International Journal of Security and Its Applications
Vol.8, No.6 (2014), pp.211-224
http://dx.doi.org/10.14257/ijsia.2014.8.6.19

Steganography Technique for *JPEG*2000 Compressed Images Using Histogram in Wavelet Domain

Geeta Kasana[1], Kulbir Singh[2] and Satvinder Singh Bhatia[3]

[1]SMCA, [2]ECED, [3]SMCA
Thapar University, Patiala
INDIA-147004
gkasana@thapar.edu, ksingh@thapar.edu, ssbhatia@thapar.edu

Abstract

In this work, a steganography technique using histogram shifting for JPEG2000 compressed images is proposed. Histogram of the wavelet coefficients of each wavelet subband is calculated and shifted to embed secret image data. This embedding is performed on the peak wavelet coefficients during wavelet decomposition process of JPEG2000 encoder using Lifting scheme. Optimal Pixel Adjustment Process (OPAP) is performed on stego images to enrich their visual quality. The results given in this work show that proposed technique provide large embedding capacity and better visual quality of stego images than existing steganography techniques for JPEG2000 compressed images. Extracted secret image using proposed technique is similar to its original secret image.

Keywords: *PSNR, Histogram, Peak Points, JPEG2000, MSE*

1. Introduction

Steganography is an information hiding technique using which the secret data is hidden in a host medium like text, image, audio or video. In information hiding terminology, host media is termed as cover media and after hiding secret data, cover media is termed as stego media. Images are widely used as a cover media for steganography as they may have high redundancy. The purpose of steganography technique is to protect confidential and sensitive information when it is transmitted using a public network. Embedding capacity, security and robustness are main research targets for a steganography technique [11].

Steganography approaches can be classified into three main categories- spatial domain, frequency domain and compressed domain techniques. In spatial domain techniques, the pixels of an image are directly manipulated to hide the secret data ([2, 3, 8, 14, 23, 25, 28]). In frequency domain, the cover image is transformed using some transform like *DCT*, *DFT*, *DWT etc*. and then transformed coefficients are manipulated to embed the secret data ([9, 10, 16, 20]). In compressed domain techniques, the secret data is embedded in the compressed bit stream of a compression standard like *JPEG*, *JPEG*2000 *etc.*, ([4-7, 12, 17, 19, 21, 24, 26, 28, 29]). Due to their less complexity, spatial domain techniques are highly used in steganographic applications. However, these techniques are susceptible to statistical attacks. In contrast, transform and compressed domain techniques provide a higher level of security as they generally resist the statistical attacks since they hide the secret data more thoroughly.

Steganography techniques proposed for *JPEG*2000 compressed images are lossy and hence are not reversible in nature. Our main objective is to propose steganography technique for *JPEG*2000 compressed images which can provide the high embedding capacity and a good visual quality stego images. The proposed technique is based on observations that the

ISSN: 1738-9976 IJSIA

histogram of the wavelet coefficients can be shifted to produce redundant space and this redundant space can be used to hide secret data. Also, as less distortion is produced in frequency domain hiding techniques, so more data can be hidden in the frequency domain and more shifting can be performed in wavelet domain to hide large amounts of data. The key issues considered in proposed work are embedding capacity, visual quality of stego images, and lossless extraction of hidden data as in steganography techniques, the relationship between the embedding capacity and resulting stego images are more important [24].

This paper is organized as follows. In Section 2, overview of *JPEG*2000 standard and histogram based data hiding approach proposed by Ni *et al.*, is briefly discussed. In Section 3, the proposed steganography technique for *JPEG*2000 compressed images is described. The experimental results and comparison with existing steganography techniques is discussed in Section 4. The conclusion of the paper is discussed in Section 5.

2. Background

In this section, *JPEG*2000 standard, Lifting scheme, reversible data hiding scheme of Ni *et al.* and *OPAP* are discussed.

2.1. Overview of *JPEG*2000 Standard

*JPEG*2000 is the new wavelet based image and video compression standard [1] which provides excellent compression performance and novel features than JPEG standard. Steps used *JPEG*2000 encoder is illustrated in Figure 1.

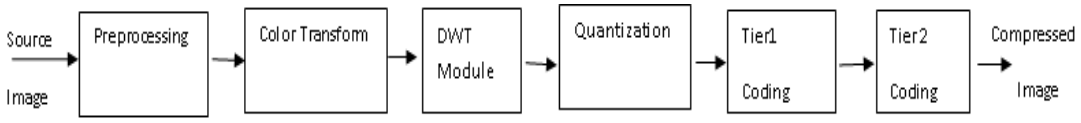
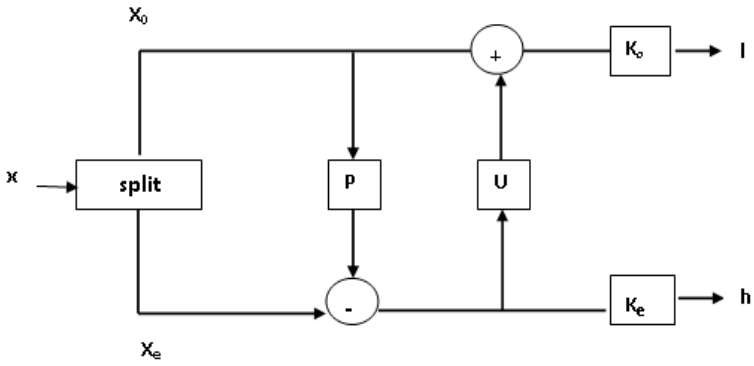


