bands, such as low, intermediate and high frequency sub band, which improves the robustness of watermark against different attacks. In the scheme proposed by P. Ramana et al. [10] watermarking is done by modifying the frequency coefficients of the image, based on human visual systems perception of image content such that its amplitude is kept below the distortion sensitivity of the pixel and thus preserving the image quality.

1.2 CONTRIBUTION TO THE PAPER

In the field of color image watermarking, most color image watermarking algorithms consider only the luminance content for watermarking. In this work, the proposed approaches DWTC utilize the chrominance and DWTLC utilizes both the luminance and chrominance content for watermarking. Watermarking is done in L*a*b* color space. A significant improvement in the peak-signal to noise ratio (PSNR) of the watermarked image and robustness to attacks is achieved with the use of DWT than an existing work based on Spatio Chromatic Discrete Fourier Transform (SCDFT) [13]. Also, the proposed approaches are shown to be robust to large classes of attacks than the DWT approach proposed by Ramana et al. [10]. Especially, the proposed schemes are resistant to JPEG compression and collusion attacks.

The rest of the paper is organized as follows: Section 2 deals with the Discrete Wavelet Transform. Section 3 describes the proposed watermarking approaches. Experimental results are discussed in Section 4. Section 5 deals with conclusion and future work.

2. THE DISCRETE WAVELET TRANSFORM

The Discrete Wavelet Transform (DWT), which is based on sub band coding, is found to yield a fast computation of Wavelet Transform. It is easy to implement and reduces the computation time and resources required. With DWT, a time-scale representation of the digital signal is obtained using digital filtering techniques. The signal to be analyzed is passed through filters with different cutoff frequencies at different scales.

Wavelets can be realized by iteration of filters with rescaling. The resolution of the signal, which is a measure of the amount of detail information in the signal, is determined by the filtering operations, and the scale is determined by up sampling and down sampling (sub sampling) operations. DWT is computed by successive low pass and high pass filtering of the discrete time domain signal as shown in Fig.1. This is called the Mallat algorithm or Mallat-tree decomposition. In the figure, the signal is denoted by the sequence x (n), where n is an integer. The low pass filter is denoted by g (n) while the high pass filter is denoted by h (n). At each decomposition level, the half band filters produce signals spanning only half the frequency band. This doubles the frequency resolution as the uncertainty in frequency is reduced by half. In accordance with Nyquist's rule, if the original signal has a highest frequency of π, which requires a sampling frequency of 2π radians, then it now has a highest frequency of π/2 radians. It can now be sampled at a frequency of π radians thus discarding half the samples with no loss of information. This decimation by 2 halves the time resolution as the entire signal is now represented by only half the number of samples. Thus, while the half band low pass filtering removes half of the frequencies and thus halves the resolution, the decimation by 2 doubles the scale. A single level of decomposition can mathematically be expressed as in Eq. (1):

$$y_{high}[k] = \sum_n x(n) \cdot g(2k-n)$$
$$y_{low}[k] = \sum_n x(n) \cdot h(2k-n) \quad (1)$$

With this approach, the time resolution becomes arbitrarily good at high frequencies, while the frequency resolution becomes arbitrarily good at low frequencies. The filtering and decimation process is continued until the desired level is reached. The maximum number of levels depends on the length of the signal. The DWT of the original signal is then obtained by concatenating all the coefficients, g[n] and h[n], starting from the last level of decomposition.

