International Journal of Science and Engineering (IJSE)

Home page: http://ejournal.undip.ac.id/index.php/ijse

Bit Plane Coding based Steganography Technique for *JPEG* 2000 Images and Videos

Geeta Kasana[1], Kulbir Singh[2], Satvinder Singh Bhatia[3]
[1]Department of Computer Science and Engineering Department, Thapar University, Patiala, INDIA
[2]Department of Electronics and Communication Engineering, Thapar University, Patiala, INDIA
[3]School of Mathematics, Thapar University, Patiala, INDIA
e-mail: gkasana@thapar.edu

Abstract:In this paper, a Bit Plane Coding (*BPC*) based steganography technique for *JPEG*2000 images and Motion *JPEG*2000 video is proposed. Embedding in this technique is performedin the lowest significant bit planes of the wavelet coefficients of a cover image. In *JPEG*2000 standard, the number of bit planes of wavelet coefficients to be used in encoding is dependent on the compression rate and are used in *Tier*-2 process of *JPEG*2000. In the proposed technique, *Tier*-1 and *Tier*-2 processes of *JPEG*2000 and Motion *JPEG*2000 are executed twice on the encoder side to collect the information about the lowest bit planes of all code blocks of a cover image, whichis utilized in embedding and transmitted to the decoder.After embedding secret data, Optimal Pixel Adjustment Process (*OPAP*) is applied on stego images to enhanceits visual quality.Experimental results show that proposed technique provides large embedding capacity and better visual quality of stegoimages than existing steganography techniques for *JPEG*2000 compressed images and videos.Extracted secret image is similar to the original secret image.

Keywords:*BPC, Code block, HVS, PSNR, JPEG2000, MSE, OPAP,SIM.*

Submission: November 14, 2015 Corrected : January 5, 2016 Accepted: January 9, 2016

Doi: http//dx.doi.org/10.12777/ijse.10.1.21-29
[**How to cite this article**: Kasana, G., Singh, K., Bhatia, S.S. (2016). Bit Plane Coding based Steganography Technique for *JPEG* 2000 Images and Videos*, International Journal of Science and Enginering*, 10(1), 21-29. Doi: http//dx.doi.org/10.12777/ijse.10.1.21-29

I. INTRODUCTION

Steganography is a technique of hiding secret data in a host medium like text, image, audio or video. Host media are termed as cover media and after hiding secret data, cover media are termed as stego media. The main objective of a steganography technique is to hide the large amount of secret data into a cover media to protect from the unauthorized users when it is transmitted using a public network. Hiding capacity, security and robustness are three main research targets for a steganography technique (Sencar *et al*., 2004). Steganography approaches can be divided into three categories- spatial domain, frequency domain and compressed domain techniques. In spatial domain techniques, the pixel values of the cover image are directly manipulated to hide the secret data(Chan *et al*., 2004; Chen *et al*., 2010; Ioannidou *et al*., 2012; Carvajal*et al*., 2013). In frequency domain, the cover image is transformed using some transform like Discrete Cosine Transform *(DCT*), Discrete Fourier Transform(*DFT*), Discrete Wavelet Transform(*DWT*) *etc*. and the secret data is embedded into the transformed coefficients(Chen, 2008; Chu *et al*., 2004; Goudia *et al*., 2011; Jafari *et al.,* 2013; Noda *et al*., 2006).In compressed domain techniques, the secret data is embedded into compressed output of a compression standard like *JPEG*, *JPEG* 2000 *etc.* (Chang *et al.,* 2006; Chang *et al.,* 2007;Chang *et al.,* 2011;Hai-ying *et al.*, 2008; Ishida *et al*., 2008; Ishida *et al*., 2009; Jin *et al.,* 2007;Ohyama*et al.* 2008; Ramkumar and Akansu, 2001; Suand Kuo, 2003;Yang *et al.,* 2011; Zhang *et al.,* 2009). Steganography techniques of all these categories have different specifications. Spatial domain techniques are widely used for steganographic applications as they provide high embedding capacity and have less complexity. However, these techniques are vulnerable to statistical analysis. Transform and compressed domain steganographic techniques possess a higher level of security as they generally resist the aforementioned steganalytic methods since they hide the secret information more thoroughly in a stego image. All steganography techniques must focus on three issues- where to hide secret data, how safe is

the embedding and how secure is the payload in case of exposure to an adversary. Each of the existing steganography technique addresses these issues differently.

In this work, the objective is to propose asteganographic technique for *JPEG*2000 images and Motion *JPEG*2000 videos at low bit rate which can provide the high embedding capacity and a good visual quality stego images.It is based on the observations some bit planes of wavelet coefficient are discarded in *Tier*-2 process of *JPEG*2000 standard and it is decided on the basis of the compression rate given by the user. If high compression rate is required by the user, thenlarge numbers of bit planes of a code block are discarded as compared to the numbers of bit planes discarded at low compression rate. Also, as less distortion is produced in frequency domain hiding techniques, so more data can be hidden in the frequency domain. The key issues considered in proposed work are embedding capacity, visual quality of stego images, and lossless extraction of hidden data as in steganographic techniques, the relationship between the embedding capacity and resulting stego images are more important (Suand Kuo, 2003;).