Figure 1. *JPEG*2000 Encoder

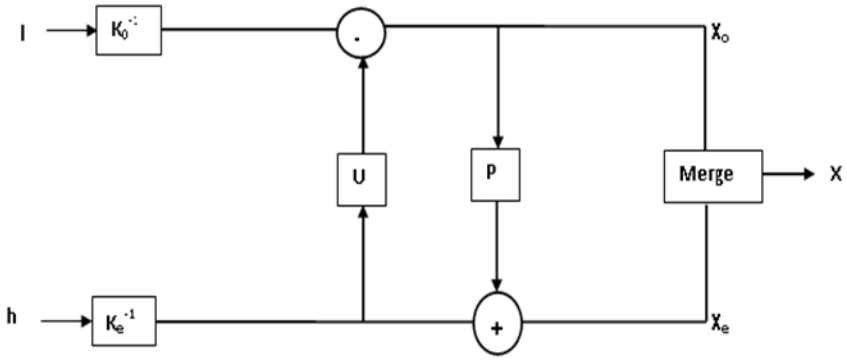
Firstly, the preprocessing is performed on the source image which is to be compressed using *JPEG*2000 encoder. The examples of preprocessing are tiling and shifting of the origin of the image pixels to 0 by subtracting 128 from its each pixel value. Shifting is performed to decrease the precision of the image pixels so that higher compression is achieved. Then irreversible or reversible color transform is performed on the preprocessed image to get the transformed image. After it, lossy or lossless discrete wavelet transform is applied to the transformed image to get its wavelet subbands. If the user requires lossy compression then *CDF* 9/7 wavelet filters are used. If the lossless compression is required then reversible *LeGall* 5/3 wavelet filters are used. Then the quantization is performed on the wavelet coefficients of a subband to decrease their precision. Quantization is required in case of lossy compression only. Quantized wavelet coefficients are partitioned into code blocks of equal size and *Tier*-1 coding is performed on each of the code blocks. Each code block is encoded using three passes which are significant propagation pass, refinement pass and cleanup pass. Post compression rate distortion optimization is performed in *Tier*-2 coding to discard the output of *Tier*-1 if number of bytes are more than required bytes in the bit stream. Then compressed bit stream is converted into packets and these packets are combined to produce the final compressed image in *JPEG*2000 format.

2.2. Lifting Scheme

Lifting scheme [22], also known as second generation wavelets, is an improved approach DWT in which the convolution operation is performed using wavelet filters. Lifting scheme is preferred because of its low computation cost and small memory space for storage. Basically the pixel direction estimation is done over here either horizontally or vertically as shown in Figure 2.



(a)



(b)

Figure 2. (a) Forward Lifting Scheme (b) Reverse Lifting Scheme

Let $\mathbf{X[m, n]}$ be a 2-*D* image data. Following steps are carried in a lifting scheme:

i) Splitting: In this step, the original data is divided into even and odd samples $X_e[2m, n]$ and $X_o[2m + 1, n]$

ii) Prediction: The odd samples are predicted from the even samples. The predictor P can be given as

$$\mathrm{P}(\mathrm{X_e})[\mathrm{m, n}] = \sum_{\mathrm{i}} \mathrm{p_i X_e}[\mathrm{m + i, n}]. \qquad (1)$$

where $\mathbf{p_i}$ are high pass filter coefficients. The prediction residual $\mathbf{z[m, n]}$ is computed as

$$z[m,n] = X_o[m,n] + P(X_e)[m,n]. \quad (2)$$

Now, the odd samples can be recovered by

$$X_o[m,n] = z[m,n] - P(X_e)[m,n]. \quad (3)$$

iii) Update: In this Lifting Step, the even samples $Xe[m,n]$ are updated based on the predicted odd samples $Xo[m,n]$ in the prediction step. The updater U is computed as

$$U(z)[m,n] = \sum_j u_j z[m+j,n]. \quad (4)$$

On the basis of which $x_e[m,n]$ is replaced with coarse approximation as given by

$$c[m,n] = X_e[m,n] + U(z)[m,n]. \quad (5)$$

iv) Normalization: The outputs of the lifting are normalized in this step. This step is basically performed to normalize the energy of scaling and wavelet functions.