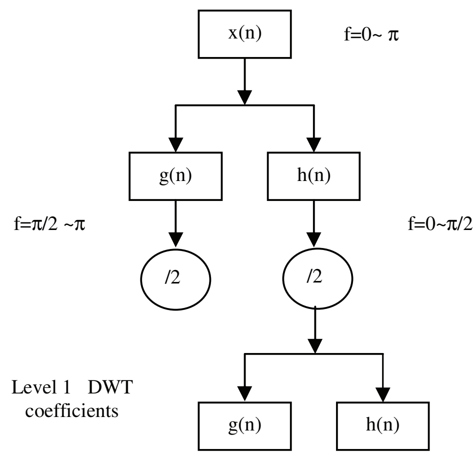


Fig.1. Single Level DWT decomposition

The Fourier transform retrieves only the global frequency content of a signal and the time information is lost. This is overcome by the short time Fourier transform (STFT) which calculates the Fourier transform of a windowed part of the signal and shifts the window over the signal. The short time Fourier transform gives the time-frequency content of a signal with a constant frequency and time resolution due to the fixed window length. This is often not the most desired resolution. For low frequencies often a good frequency resolution is required over a good time resolution. For high frequencies, the time resolution is more important. A multi-resolution analysis becomes possible only by using wavelet analysis. The continuous wavelet transform is calculated analogous to the Fourier transform, by the convolution between the signal and analysis function and retrieves the time-frequency content information with an improved resolution compared to the STFT. However the trigonometric analysis functions are replaced by a wavelet function. The specialty with wavelets is that the wavelet is a short oscillating function which contains both the analysis function and the window. Time information is obtained by shifting the wavelet over the signal. The frequencies are changed by contraction and dilatation of the wavelet function.

In a two dimensional DWT, a single level decomposition on an image produces four bands of data, one corresponding to the low pass band (LL) and two others corresponding to mid frequency bands namely horizontal (HL), vertical (LH) and one