This paper is organized as follows. In Section 2, overview of *JPEG*2000 standard and *OPAP* are discussed. In Section 3, the proposed steganography technique for *JPEG*2000 compressed images is described. The experimental results and comparison with existingsteganography techniques are discussed in Section 4. Steganalysis test of the proposed steganography technique is discussed in Section5. Conclusion of the paper isgiven in Section 6.

II. BACKGROUND

In this section, processes used in *JPEG*2000 standard and *OPAP* are discussed.

Overview of *JPEG*2000 Standard

*JPEG*2000 is the new state-of-art image and video coding standard (Aacharyaand Tsai, 2005). It has an excellent coding performance and novel features such as superior low bit rate compression performance, lossless and lossy compression, progressive transmission, region of interest coding, error resilience and random code stream access etc. *JPEG*2000 encoder is illustrated in Figure 1.

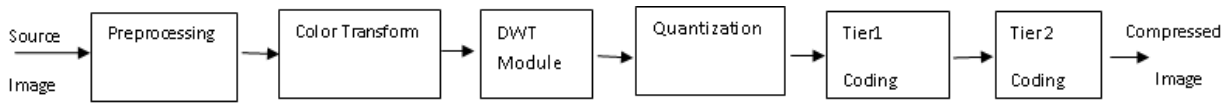

Figure 1. *JPEG*2000 Encoder

Firstly, the preprocessing is performed on the source image/ video frame 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 applied to the preprocessed image to get the transformed image. After it, lossy or lossless discrete wavelet transform is applied to the transformed image to get the wavelet subbands. If the lossy compression is required 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 to decrease theirprecision. Quantization is required in case of lossy image compression only. Quantized wavelet coefficients are partitioned into code blocks 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.*Tier*-2 coding in which post compression rate distortion optimization is applied. The compressed data are converted into packets and these packets are combined to produce the final compressed image in *JPEG*2000 format.

If the precision of the wavelet coefficients in the code blocks is *p*, then the code block is decomposed into p bit planes and these are sequentially encoded from the most significant bit plane to the least significant bit plane. Each bit plane is first encoded by a fractional *BPC* process to generate intermediate data in the form of a context and a binary decision value for each bit position. Embedded Block Coding with Optimized Truncation (*EBCOT*) has been adopted for *BPC*. *EBCOT* encodes each bit plane in three coding passes, with a part of a bit plane being coded in each coding pass without any overlapping with the other two coding passes. Due to this reason, *BPC* is called fractional bit plane coding. The three coding passes in the order in which they are performed on each bit plane are Significant Propagation Pass (*SPP*), Magnitude Refinement Pass (*MRP*) and Cleanup Pass (*CUP*). In *SPP*, a bit is encoded if its location is not significant, but at least one of its eight-connected neighbors is significant. In *MRP*, all bits from locations that became significant in a previous bit plane are encoded. The *CUP* pass takes care of the bits of a bit plane which are not encoded in the first two passes. Bit planes which are encoded by *EBCOT* are termed as significant bit planes in this work. Numbers of significant bit planes are dependent on the compression rate specified by the user. If compression rate is higher than the significant

bit planes are higher than the significant bit planes required by the lower bit planes.

In *JPEG*2000 encoder, *Tier*-1 is followed by *Tier*-2 encoding. The input to the *Tier*-2 encoding process is the set of bit plane coding passes of each code block generated during *Tier*-1 encoding. In *Tier*-2 encoding, the coding pass information is packaged into data units called packets, in a process referred to as packetization. Packets from all subbands are then collected in so-called layers. The way the packets are built up from the code block coding passes, and thus which packets a layer will contain, is not defined by the *JPEG*2000 standard, but in general a coder tries to build layers in such a way that the image quality will increase monotonically with each layer, and the image distortion will shrink from layer to layer. Thus, layers define the progression by image quality within the code stream of a compressed image.

OPAP

The proposed steganography technique uses *OPAP*(Chan and Cheng, 2004) to enhance the distortion introduced due to embedding of the secret data. Any significant change in the value will produce different value of *k*(number of bits that can hide) to be calculated to the receiver. The main idea of applying *OPAP* is to minimize the error between the cover image and stego image. *OPAP* is applied where $(k+1)^{th}$ bit of every pixel is modified, if the modified version seems to give better results and thus contributing to a decrease in the *MSE* value. For example if binary number 11001(decimal number 25) is changed to 11111(decimal number to 31) because three Least Significant Bits (*LSB*) were replaced with embedded data. The difference from the original number is 6. This difference in the original value is called the embedding error. By adjusting the 4^{th} bit from a value 1 to value 0, the binary number becomes 10111(binary number 23) and the embedding error reduced to 2 while at the same time preserving the value of the three embedded bits. The algorithm depends on calculating 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'.

$\delta(x,y) = S'(x,y) - C(x,y)$where $-2^k < \delta < 2^k$

The value of S' is then changed to the new gray value S'' as follows

Case1:

$(2^{k-1} < \delta(x,y) < 2^k \ \ and \ \ S'(x,y) \geq 2^k)$

$S''(x,y) = S'(x,y) - 2^k$

Case2:

$(2^{k-1} < \delta(x,y) < 2^k \ \ and \ \ S'(x,y) < 2^k)$

$S''(x,y) = S'(x,y)$

Case3: $(-2^{k-1} < \delta(x,y) < 2^k)$

$S''(x,y) = S'(x,y)$

Case4:

$(-2^k < \delta(x,y) < -2^{k-1} \ \ and \ \ S'(x,y) \geq 256 - 2^k)$

$S''(x,y) = S'(x,y)$

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 employing *OPAP*, the absolute embedding error between pixels in the cover image and the stego image is limited to $0 \leq |S''(x,y) - C(x,y)| < 2^{k-1}$ so that the quality of the stego image is enhanced.