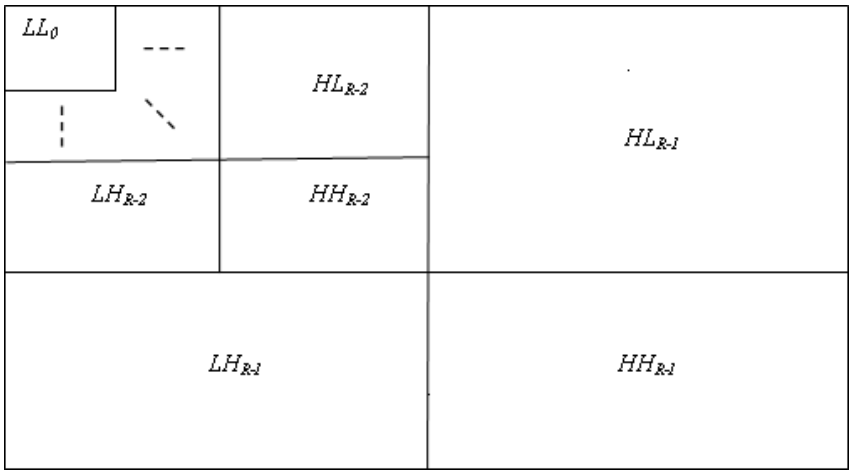


Figure 3. Lifting Scheme Structure

Four subbands are produced by one level lifting scheme which are horizontally low pass and vertically low pass (LL), horizontally low pass and vertically high pass (LH), horizontally high pass and vertically low pass (HL), and horizontally high pass and vertically high pass (HH). Wavelet decomposition of R − 1 level is associated with R resolution levels numbered from 0 to R − 1. At each resolution level (except the lowest), LL subband is further decomposed to obtain subbands at the next level. For example, LL_{R-1} subband is decomposed to obtain LL_{R-2}, LH_{R-2}, HL_{R-2}, and HH_{R-2} subbands. This process is repeated until LL_0 is obtained, as illustrated in Figure 3.

2.3. Reversible Data Hiding using Histogram

In data hiding technique, proposed by Ni, *et al.*, [18], the most frequently occurring pixel value is calculated from the histogram of the cover image, which is termed as peak value. Also, a pixel value which occurred minimum times in the histogram of the cover image, termed as the zero point, is determined. For example, the histogram of a grayscale Lena image, illustrated in Figure 4, has a peak point as 154 and zero point as 255. In this technique, all the grayscale values greater than the peak values are shifted one bin to the right or left, so that the bin just next or before to the peak value is now empty. Now, the image pixels are scanned in a sequential order. The secret data are added (or subtracted) to the peak pixel values occurring in the cover image. Thus, when the secret bit is a '1', the marked pixel will occupy the position just emptied. This technique not only embeds more data, but also recovers the original image without any distortion from the stego image. Embedding capacity in histogram based technique is directly proportional to the number of peak values occurring in the histogram of the cover image.

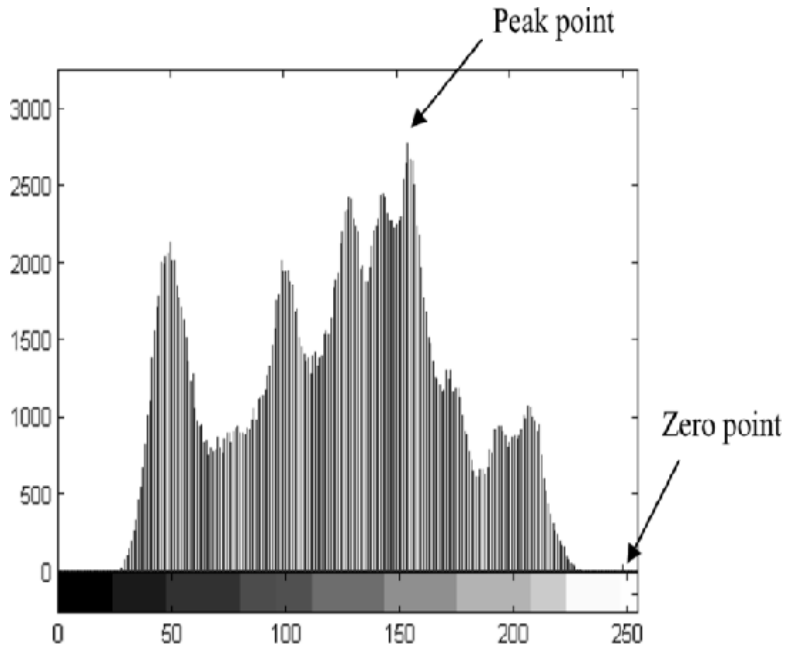


Figure 4. Histogram of Lena Image

2.4. OPAP

The proposed technique uses *OPAP* [3] to enhance the visual quality of the stego images. The main advantage of applying *OPAP* is to minimize the error between the cover image and stego image. *OPAP* is applied to modified $(k+1)^{th}$ bit of stego pixel value, if the modified version seems to give better results and thus contributing to a decrease in the *MSE* value. For example if decimal number 25 (binary equivalent 11001) is changed to decimal number 31 (11111) when three (k=3) Least Significant Bits (*LSB*) are replaced with secret data. The difference between original number and modified stego number is 6. This difference between the original value and stego pixel is called the embedding error. By inverting the k+1 (*i. e.* 4^{th}) bit, the binary number becomes 10111(binary number 23) and the embedding error between cover pixel value and modified stego pixel value is reduced to 2 and embedded secret bits are

also preserved. Hence *OPAP* depends on the difference $\delta(x,y)$ between cover value $C(x,y)$ and the modified value $S'(x,y)$.

