth and fifth decomposition levels contain important low frequency information that can not be modified to hide secret messages. Only the first, second and third decomposition levels

are used to embed secret messages. The procedures of wavelet decomposition, uniform quantization, bit-plane encoding and rate distortion optimization have been specified in JPEG2000 recommendations. We mainly discuss on the hiding procedure.

1) The lowest embed-allowed bit-plane of each code block is determined. The example is a code block which locates in the HL subband of the second decomposition level. According to rate-distortion optimization, the bitstream of this code block should be truncated after the third coding pass of its sixth bit-plane, counting from the highest nonzero bit-plane. All three coding passes of the sixth bit-plane will be contained in the final bitstream. This bit-plane can keep unabridged even after bitstream truncation. So the sixth bit-plane should be determined as the lowest embed-allowed bit-plane of this codeblock. Otherwise, if one or more coding passes of the sixth bit-plane has to be truncated, then the fifth bit-plane should be chosen as the lowest embed-allowed bit-plane.
2) The wavelet coefficients with magnitudes not less than a given threshold are chosen as candidate embedding points. Because the low bits will be modified by information embedding, the threshold should be the n^{th} power of two. This ensures that the embedding points chosen by the receiver are

consistent with that of the sender. In our experiments, the threshold is set to 16. With four typical wavelet coefficients as examples, the embedding points are shown in Figure7.

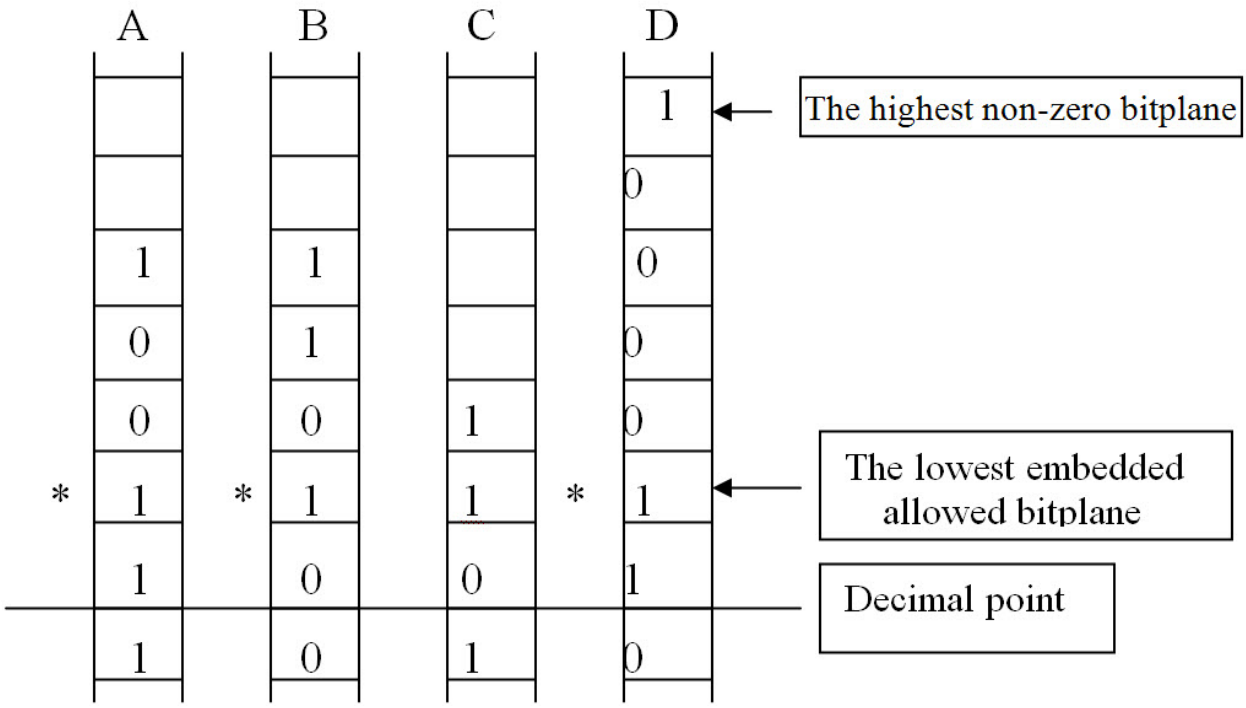

Figure7: candidate embedding points

The wavelet coefficient C can not be chosen to be a embedding point, because it is below the given threshold. Wavelet coefficients A, B, and D are chosen to be candidate embedding points, whose bits on the sixth bit-plane are labeled to be embed-allowed. The star pentagon in Figure7 denotes the position into which allow to embed message bits.