III. PROPOSED STEGANOGRAPHY TECHNIQUE

In this section, *BPC* based steganography technique for *JPEG*2000 compressed imagesis discussed. As discussed in section above, *JPEG*2000 compressed image is obtained after *Tier*-2 encoding. *Tier*-2 encoding discards the passes encoded in *Tier*-1 on the basis of the compression rate specified by the user. If compression rate is low, a large number of passes are discarded by *Tier*-2 to produce a compressed image of the required compression rate. The proposed technique is based on the principle that if information about the passes which are to be retained by *Tier*-2 is known then secret data can be hidden in those passes of a particular subband which are to be retained in the final compressed bit stream. Soto get information about these passes,*Tier*-1 and *Tier*-2 decoding are executed on the encoder side. On the basis of this side information, secret data is embedded into those passes and then *Tier*-1 and *Tier*-2 encoding are again executed to produce the final stego 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 proposedtechnique as more than one bitis hidden into eligible wavelet coefficients and this increase the visual quality of stego images.

EmbeddingAlgorithm

Step1. Execute *Tier*-2 and *Tier*-1 decoding after generation of bit stream to get the wavelet coefficients of code blocks of a subband.

Step 2. For each code blockCB_i, perform the following steps:

a. Embed secret data into lowest *k* bit planes using LSB replacement.

b. Apply *OPAP* process on the code blocks CB_i.

Step 3.Execute other remaining process of *JPEG*2000, as shown in Figure 2, to compress the input image in *JPEG*2000 format and to get stego image.

Extraction process of the proposed technique is just the reverse of the embedding process.

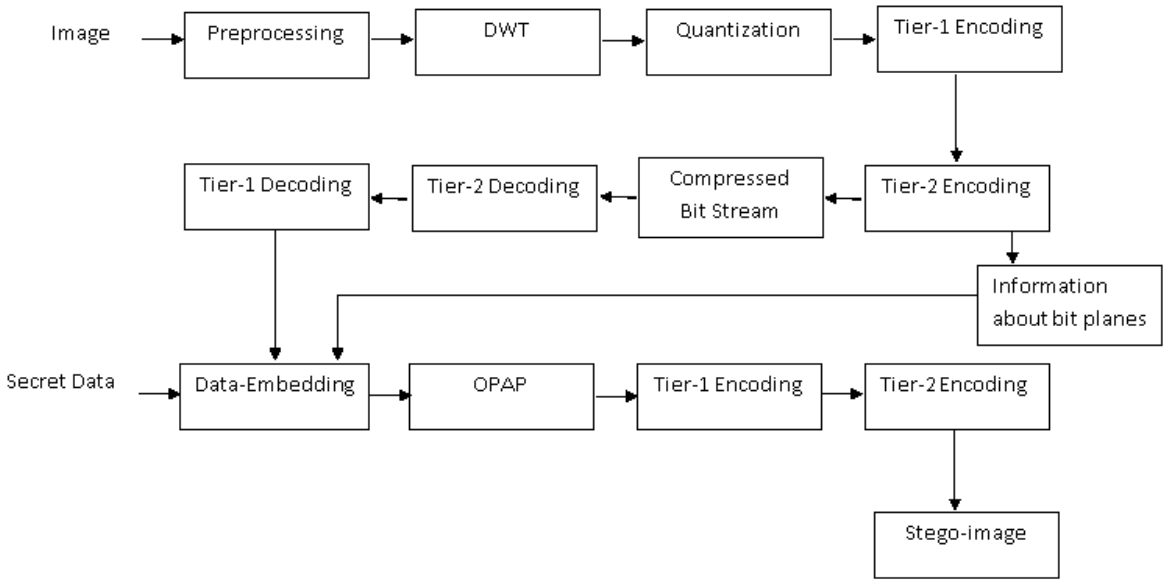

Figure 2. Flowchart of proposed technique using BPC

IV. EXPERIMENTAL RESULTS

To implement the proposed steganography technique, *KAKADU* software tool is modified. Cover images considered in this work are uncompressed Lena, Barbara, Baboon, Pepper, Bike, Woman and Crowd, GoldHill and Boat, few of them are shown in Figure 3(a) to 3(d). These cover images are of size 512×512. Their corresponding stego images are shown in Figure 3(e) to 3(h). *PSNR* is fidelity criteria tomeasure the distortion in the stego image and is given by:

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

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

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.

Similarity Index Modulation (*SIM*) between original secret image and recovered secret image is also evaluated, which is defined by

$$SIM = \frac{\sum_m \sum_n W(m,n) \times W'(m,n)}{\sum_m \sum_n [W(m,n)]^2}$$

It is used to evaluate the quality of the recovered secret data by measuring the similarity between the original secret image$W$ and the extracted secret image W'.