Let δ be the embedding error between C and S' which is given by
$\delta(x,y) = S'(x,y) - C(x,y)$ where $-2^k < \delta < 2^k$
The value of S' is modified to the new value S'' as follows
Case 1: $(2^{k-1} < \delta(x,y) < 2^k \ and \ S'(x,y) \geq 2^k)$
$$S''(x,y) = S'(x,y) - 2^k$$
Case 2: $(2^{k-1} < \delta(x,y) < 2^k \ and \ S'(x,y) < 2^k)$
$$S''(x,y) = S'(x,y)$$
Case 3: $(-2^{k-1} < \delta(x,y) < 2^k)$
$$S''(x,y) = S'(x,y)$$
Case 4: $(-2^k < \delta(x,y) < -2^{k-1} \ and \ S'(x,y) \geq 256 - 2^k)$
$$S''(x,y) = S'(x,y)$$
Case 5: $(-2^k < \delta(x,y) < -2^{k-1} \ and \ S'(x,y) < 256 - 2^k)$
$$S''(x,y) = S'(x,y) + 2^k$$

By using *OPAP*, the absolute difference between the cover image pixel values and stego pixel values is limited to $0 \leq |S''(x,y) - C(x,y)| < 2^{k-1}$ so that the MSE between cover and stego images is reduced which enhances the visual quality of the stego image.

3. Proposed Steganography Technique

In this section, wavelet coefficients based steganography technique for JPEG2000 compressed images is discussed. This technique divides the wavelet coefficients of a cover image into subbands and finds the peak point wavelet coefficients having the maximum number of occurrences in the histogram of each subband of the cover image. These peak points are shifted to create the space into the secret data is hidden. Unlike Ni *et al*. method, shifting in wavelet coefficients are by$2^k - 1$, where *k* is the number of secret bits to be embedded into wavelet coefficients of subbands of the cover image. The proposed technique is based on the observation that less distortion occurs in frequency domain steganography techniques as compared to spatial domain techniques. Also, *OPAP* technique is well suited for the proposed technique as more than one bit is hidden into peak wavelet coefficients of the histogram of subbands and this increase the visual quality of stego images.

3.1. Embedding Algorithm

Step 1. Apply *DWT* using lifting scheme on the input image to get the subband B_i where i=1 to 3R+1, R is level of wavelet transform decomposition.

Step 2. For each subband B_i, perform the following steps:

a. Take Histogram H of the wavelet coefficients of subband B_i. Find the peak point p_0 and zero point's z_0.

b. Shifting each wavelet coefficient between zero point and peak point by$2^k - 1$, where k is the number of secret bits to be embedded in peak wavelet coefficients, as shown in Figures 5 and 6.

If $p_0 < z_0$

$$B_i(u,v) = B_i(u,v) + 2^k - 1 \quad \text{for } p_0 < B_i(u,v) < z_0$$

else

$B_i(u,v) = B_i(u,v) - 2^k + 1$ for $p_0 > B_i(u,v) > z_0$

End if

where u and v are the index of peak wavelet coefficients of a subband.

c. Modify the peak points of subband B_i using the following condition:

If $p_0 < z_0$

$B_i(u,v) = B_i(u,v) + S_k$ for $p_0 < B_i(u,v) < z_0$

else

$B_i(u,v) = B_i(u,v) - S_k$ for $p_0 > B_i(u,v) > z_0$

End if

where S_k is the value of k secret bits.

Step 3. Execute other remaining process of *JPEG*2000, as shown in Figure 1, to compress the input image in *JPEG*2000 format and to get stego image.

Step 4. Apply *OPAP* on the stego image to improve its visual quality.