3) The candidate embedding points are adjusted image adaptively based on redundancy evaluation to increase hiding capacity. The parameters in those equations are set to be: N=5, α =0.7, β=0.2. Evaluation results for wavelet coefficients A, B, and D are as follows:

$r_A = 1.72$ $r_B = 2.59$ $r_D = 13.4$

as $1.72 < 2$, so that wavelet coefficient A can not be used to embed message bits. It should be removed from the group of candidates, and consequently, the star pentagon marked on it should be erased.

as $2^1 < 2.59 < 2^2$, so that wavelet coefficient B can be used to embed message bits. But its embedding intensity can not be enlarged any more.

As $2^3 < 13.4 < 2^4$, so that wavelet coefficient D can be used to embed message bits, and extra two bits can be embedded into wavelet coefficient D. Therefore, the bits on the fifth and forth bit-planes of wavelet coefficient D are labeled with star pentagons to allow message embedding.

The result of adaptively adjustment is shown in Figure8.

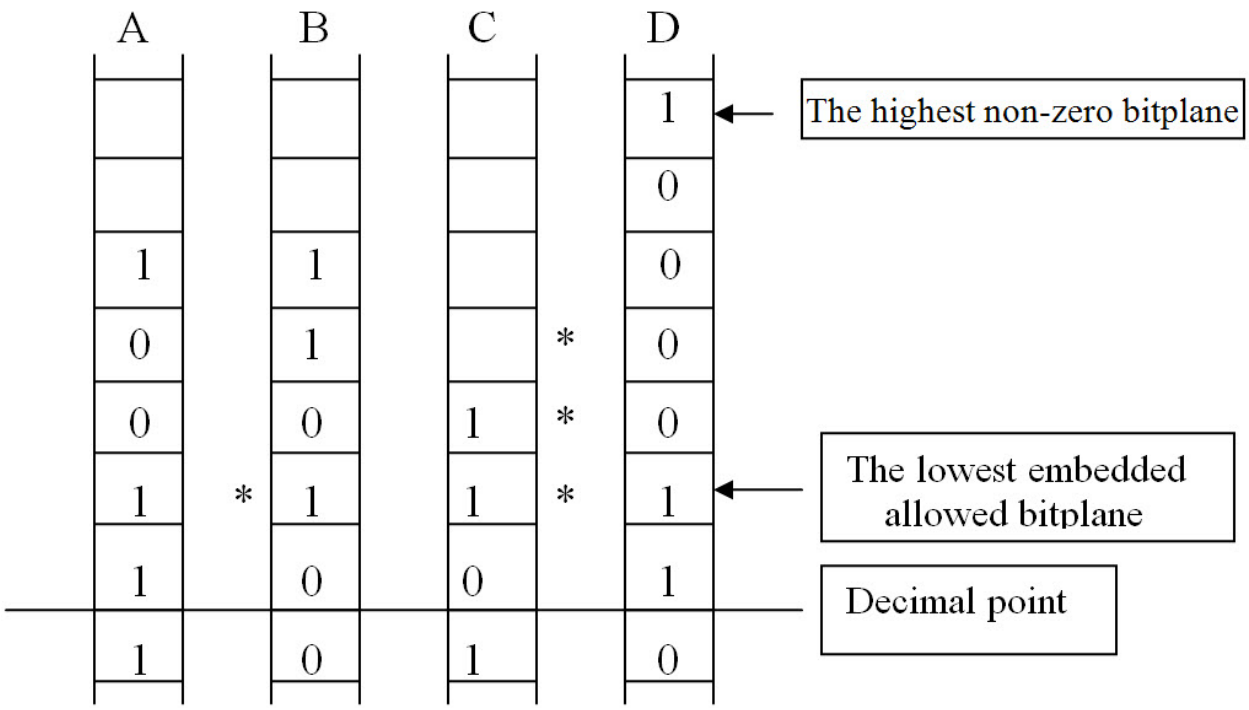

Figure8: Finally adjusted embedding points and their intensity

4) In the fourth step, we embed message bits into the selected wavelet coefficients and finish encoding the stegoimage. There are totally 63 code blocks in the first, second, and third decomposition levels of the test image. The embedding payload of each code block can be calculated to show roughly direct proportion to its hiding capacity. After payload assignment, synchronization information is added and message scrambling is conducted. Then, the code block is scanned bit-plane by bit-plane, from low to high, beginning with the lowest embed-allowed bit-plane. Once it comes across an embed-allowed position, one message bit is embedded, until all the message bits are embedded. After message embedding, secondary bit-plane encoding is operated on the modified code blocks, and, finally, the final bitstream is organized.