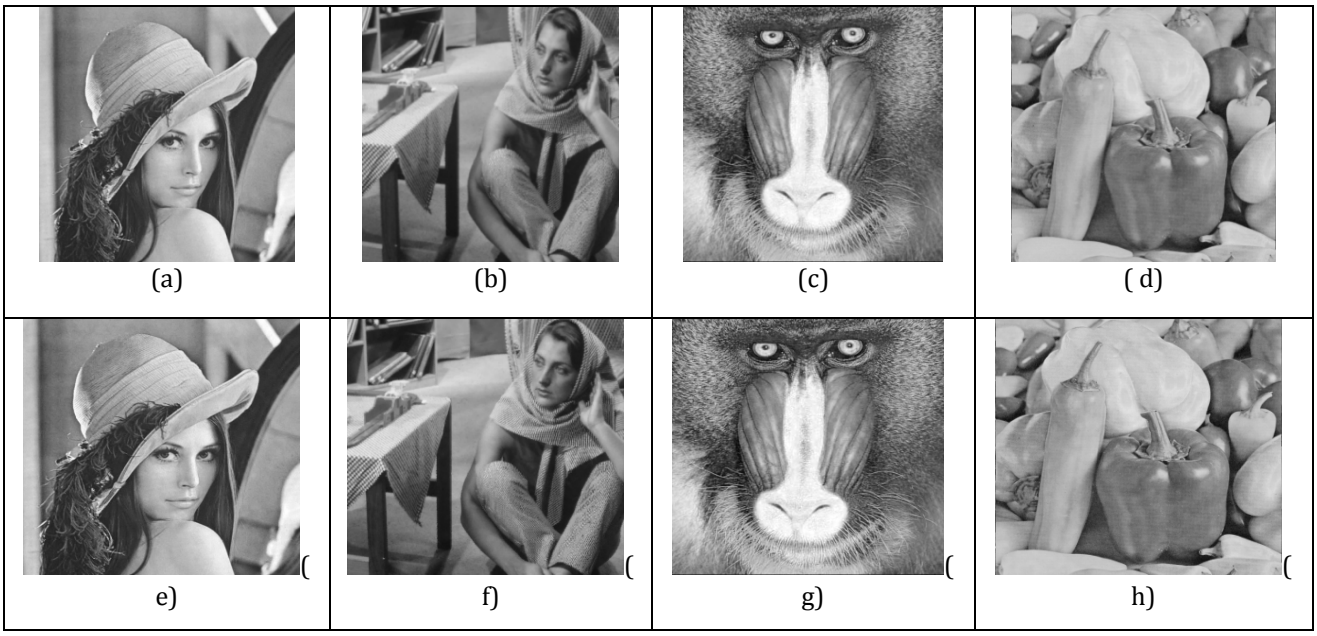

Figure 3. (a) to (d) Cover images of Lena, Barbara, Baboon and Pepper. **(e) to (h)**stego images of Lena, Barbara, Baboon and Pepper

PSNR and PSNR-HVS of different imagesat a different compression rate, without embedding any secret data, are shown in Table 1. Secret data is embedded after *DWT* decomposition process of *JPEG*2000 encoder using proposed technique. *PSNR* and *PSNR-HVS* between cover and stego images with *OPAP* at different compression rates in bit per pixels (*bpp*) are shown in Table 2.

Table 1. *PSNR* (in *d*B) and *PSNR-HVS* (in *d*B) of different cover images at different bit rates without embedding any payload

Image	Rate(in bpp)							
	0.250		0.50		1.00		2.00	
	PSNR	*PSNR-HVS*	*PSNR*	*PSNR-HVS*	*PSNR*	*PSNR-HVS*	*PSNR*	*PSNR-HVS*
Lena	33.22	36.19	36.45	39.36	39.51	42.45	45.12	48.25
Barbara	27.38	32.13	30.95	36.5	36.04	40.20	40.54	44.15
Baboon	22.87	25.15	25.17	27.32	28.62	32.37	34.73	38.12
Boat	29.89	30.94	33.21	36.48	36.66	39.85	41.91	46.74
GoldHill	30.54	32.06	33.25	35.45	36.60	39.96	39.76	42.47
Bike	29.06	31.65	33.09	35.70	37.73	40.12	41.26	44.62
Woman	29.24	31.34	33.00	35.98	37.96	40.10	40.53	42.75
Pepper	32.32	34.81	35.89	38.07	40.60	42.86	45.59	47.91

Table 2.*PSNR* (in dB)/ *PSNR-HVS* (in dB) between different cover and stego images at different compression rates and embedding capacity using proposed Technique