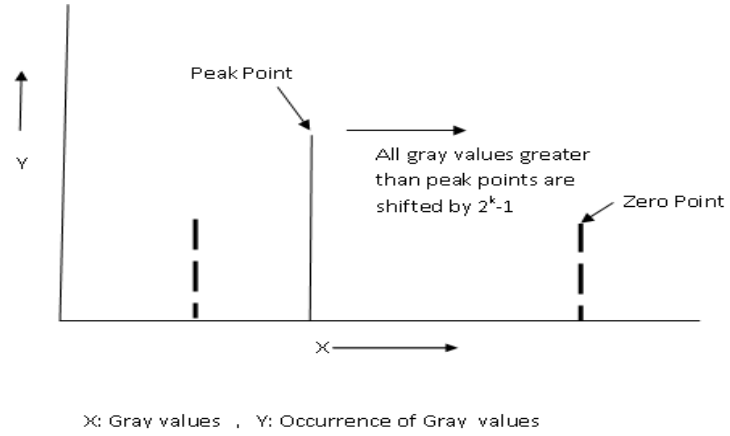


Figure 5. Histogram Shifting when Peak Point is Less than Zero Point

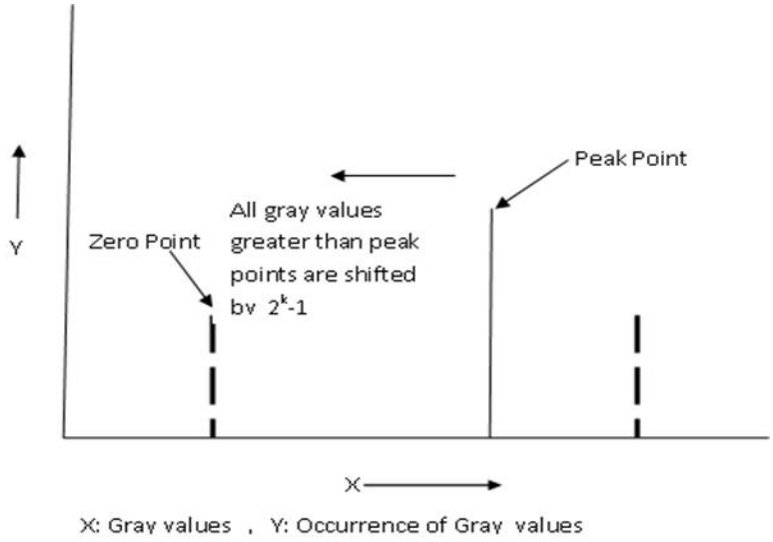


Figure 6. Histogram Shifting when Peak Point is Greater than Zero Point

Extraction process of the proposed technique is just the reverse of the embedding process. Also, value of peak points of each subbands are transmitted to the receiver side as a key.

4. Experimental Results

To implement the proposed steganography technique, *JASPER* software tool [15] is modified. Cover images considered in this work are uncompressed Lena, Barbara, Boat, Baboon, Bridge, Airplane, Couple and Crowd, Pepper which are easily available in the literature and are used by the researcher in the image processing domain as shown in Figure 7(a) to (d). All these cover images are of size 512×512. Their corresponding stego images are shown in Figure 7(e) to (f). *PSNR* is used as a parameter to measure visual quality between the cover and its corresponding stego image and is defined by:

$$PSNR = 10log_{10}\frac{255^2}{MSE}$$

$$MSE = \sum_{m=1}^{M}\sum_{n=1}^{N}\frac{(Y(m,n) - X(m,n))^2}{M \times N}$$

where $Y(m,n)$ is the pixel of stego image and $X(m,n)$ is the pixel of cover image, M and N is the height and width of the images, respectively.

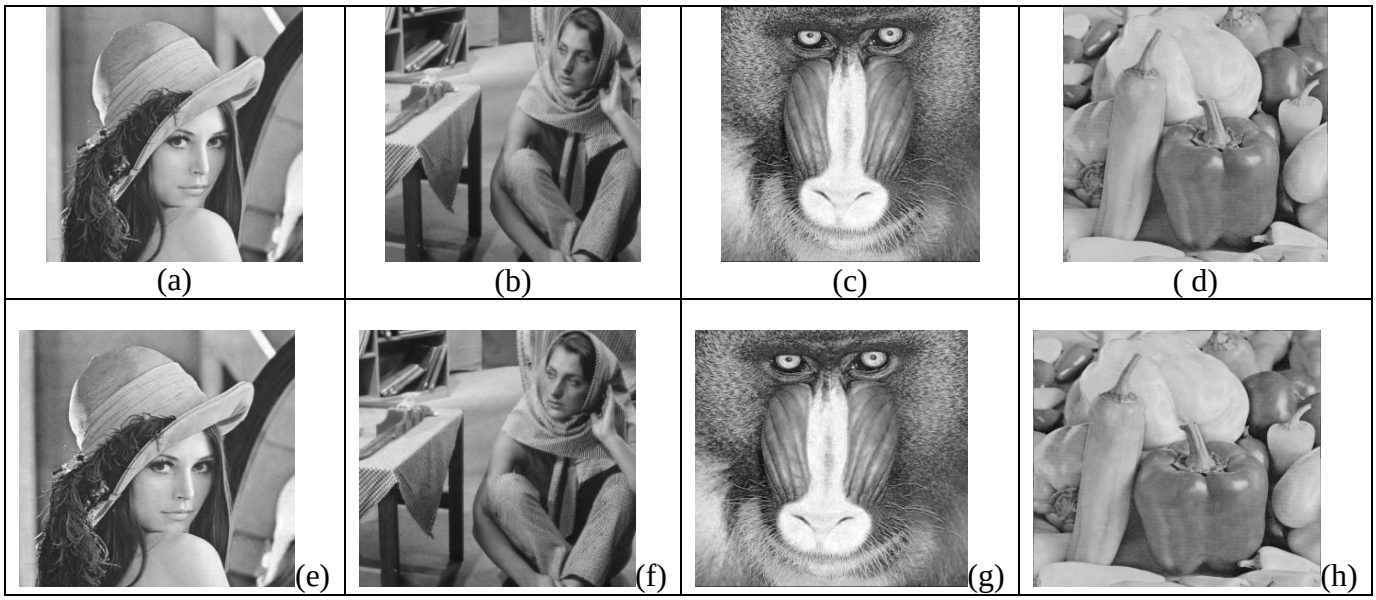


Figure 7. (a) to (d) Cover image of Lena, Barbara, Baboon and Pepper. (e) to (h) stego images of Lena, Barbara, Baboon and Pepper

Secret data is embedded after *DWT* decomposition process of *JPEG*2000 lossless encoder using proposed technique. *PSNR* between the cover and stego images without and with *OPAP* are shown in Tables 1, 2 and 3 for different values of *k*, where *k* is number of secret bits embedded into peak wavelet coefficients of subbands of the cover image.