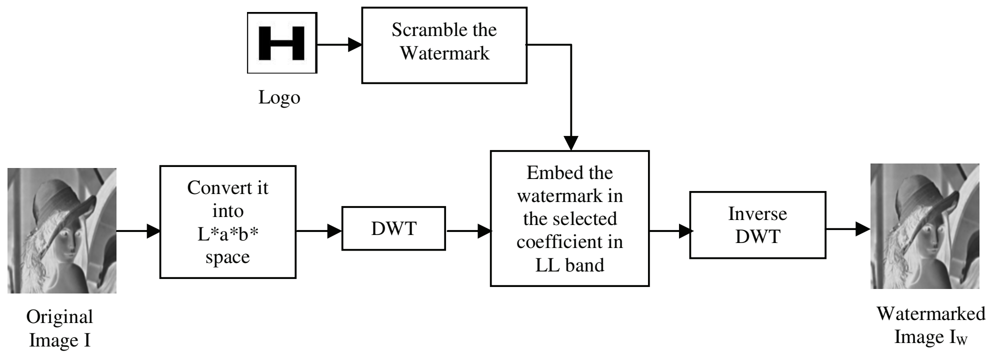


Fig.2. Watermark embedding using the proposed DWTC/DWTLC Watermarking

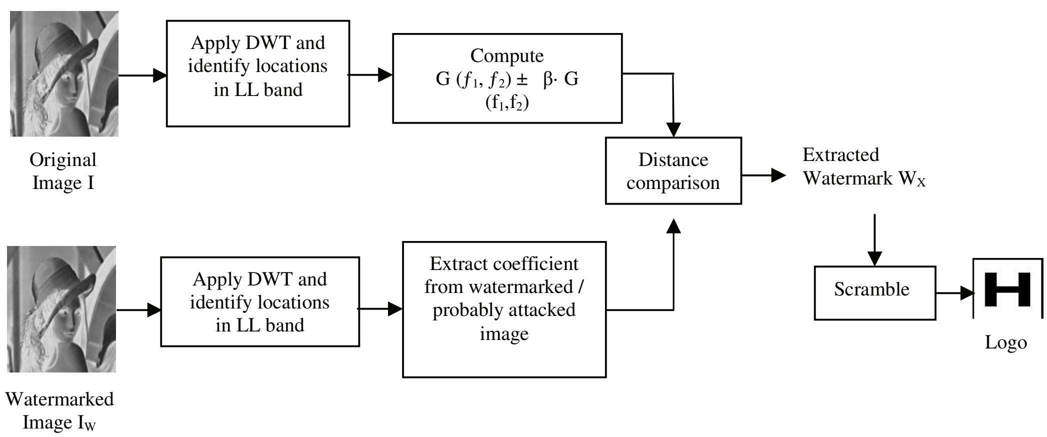


Fig.3. Watermark extraction using the proposed DWTC/DWTLC Watermarking

4. EXPERIMENTAL RESULTS

In this section, the effect of DWTC and DWTLC schemes implemented using MATLAB R2007b is presented. The fidelity criteria and robustness of the proposed watermarking schemes are evaluated with standard test images available in USC-SIPI image database [14] and those discussed in tables are shown in Fig.4. The proposed approaches are compared with an existing SCDFT based approach proposed by Tsz Kin Tsui et al. [13] and a DWT based approach proposed by Ramana et al [10]. In Tsz Kin Tsui et al. approach, watermarking is done on chrominance content. In Ramana et al. approach, watermarking is done on the mid frequency bands with a gain $\alpha = 0.6$.

In the experiments for the proposed schemes, an image of size 256×256 is subjected to a single level decomposition using Haar filter. This results in four bands of data and the LL band is chosen for embedding the watermark. Watermark to be embedded is a Logo. Experiments are conducted with many Logos each of different sizes and for readability sake only one is shown in Fig. 5 (b). This is scrambled first to be robust enough to attacks. The scrambled watermark is then embedded in the LL band in those coefficients decided by the random function using Eq. (4). The original and watermarked Lena images using DWTC and DWTLC approaches are shown in Fig.5 (c) and (d) along with associated PSNR.

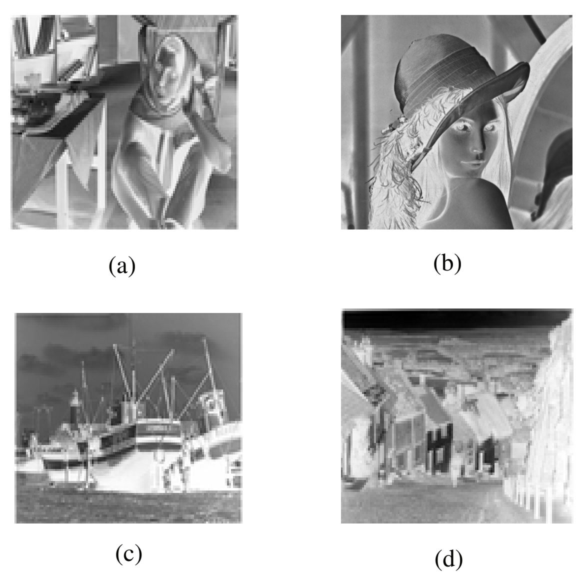


Fig.4. Test images used – (a) Barbara (b) Lena (c) Boats (d) Goldhill

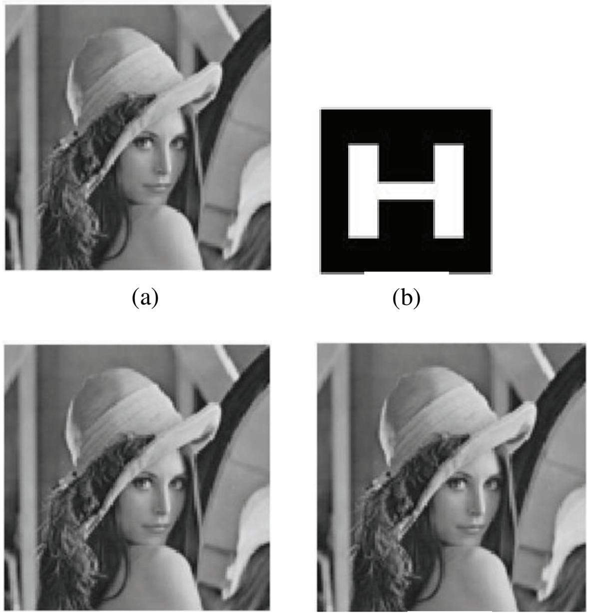


Fig.5. (a) Original Image (b) Logo (c) and (d) Watermarked Images using DWTC with PSNR: 57.09dB and DWTLC with PSNR: 56.76dB respectively

An important parameter used in the embedding procedure is the value of β, which is the embedding strength that is fixed depending on the level of imperceptibility needed. In the experiments β value is chosen as $\beta = 0.02$. It is chosen after the conduct of experiments and its impact against PSNR is reported in Fig.6. From the figure, it is clear that the PSNR is good for values $\beta < 0.2$ and hence $\beta = 0.02$ is taken for further experiments.