Embedding Capacity	Rate(in bpp)			
	0.250	0.50	1.00	2.00
		Lena		
1024	31.27/32.18	33.48/34.25	36.76/37.65	42.05/43.21
2048	30.39/32.01	32.78/33.80	35.23/37.01	41.87/42.25
4096	30.12/31.96	31.77/33.04	35.05/36.73	41.23/42.06
8192	29.86/31.61	31.47/32.13	34.66/36.03	39.02/41.32
16384	29.43/31.25	30.23/31.47	33.21/35.89	38.35/41.02
32768	28.92/30.90	28.76/29.25	31.25/33.26	36.40/39.75
		Barbara		
1024	24.48/26.83	26.35/33.23	33.54/36.56	37.95/40.25
2048	24.08/26.54	26.12/33.15	32.91/36.05	37.66/39.60
4096	23.12/26.24	25.85/30.20	31.33/35.45	37.11/39.42
8192	23.08/25.56	25.08/29.01	30.31/35.04	36.27/38.61
16384	21.45/24.77	24.67/28.29	30.04/34.75	35.35/38.02
32768	20.89/23.96	24.13/26.61	28.25/32.28	34.01/36.77
		Baboon		
1024	19.67/ 21.53	22.42/ 24.32	25.56/ 28.46	31.25/33.65
2048	19.45/ 21.15	22.30/ 24.13	25.04/ 28.16	30.62/33.15
4096	18.82/ 21.04	22.09/ 24.05	24.78/ 27.24	30.03/32.24
8192	18.31/ 20.56	21.75/ 23.75	24.23/ 27.03	28.53/32.04
16384	17.82/ 19.55	21.02/ 23.65	24.01/ 26.57	27.25/30.52
32768	17.00/18.89	19.27/ 21.89	23.21/ 25.31	26.47/29.36
		Boat		
1024	26.56/27.46	30.32/33.44	34.23/36.65	38.76/42.34
2048	26.02/27.09	30.10/32.61	33.71/36.32	37.54./42.02
4096	25.54/26.15	29.75/32.13	33.21/36.05	37.02/41.26
8192	25.04/26.02	28.84/31.27	32.62/33.61	36.29/40.26
16384	24.53/25.73	27.36/30.22	31.24/33.27	35.13/38.76
32768	23.88/24.98	25.85/28.88	30.13/31.32	33.21/37.05

		GoldHill		
1024	28.35/30.04	31.31/32.93	34.72/35.96	37.64/39.02
2048	27.89/29.57	30.67/32.15	34.15/35.29	36.72/38.58
4096	27.17/29.07	30.13/31.69	33.82/34.84	36.25/38.12
8192	26.46/28.42	29.69/30.75	33.15/34.49	35.17/37.84
16384	25.19/27.93	29.18/30.07	32.58/33.14	34.92/36.13
32768	24.79/27.10	28.39/29.29	31.19/32.17	34.23/35.45
		Bike		
1024	27.25/29.54	31.29/33.47	36.08/37.25	38.74/41.56
2048	26.73/28.79	30.85/32.79	35.24/36.73	38.17/40.83
4096	26.12/27.35	30.14/32.17	34.87/35.94	37.84/39.72
8192	25.59/26.75	29.82/31.65	33.78/35.62	37.31/39.39
16384	24.11/25.84	29.17/31.05	33.05/34.51	36.51/38.64
32768	23.88/25.02	27.35/29.15	31.85/34.19	34.85/36.73
		Woman		
1024	27.47/29.15	31.42/33.45	35.35/37.48	38.69/40.25
2048	26.12/28.73	30.85/33.03	35.02/37.21	38.28/39.62
4096	25.81/26.35	30.26/32.24	34.78/36.68	37.73/39.15
8192	24.84/26.02	29.72/31.78	34.15/35.48	36.95/38.72
16384	24.23/25.87	29.16/31.02	33.11/35.14	35.84/38.15
32768	23.22/25.04	27.88/28.95	31.84/34.62	33.92/36.02
		Pepper		
1024	31.47/32.46	34.85/35.61	39.14/40.23	44.12/45.49
2048	30.95/31.94	34.02/34.93	38.65/39.45	43.63/45.02
4096	30.34/31.35	33.56/34.12	37.95/38.82	42.92/44.17
8192	29.85/30.85	32.21/33.79	37.45/38.04	42.02/43.85
16384	29.03/29.55	30.96/33.08	36.43/37.17	40.15/43.21
32768	28.98/29.09	30.42/32.34	35.18/35.15	39.49/41.81

If one compares Table 2 with Table 1,*PSNR* between cover and stego image decreases,as the payload is increased but it is highly acceptable by the human visual system (*HVS*).Also *SIM* between original secret image and extracted secret image is always '1' for all images at all compression rates.

Proposed steganography technique is also applied for Motion *JPEG*2000 video frames as *JPEG*2000 encoder is directly applicable to video frame. This is due to the reason that no motion compensation is performed in Motion *JPEG*2000 video standard. In this work, four videos, namely Miss American, Foreman, Coastguard and Football are considered as these are used by the research of image processing domain. Each frame of these video is compressed using Kakadu software tool and average *PSNR* of each frame is calculated. In Table 3, average *PSNR*and *PSNR-HVS*of all these video framesare shown when no secret data is embedded. The*PSNR and PSNR-HVS* is evaluated for all videos considered in this workat different compression rates are shown in Table 4.

Table 3.Average *PSNR* (in dB)/ *PSNR-HVS* (dB) at different compression rate for different video frames, without any payload

Video Sequence	Rate(*in bpp)*			
	0.250	0.50	1.00	2.00
Miss American	33.19/34.39	40.07/41.31	42.85/44.27	44.76/45.79
Foreman	31.23/32.68	35.39/36.28	37.87/38.29	42.91/43.72
Coastguard	33.41/34.29	36.25/37.42	39.27/40.38	41.31/42.63
Football	34.21/35.42	39.15/40.39	41.76/42.93	43.62/44.81

Table 4. Average *PSNR* (in dB)/ *PSNR-HVS* (in dB) between different cover and stego video frames at different compression and different payload by using proposedTechnique