Table 1. PSNR (in dB) of Different Stego Images for k=1 (Embedding Capacity= 32768 Bits)

Image	*PSNR* between cover and stego image without *OPAP*	*PSNR* between cover and stego image with *OPAP*
Boat	43.71	43.71
Bridge	43.55	43.55
Lena	43.39	43.39
Barbara	43.81	43.81
Baboon	43.53	43.53
Airplane	43.12	43.12
Couple	43.04	43.04
Crowd	43.28	43.28

Table 2. PSNR (in dB) of Different Stego Images for k=2(Embedding Capacity= 65536 Bits)

Image	*PSNR* between cover and stego image without *OPAP*	*PSNR* between cover and stego image with *OPAP*
Boat	41.70	42.91
Bridge	41.54	42.85
Lena	41.42	42.89
Barbara	41.80	42.98
Baboon	41.53	43.33
Airplane	41.09	42.29
Couple	41.05	42.54
Crowd	41.27	42.78

Table 3. PSNR (In Db) Of Different Stego Images for k=3(Embedding Capacity= 98304 Bits)

Image	*PSNR* between cover and stego image without *OPAP*	*PSNR* between cover and stego image with *OPAP*
Boat	39.66	41.59
Bridge	39.65	41.53
Lena	39.43	41.39
Barbara	39.92	41.81
Baboon	39.56	41.53
Airplane	39.21	41.09
Couple	39.15	41.04
Crowd	39.38	41.24

From these Tables, one can observe that *PSNR* between cover images and stego images decreases as the value of *k* is increased but it is highly acceptable by the human visual system as upto k=*3*, *PSNR* is around 40 dB [13]. Also, when *OPAP* is blended with the proposed technique, there is maximum 2 dB improvement in *PSNR* of stego images.

The proposed technique is compared with the existing steganography techniques for *JPEG*2000 images and this comparison is shown in Table 4. In this comparison, embedding capacity is considered as an effective parameter, as *PSNR* comparison is not considered in existing steganography techniques.

Table 4. Embedding Capacity (in Bits) Comparison of Proposed Technique with Existing Techniques

Image	Noda *et al.* [19]	Su *et al*. [24]	Zhang *et al*.[29]	Proposed Technique	
Boat	58656	16384	14000	*k*=1	32768
				k=2	65536
				k=3	98304
Lena	58656	16384	14000	*k*=1	32768
				k=2	65536
				k=3	98304
Pepper	58656	16384	14000	*k*=1	32768
				k=2	65536
				k=3	98304
Baboon	58656	16384	19500	*k*=1	32768
				k=2	65536
				k=3	98304

From this Table, one can infer that maximum embedding capacity of Noda *et al*. is 58656 bits; Su, *et al.*, is 16384 bits; Zhang, *et al.*, is 19500 bits while maximum embedding capacity of the proposed technique is 32768 bits when k = 1; 65536 bits when k = 2 and 98304 bits when k =3. Capacity of Noda, *et al.*, is effective but it increases the size of stego images, hence it is easily detectable. Capacity of Su, *et al*., and Zhang, *et al*., is very less as compared to the capacity of the proposed technique. Hence proposed technique shows a high performance, as evidenced by comparison table.

5. Steganalysis Test

In this test, wavelet subbands characteristics are used for detecting hidden message in images. For this, 1100 gray scale images are considered with resolution of 512×512. We randomly choose 750 original images and correspondingly 750 stego images for calculating the projection vector of Fisher Linear Discriminator (*FLD*) classifier. The remaining 350 original cover images and corresponding stego images are used for testing purpose. These images are decomposed using wavelet transform on 5 levels and then compute the mean, variance, skewness and kurtosis of each the wavelet subband. On the basis of these statistical characteristics, Receiver Operating Characteristics (*ROC*) curves are drawn and shown in Figures. 8.