In the rest of this section, first the Fidelity criteria of the proposed watermarking approaches are analyzed. Then, the robustness of the proposed watermarking approaches is shown by the conduct of various experiments. Next to that, comparison of the proposed approaches against existing SCDFT approach [13] and DWT approach [10] is discussed. Finally, the resistance of the proposed approaches against Collusion attack is discussed.

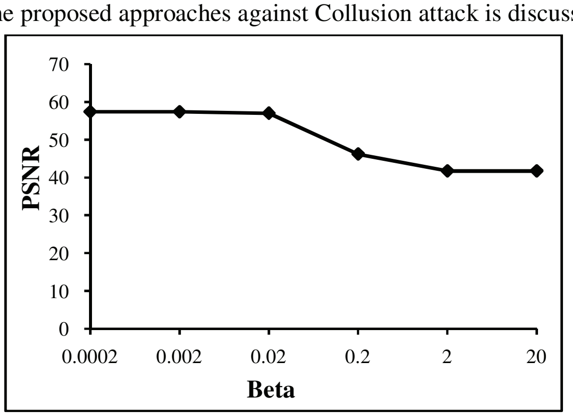


Fig.6. Impact of Beta vs. PSNR

4.1 FIDELITY CRITERIA

When the level of information loss is expressed as function of original image and watermarked image, then it is said to be based on objective fidelity criterion [12]. The root mean square error is one such best criteria and is given in Eq. (5).

$$RMSE = \sqrt{\frac{1}{w \times h}\sum_{j=0}^{h-1}\sum_{i=0}^{w-1}\left(\left(\Delta R_{ij}\right)^2 + \left(\Delta G_{ij}\right)^2 + \left(\Delta B_{ij}\right)^2\right)} \quad (5)$$

where Rij, Gij and Bij are the red, green and blue values of the pixel and w and h are the width and height of the image.

Table.1. PSNR of the proposed schemes

Images	Dimension	PSNR	
		DWTC	DWTLC
Barbara	256×256	57.28	57.02
	512×512	57.55	57.57
Lena	256×256	57.09	56.76
	512×512	57.34	57.26
Boats	256×256	57.15	56.96
	512×512	57.46	57.39
Goldhill	256×256	56.92	56.64
	512×512	57.29	57.25

Table.2. BER for various attacks

Attack	Parameter	BER
Mean Filtering	3×3 mask	0
	5×5 mask	0
	7×7 mask	0
Median Filtering	3×3 mask	0
	5×5 mask	0
	7×7 mask	0
Average Filtering	3×3 mask	0
	5×5 mask	0
	7×7 mask	0
Weiner Filtering	3×3 mask	0
	5×5 mask	0
	7×7 mask	0
Blurring		0
Sharpening		0
Histogram Equalization		0
Intensity Adjustment		0
Decorrelation Stretch		0
JPEG Compression	Qf - 80	1.8
	Qf - 40	2.77
	Qf - 20	4.6
Scaling	sf - 1.5	0
	sf - 3	0
	sf - 5	0
Additive noise	v=1	0
	v=2	2.77
	v=3	4.33
	v=4	8.33

To evaluate the fidelity of the watermark, the peak signal to noise ratio is used and it is measured as in Eq. (6). The typical value for PSNR is between 30 and 50 dB and the higher, the better. The proposed watermarking schemes are tested for various images and the PSNR obtained is shown in Table 1.

$$PSNR = 10\log_{10}\left(\frac{3\times255^2}{RMSE}\right) \quad (6)$$

From Table 1, it can be seen that the PSNR of the watermarked images is very good with good visible quality irrespective of the image dimensions. This is shown in Fig. 5. It is observed that there is a slight increase in image quality while considering the chrominance alone for watermarking in the DWT domain.