Embedding Capacity(in bits)	*Rate(in bpp)*			
	0.250	0.50	1.00	2.00
		Miss American		
1024	32.31/33.87	39.25/40.63	41.55/43.78	43.38/45.05
2048	31.75/33.41	38.79/40.24	41.25/43.23	43.05/44.75
4096	31.25/32.93	38.21/39.92	40.65/42.82	42.74/44.21
8192	30.75/32.32	37.78/39.39	40.05/42.34	42.21/43.92
16384	30.09/31.95	37.17/38.87	39.45/41.89	41.46/43.32
32768	29.75/31.34	36.75/38.31	39.01/41.42	40.95/42.87
		Foreman		
1024	30.21/32.05	34.21/35.64	36.21/37.23	41.20/42.78
2048	29.86/31.28	33.88/35.04	35.74/36.92	40.75/42.21
4096	29.37/31.05	33.20/34.83	35.15/36.43	40.12/41.87
8192	28.89/30.48	32.70/34.17	34.75/35.98	39.67/41.33
16384	28.35/29.96	31.25/33.68	34.06/35.54	39.02/40.89
32768	27.67/29.10	30.95/33.04	33.62/34.89	38.52/40.42
		Coastguard		
1024	32.15/33.28	34.85/36.84	37.67/39.43	40.24/42.02
2048	31.84/32.87	34.17/36.34	37.14/38.92	39.79/41.65
4096	30.92/32.35	33.67/35.99	36.74/38.25	39.24/41.05
8192	30.28/31.88	33.24/35.45	36.25/37.78	38.75/40.56
16384	29.75/31.43	32.56/34.92	35.70/37.35	38.20/40.05
32768	29.01/30.74	31.94/34.54	35.21/36.95	37.84/39.71
		Football		
1024	32.68/34.75	37.75/39.79	40.14/42.25	42.24/43.76
2048	32.22/34.23	37.29/39.34	39.72/41.78	41.78/43.04
4096	31.75/33.86	36.78/38.95	39.16/41.21	41.35/42.78
8192	31.10/33.35	36.13/38.32	38.71/40.89	40.71/42.35
16384	30.69/32.98	35.65/37.87	38.25/40.23	40.09/41.97
32768	29.10/32.08	35.16/37.47	37.65/39.67	39.53/41.32

From Table 4, one can conclude that when higher amount of the secret data is hidden in a frame of a video, *PSNR and PSNR-HVS* decreases at all compression rates, but it is acceptable to *HVS* as *PSNR* is higher than 30 dB, in most of the cases.(Hsieh, 2010).

Proposed technique is compared with the existing steganography techniques for *JPEG*2000 images and this comparison is shown in Table 5. In this comparison, embedding capacity and *PSNR*are considered as effective parameters. In this comparison, embedding capacity is considered till the stego image is not susceptible (undetectable) to a steg analysis attack.

Table 5. Embedding capacity (in bits)/ average *PSNR* comparison of proposed technique with existing techniques

Image	Boat	Lena	Pepper	Baboon
Noda *et al.*(2002)	-	58656/37	-	58656/-
Su *et al*. (2003)	16384/-	16384/-	16384/-	16384/-
Zhang *et al*. (2009)	14000/-	14000/-	14000/-	19500/-
Ishida *et al*. (2008)*	-	19568/ 37.1	19568/ 36.3	19568/ 30.1
Ishida *et al*. (2009)*	-	14936/37.4	14936/35.2	14936/33.25
Ohyama*et al.*(2008)*	-	11814/36.38	-	-
Goudia*et al.* (2011)	-	6768/34.29	-	10480/34.01
Proposed	32768/27.78	32768/31.33	32768/33.52	32768/21.49

- *PSNR* of stego images is not given in Zhang *et al*. technique
* File size of the stego images increases in these techniques.

From this table, one can infer that maximum undetectable embedding capacity of Noda *et al.* is 58,656 bits, Su *et al.* is 16,384 bits; Zhang *et al.* is 14,000 bits; Ishida *et al*. is 19,568 bits; Ishida *et al*. is 14936 bits; Ohyama*et al*. 11,814 bits; Goudia*et al*. is 10,480 bits. *PSNR* of proposed technique is average as

more than one compression rates are considered in this work. Proposed technique is also highly suitable to a *HVS* system. Hence proposed technique shows a good performance, as evidenced by comparison table. In their work, Zhang *et al*. has not taken *PSNR* as parameter, butthey considered*HVS* as image quality parameter. Proposed technique is also highly suitable to a *HVS* system and is applicable to lossy*JPEG*2000 compression standard, while all existing techniques are applicable to lossless mode of *JPEG*2000 standard. Hence proposed technique shows a good performance, as evidenced by comparison table.

V. STEG ANALYSIS TEST

Proposed technique exhibits extremely low probability when subjected to Receiver Operating Characteristics (*ROC*) 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 mean, variance, skewness and kurtosis of each wavelet subband are computed. On the basis of these statistical characteristics, *ROC* curves are drawn and shown in Figure 5.