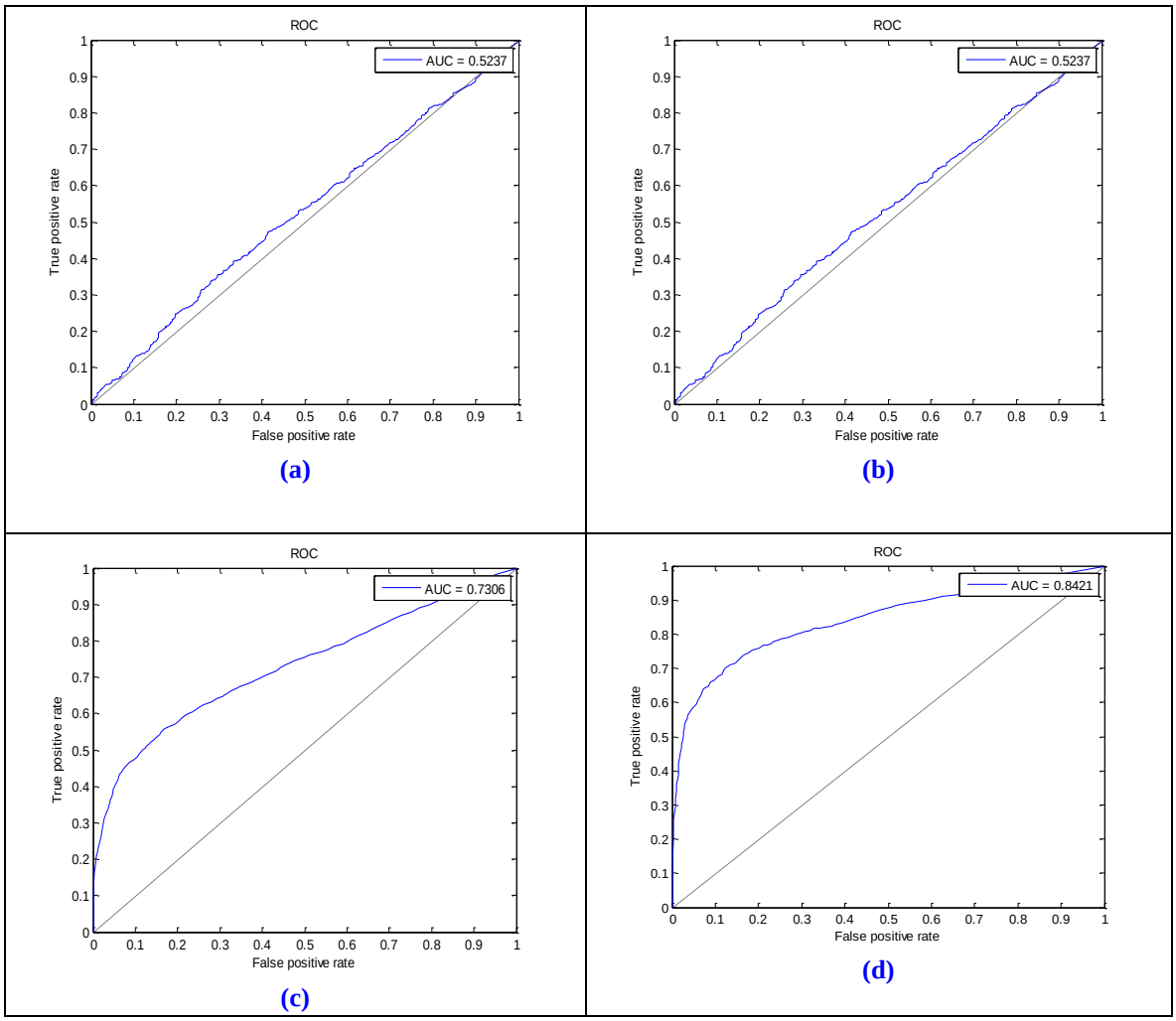


Figure 8. ROC Curve for Different Embedding Capacities (a) 32768 Bits (b) 65536 Bits (c) 100000 Bits (d) 150000 Bits

Figures 8(a)-8(d) show *ROC* curves of the test images different capacities: 32768 bits, 65536 bits, 100000 bits and 150000 bits. From this one can observe that the detector is in vain when the embedding capacity is 100000 bits. And when the embedding capacity is increased to 150000 bits or above, the detector may able to detect the presence of hidden data. So the proposed technique is undetectable when the embedding capacity is very high as compared to the existing steganography techniques for *JPEG*2000 compressed images.

6. Conclusion

In this work, a steganography technique for *JPEG*2000 compressed images is proposed. Histogram of wavelet subabnds of the cover image is taken and then shifting of the wavelet coefficients is performed to create spaces to hide the secret data. Only the peak wavelet coefficients values of subbands are transmitted to the receiver as key. Using these peak wavelet coefficients, hidden secret data is extracted. Using proposed technique, hidden secret is extracted without any loss and the original cover image is also same. Comparison with existing techniques shows the effectiveness of the proposed technique.