The bitstream can be decoded using a standard JPEG2000 decoder. The reconstructed image is shown in Figure9, which can not be distinguished from the original one shown in Figure6. Information extraction

Figure9: (a) Reconstructed Lena image (b) the retrieved logo image

is just the reverse operation of information embedding. Experiment shows that information hiding has caused slight change on PSNR (Peak Signal to Noise Ratio) and the actual compression ratio. Because information hiding

techniques are often based on the visual masking effect of human visual system, it is not suitable to use PSNR to evaluate the stegoimage degradation. The most reasonable method for evaluating subjective quality is by observation, which is also in common use. We have many people vote for the visible degradation of the stego-image to improve hiding capacity measurement. Beginning with a small quantity, the hidden message is increased by 100 bits each time. The capacity is obtained when the stego-image degradation becomes visible. The slight change of compression ratio is due to the bitstream of the secondary bit-plane encoding is different from the initial one. This small change, less than one percent in our experiments, is usually acceptable.

In order to test and measure the effectiveness on hiding capacity enlargement, we simply bypass the redundancy evaluation for comparison. Two methods are tested in the experiments.

• Method 1: With redundancy evaluation.
• Method 2: Without redundancy evaluation.

The two methods should be tested with different cover images and different

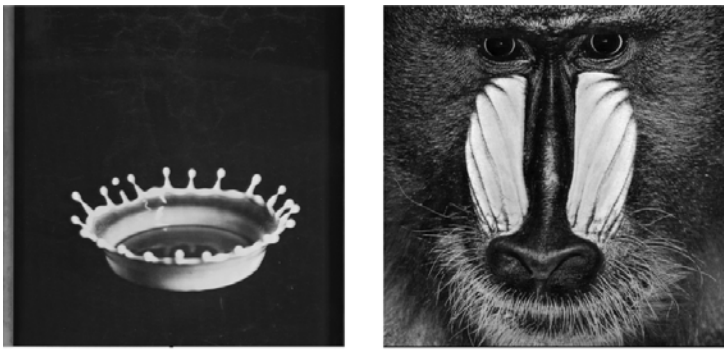

Figure10: Two images with different texture activity: (a) Crown (b) Baboon

Table 1: Hiding capacity of three test images

	Crown	Lena	Baboon
Method 2	3000	6500	11000
Method 1	4500	14000	19500

compression ratios. Together with Lena, two more images shown in Figure10 are used. The three images have same size, same pixel depth, and different texture activity. Both the two methods are tested on these images, with a compression ratio of 0.8 bits per pixel. The results are listed in Table I. The hiding capacity of Lena at different compression ratios is shown in Figure11. It can be seen that the proposed method is effective, especially for those images with uneven brightness and diverse texture activity.

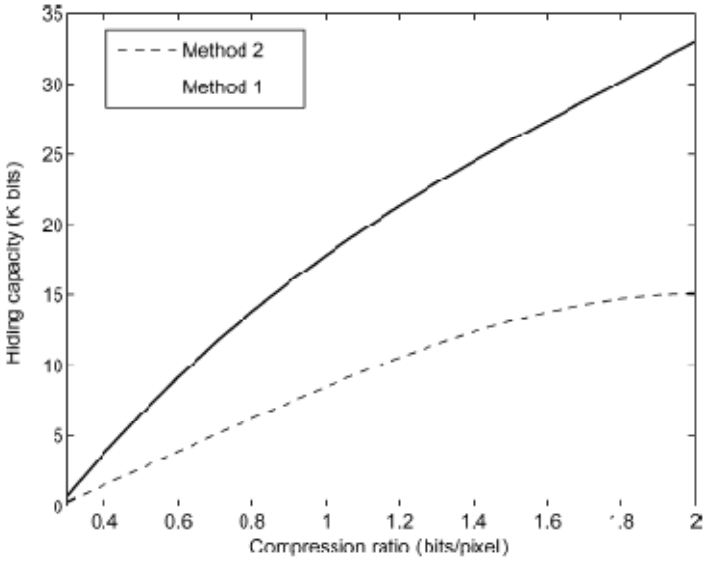

Figure11: Hiding capacity of different compression ratios

The proposed method hides information by modifying wavelet coefficients. Accordingly, a wavelet domain steganalysis method should be the best choice for the security verification. The universal steganalysis method described in, which extracts features from wavelet domain, is used to do the security verification. The stego image estimation method used has been detailed described in the author's earlier work reported. In the following experiment, samples are 1100 never compressed gray-scale digital pictures with resolution of 640480. Four examples of these pictures are shown in Figure12. We randomly choose 800 original images and the corresponding 800 stego ones for calculating the projection vector of the FLD (Fisher Linear Discriminator) classifier. The remaining 300 original images and the