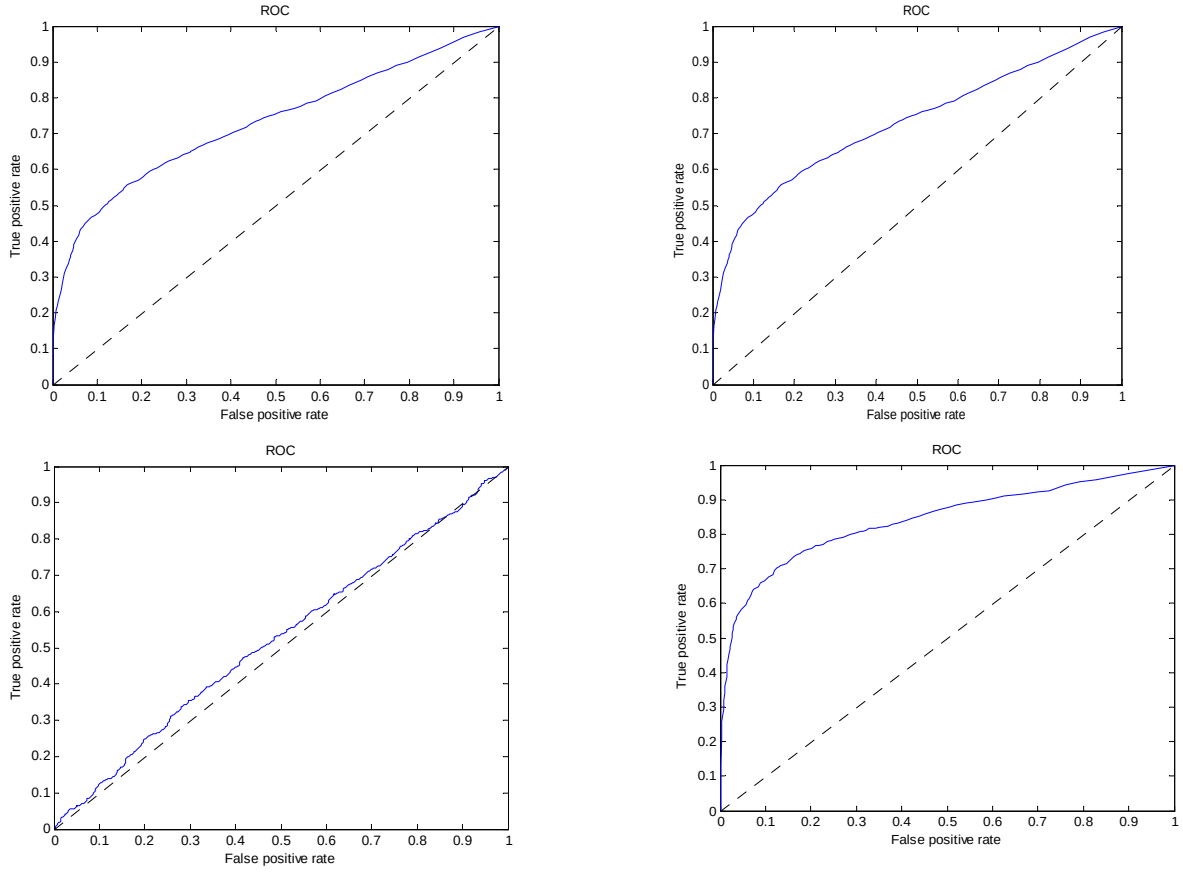

Figure 5. *ROC* curve for different embedding capacities **(a)**16,384 bits **(b)** 32,768 bits **(c)** 49152 bits **(d)** 65,536 bits

Figures 5(a)-5(d) show *ROC* curves of the test images different capacities: 16,384 bits, 32,768 bits, 49152 bits and 65,536 bits. From this one can observe that the detector is in vain when the embedding capacity is upto32,768 bits. And when the embedding capacity is increased to 32,768 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.

VI. CONCLUSION

In this work, BPC based steganography technique for *JPEG*2000 compressed images and videos, is proposed. Secret data bits are embedded in the lowest significant bit planes of wavelet coefficients of a cover image rather than higher significant bit planes to keep the distortion in stego images low. *OPAP* is also performed to enhance visual quality of stego images. Experimental results show that the technique provides large embedding capacity and high quality of stego images than existing steganography techniques for *JPEG*2000 compressed images.

REFERENCES

Aacharya, T. and Tsai, P.S.*JPEG*2000 Standard For Image Compression – Concepts, Algorithms and VLSI Architectures, Wiley, 2005.

Carvajal, B. E., Gallegos-Funes F. J., and Rosales-Silva, A. J. 2013. Color local complexity estimation based steganographic method, *EXPERT SYSTEMS WITH APPLICATIONS*, 40(4): 1132–1142. doi: http://dx.doi.org/10.1016j.eswa.2012.08.024

Chan, C. K. and Cheng, L. M.2004. Hiding data in images by simple LSB substitution, *PATTERN RECOGNITION*, 37(3):469–474. doi:10.1016/j.patcog.2003.08.007

Chang, C. C., Tai, W. L., and Lin, C. C., 2006. A reversible data hiding scheme based on side match vector quantization. *IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY*, 16(10):1301–1308. doi: 10.1109/TCSVT.2006.882380

Chang, C. C. *et al*,2007. Reversible hiding in DCT-based compressed images. *INFORMATION SCIENCES*, 177(13): 2768–2786. doi:10.1016/j.ins.2007.02.019

Chang, C. C., Wu, W. C. and Hu Y.C. 2007. Lossless recovery of a VQ index table with embedded secret data. *JOURNAL OF VISUAL COMMUNICATION AND IMAGE REPRESENTATION,* 18(3):207–216. doi:10.4304/jsw.8.3.547-553

Chang, C. C., Nguyen, T. S., and Lin, C. C.2011. A reversible data hiding scheme for VQ indices using locally adaptive coding. *JOURNAL OF VISUAL COMMUNICATION AND IMAGE REPRESENTATION*, 22(7): 664–672. doi:10.1016/j.jvcir.2011.06.005