References

[1] ISO/IEC 15444-1, Information Technology – JPEG2000 Image Coding System – Part 1: Core Coding System, **(2001)**.
[2] B. E. Carvajal-Gamez, F. J. Gallegos-Funes and A. J. Rosales-Silva, "Color local complexity estimation based steganographic method", Expert Systems with Applications, vol. 40, no. 4, **(2013),** pp. 1132–1142.
[3] C. K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution", Pattern Recognition, vol. 37, no. 3, **(2004),** pp. 469–474.
[4] C. C. Chang, W. L. Tai and C. C. Lin, "A reversible data hiding scheme based on side match vector quantization", IEEE Transactions on Circuits and Systems for Video Technology, vol. 16, no. 10, **(2006),** pp. 1301–1308.
[5] C. C. Chang, "Reversible hiding in DCT-based compressed images", Information Sciences, vol. 177, no. 13, **(2007),** pp. 2768–2786.
[6] C. C. Chang, W. C. Wu and Y. C. Hu, "Lossless recovery of a VQ index table with embedded secret data", Journal of Visual Communication and Image Representation, vol. 18, no. 3, **(2007),** pp. 207–216.
[7] C. C Chang, T. S. Nguyen and C. C. Lin, "A reversible data hiding scheme for VQ indices using locally adaptive coding", Journal of Visual Communication and Image Representation, vol. 22, no. 7, **(2011)**, pp. 664–672.
[8] W. J Chen, C. C. Chang and T. Le, "High payload steganography mechanism using hybrid edge detector", Expert Systems with Applications, vol. 37, no. 4, **(2010),** pp. 3292–3301.
[9] W. Y. Chen, "Color image steganography scheme using DFT, SPIHT codec, and modified differential phase-shift keying techniques", Applied Mathematics and Computation, vol. 196, no. 1, **(2008),** pp. 40–54.
[10] R. Chu, X. You, X. Kong and X. Ba, "A DCT-based image steganographic method resisting statistical attacks", Proceedings of IEEE international conference on acoustics, speech, and signal processing, **(2004)** May 17-21, Montreal, Canada.
[11] I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich and T. Kalker, "Digital Watermarking and Steganography", 2nd Ed., Burlington, MA: Morgan Kaufmann, **(2008)**.
[12] G. Hai-Ying, X. Yin and L. Guo-Qiang, "A steganographic algorithm for JPEG2000 images", IEEE computer society, Int. Conf. on Computer Science and Software Engineering, **(2008),** pp. 1263-1266.
[13] M. S. Hsieh, "A robust image authentication method based on wavelet transform and Teager energy operator", International Journal of Multimedia and its Applications, vol. 2, no. 3, **(2010),** pp. 1-17.
[14] A. Ioannidou, S. T. Halkidis and G. Stephanides, "A novel technique for image steganography based on a high payload method and edge detection", Expert Systems with Applications, vol. 39, no. 14, **(2012),** pp. 11517–11524.
[15] "JasPer software", www.ece.uvic.ca/~frodo/jasper/.
[16] R. Jafari, D. Ziou and M. M. Rashidi, "Increasing image compression rate using steganography", Expert Systems with Applications, vol. 40, no. 17, **(2013),** pp. 6918–6927.
[17] H. L. Jin, M. Fujiyoshi, Y. Sheki and H. Kiya, "A Data Hiding Method for JPEG2000 Coded Images Using Module Arithmetic", Electronics and Communications in Japan, vol. 90, no. 7, **(2007),** pp. 37-45.
[18] Z. Ni, Y. Q. Shi, N. Ansari and W. Su, "Reversible data hiding", IEEE Transactions on Circuits Systems and Video Technology, vol. 16, no. 3, **(2006),** pp. 354–362.
[19] H. Noda, J. Spaulding, M. N. Shirazi and E. Kawaguchi, "Application of bit plane decomposition steganography to JPEG2000 encoded images", IEEE Signal Processing Letters, vol. 9, no. 12, **(2002),** pp. 410-413.
[20] H. Noda, M. Niimi and E. Kawaguchi, "High-performance JPEG steganography using quantization index modulation in DCT domain", Pattern Recognition Letters, vol. 27, no. 5, **(2006),** pp. 455–461.
[21] S. Ohyama, M. Niimi, K. Yamawaki and H. Noda, "Lossless data hiding using bit-depth embedding JPEG 2000 compressed bit-stream", Journal of Communication and Computer, vol. 6, no. 2, **(2009),** pp. 35-39.
[22] W. Sweldens, "The lifting scheme: a custom-design construction of second generation wavelets", SIAM Journal of Mathematical Analysis, vol. 29, **(1997),** pp. 511-546.
[23] H. Sajedi and M. Jamzad, "Boosted steganography scheme with cover image preprocessing", Expert Systems with Applications, vol. 37, no. 12, **(2010),** pp. 7703–7710.
[24] P. C. Su and J. Kuo, "Steganography in JPEG2000 compressed images", IEEE Transactions on Consumer Electronics, vol. 49, no. 4, **(2003),** pp. 824-832.
[25] D. C. Wu and W. H. Tsai, "A steganographic method for images by pixel-value differencing", Pattern Recognition Letters, vol. 24, no. 9, **(2003),** pp. 1613–1626.
[26] C. H. Yang, "Reversible steganography based on side match and hit pattern for VQ-compressed images", Information Sciences, vol. 181, no. 11, **(2011),** pp. 2218–2230.
[27] C. H. Yang, "Adaptive data hiding in edge areas of images with spatial LSB domain systems", IEEE Transactions on Information Forensics and Security, vol. 3, no. 3, **(2008),** pp. 488–497.

[28] C. H. Yang, "Reversible steganography based on side match and hit pattern for VQ-compressed images", Information Sciences, vol. 181, no. 11, **(2011),** pp. 2218–2230.
[29] L. Zhang, H. Wang and R. Wu, "A high capacity steganography scheme for JPEG2000 baseline system", IEEE Transactions on Image Processing, vol. 18, no. 8, **(2009),** pp. 1797-1803.