Figure 12: Four different images

corresponding 300 stego ones are used for testing purpose. Figure13 shows ROC (Receiver Operating Characteristic) curves tested on different payloads: 15000 bits, 25000 bits, 35000 bits, 60000 bits, and 80000 bits. According to the experimental data, the detector is in vain when the message length is 15000 or 25000. And when we increase the payload to 35000 bits,

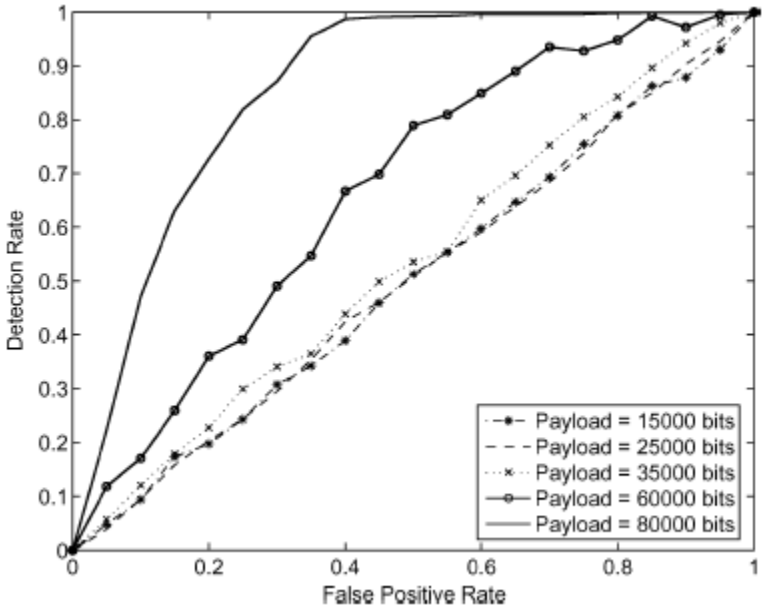

Figure13: ROC carves tested on different payloads

there is still no obvious detection effect. The detector does work only if the message length greatly exceeds the hiding capacity. In general case, the proposed steganography scheme can be considered undetectable in the situation of lower payloads than hiding capacity.

VII. CONCLUSION

In this study, a high-capacity steganographic scheme has been proposed for the JPEG2000 baseline system. The contributions of this work are mainly focused on dealing with two problems: bitstream truncation and redundancy measurement. The steganographic encoding procedure is explained to execute bit-plane encoding twice, whereas the rest parts, such as wavelet transform, quantization, rate-distortion optimization, bitstream organization, still are executed only once. Therefore, the computational complexity hasn't been increased too much.

REFERENCES

[1] C. C. Chang,Y. C. Chou, and T.D.Kieu, "High capacity data hiding for grayscale images," in Proc. 1st Int. Conf. Ubiquitou Information Management and Communication, Seoul, Korea, Feb. 2007, pp. 139–148.
[2] S.A.M.Gilani, I.Kostopoulos, andA.N. Skodras, "Color image-adaptive watermarking," in Proc. 14th Int. Conf. Digital Signal Processing, 2002, vol. 2, pp. 721- 724.
[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] J. Fridrich and M. Goljan, "Practical steganalysis of digital imagesState of the art," in Proc. SPIE, 2002, vol. 4675, pp. 1–13.
[5] JPEG2000 Part 1: Final Committee Draft Version 1.0, ISO/IEC. FCD 15444-1, 2000.
[6] JPEG2000 Part 2: Final Committee Draft, ISO/IEC FCD 15444-2,2000.
[7] A. Westfeld and A. Pfitzmann, "Attacks on steganographic systems,"in Lecture Notes in Computer Science. Berlin, Germany: Springer- Verlag, 2000, vol. 1768, pp. 61–75.
[8] H. Farid, "Detecting hidden messages using higher-order statistics models," in Proc. EEE Int. Conf. Image Processing, New York, 2002, pp. 905–908.
[9] T. Holotyak, J. Fridrich, and S. Voloshynovskiy, "Blind statistical steganalysis of additive steganography using wavelet higher order statistics," presented at the 9th IFIP TC-6 TC-11 Conf. Communications and Multimedia Security, 2005.