Chen, W. J., Chang, C. C., and Le, T. (2010). High payload steganography mechanism using hybrid edge detector. *EXPERT SYSTEMS WITH APPLICATIONS*, 37(4):3292–3301. doi:10.1016/j.eswa.2009.09.050

Chen, W. Y. 2008. Color image steganography scheme using DFT, SPIHT codec, and modified differential phase-shift keying techniques. *APPLIED MATHEMATICS AND COMPUTATION,* 196(1): 40–54. doi:10.1016/j.procs.2015.08.168

Chu, R., You, X., Kong X., and Ba, X.2004. DCT-based image steganographic method resisting statistical attacks. Proceedings of IEEE international conference on acoustics, speech, and signal processing, 5. http://ieeexplore.ieee.org/xpls/abs_all.jsp%3Farnumber%3D1327270

Goudia, D., Chaumont M., Puech W. and Said N. H. 2011. A Joint Trellis Coded Quantization Data Hiding Scheme in the *JPEG*2000 Part-2 Coding Framework, 19th European Signal Processing Conference, pp. 1110-1114, Sept. http://ieeexplore.ieee.org/xpls/abs_all.jsp%3Farnumber%3D7073918

Hai-ying, G., Yin, X. and Guo-qiang, L. 2008. A steganographic algorithm for *JPEG*2000 images. IEEE computer society, Int. Conf. on Computer Science and Software Engineering, pp. 1263-1266. doi: 10.1109/CSSE.2008.139

Hsieh, M. S. 2010. A robust image authentication method based on wavelet transform and Teager energy operator. *INTERNATIONAL JOURNAL OF MULTIMEDIA AND ITS APPLICATIONS*, 2(3):1-17. doi: : 10.5121/ijma.2010.2301

Ioannidou, A., Halkidis, S. T., and Stephanides, G. (2012). A novel technique for image steganography based on a high payload method and edge detection. *EXPERT SYSTEMS WITH APPLICATIONS,* 39(14): 11517–11524. doi:10.1016/j.eswa.2012.02.106

Ishida, T., Yamawak,i K., Noda H., and Niimi M.2008. Performance improvement of *JPEG*2000 steganography using *QIM*. Intelligent Information Hiding and Multimedia Signal Processing, International Conference, IEEE Computer Society, pp: 155-158. doi:10.1109/IIH-MSP.2008.120

Ishida T., Yamawaki K., Noda H. and Niimi M. 2009. An Improved *QIM-JPEG*2000 Steganography and Its Evaluation by Steganalysis. *JOURNAL OF INFORMATION PROCESSING*, 17: 267-272. http://doi.org/10.2197/ipsjjip.17.267

KAKADU software, www.kakadusoftware.com/

Jafari, R., Ziou, D. and Rashidi, M. M.2013. Increasing image compression rate using steganography. *EXPERT SYSTEMS WITH APPLICATIONS*, 40(17): 6918–6927. doi:10.1016/j.eswa.2013.06.008

Jin, H. L., Fujiyoshi, M., Sheki Y. and Kiya, H. 2007. A Data Hiding Method for JPEG2000 Coded Images Using Module Arithmetic. *ELECTRONICS AND COMMUNICATIONS IN JAPAN*, 90(7): 37-45. doi: 10.1002/ecjc.20286

Noda, H., Spaulding, J., Shirazi, M. N., Kawaguchi, E. 2002. Application of bit plane decomposition steganography to JPEG2000 encoded images. IEEE Signal Processing Letters, 9(12), pp. 410-413. doi: 10.1109/LSP.2002.806056

Noda, H., Niimi, M., and Kawaguchi, E. (2006). High-performance JPEG steganography using quantization index modulation in DCT domain. *PATTERN RECOGNITION LETTERS*, 27(5): 455–461, 2006. doi:10.1016/j.patrec.2005.09.008

Ohyama, S., Niimi, M., Yamawaki, K., and Noda, H. 2008. Reversible data hiding for full color JPEG2000 compressed bit-stream preserving bit-depth information. In Proc. ICPR 08: the 19th International Conference on Pattern Recognition, pp. 1-4, December. doi:10.1109/ICPR.2008.4761625

Ramkumar, M. and Akansu, A. N., 2001.Capacity Estimates for Data Hiding in Compressed Images, IEEE Transactions on Image Processing,10(8): 1252-1263.doi:1057-7149(01)06043-2.

Sencar, H. T., Ramkumar, M. and Akansu, A. N., 2004.Data Hiding Fundamentals and Applications: Content Security in Digital Multimedia, Elsevier Academic Press, July.

Su, P. C. and Kuo, J. 2003. Steganography in JPEG2000 compressed images. IEEE Transactions on Consumer Electronics, 49(4), pp. 824-832. **doi:**10.1109/TCE.2003.1261161

Yang, C. H., Yang W. J., Huang, C. T., and Wang, S. J. (2011). Reversible steganography based on side match and hit pattern for VQ-compressed images. *INFORMATION SCIENCES*, 181(11):2218–2230. doi:10.1016/j.ins.2011.01.015

Zhang, L., Wang, H., and Wu, R., 2009. A high capacity steganography scheme for JPEG2000 baseline system. IEEE Transactions on Image Processing, 18(8), pp. 1797-1803. doi: 10.1109/TIP.2009.2021544