4.2. ROBUSTNESS OF THE WATERMARK

In order to show the robustness of the proposed DWTC and DWTLC schemes against attacks, a series of experiments have been conducted by applying the attacks to watermarked Lena image of size 256×256. We consider both geometric and non geometric attacks. Non geometric attacks include JPEG compression, filtering, histogram equalization, sharpening, blurring, image intensity adjustment and decorrelation stretch. Geometric attacks include scaling, rotation and additive noise.

The test results indicate that the proposed watermarking schemes produce watermarked images with best quality and in addition to that, the watermark is resistant to various geometric attacks and common image processing operations. The robustness is illustrated with the given bit error rate (BER) which is defined as the ratio between the number of incorrectly extracted bits and the length of the watermark [15]. BER for various attacks conducted are listed in Table 2.

4.2.1. Non Geometric Attacks

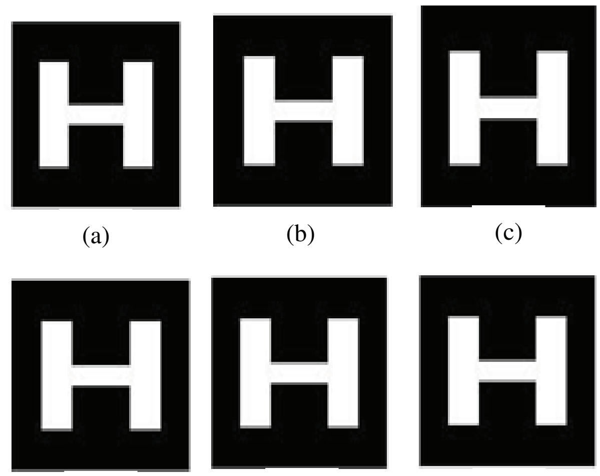
Filtering - Images watermarked using proposed watermarking schemes are attacked by mean, median, average and Weiner filters with a mask of size 3×3, 5×5, 7×7. In all the cases, the watermark is recovered with zero BER. The recovered watermark after average filtering with a mask of size 7×7 is shown in Fig.7 (a). This robustness is achieved because the watermarking is done by modifying only selected coefficients in the approximation band and the watermark is embedded in a multiplicative way.

Blurring - Blurring in the fre0000quency domain refers to the suppression of high frequencies. Blurring attack is performed by image filtering that convolves a point spread function with the watermarked image to produce a blurred watermarked image. The proposed scheme resists blurring attack with zero BER and is shown in Fig.7 (b).

Sharpening - Both the proposed methods can resist sharpening strongly with zero BER over the whole range of intensity as shown in Figure 7(c).

Histogram Equalization - Histogram equalization is usually used for image enhancement. It is a kind of histogram modeling technique that modifies the dynamic range and contrast of an image so that its intensity histogram has a desired shape. The watermarked image is histogram equalized by making use of a nonlinear mapping that reassigns the intensity values so that the attacked image has a flat histogram. Figure 7 (d) shows the watermark recovered with zero BER after histogram equalization.

Image intensity adjustment - The watermarked image is attacked by intensity adjustment. Intensities between 0.2 × 256, 0.3 × 256 and 0×256 in each plane are mapped to intensities between 0.6×256, 0.7×256 and 1× 256. Though, the watermark is embedded in luminance and chrominance content, the proposed schemes are immune to image intensity adjustment with zero BER as shown in Fig.7 (e).



(a) (b) (c)

(d) (e) (f)

Fig.7. Watermarks recovered after the non geometrical attacks (a) Average filtering by a mask of size 7×7 (b) Blurring (c) Sharpening (d) Histogram Equalization (e) Intensity adjustment (f) Decorrelation stretch

Decorrelation Stretch - Decorrelation stretch attack as available in MATLAB enhances the color separation of an image with significant band-band correlation. The exaggerated colors improve visual interpretation and make feature discrimination easier. However, when this is applied to watermarked images, it does not affect the watermark recovery and it ensures zero BER as shown in Fig.7 (f).

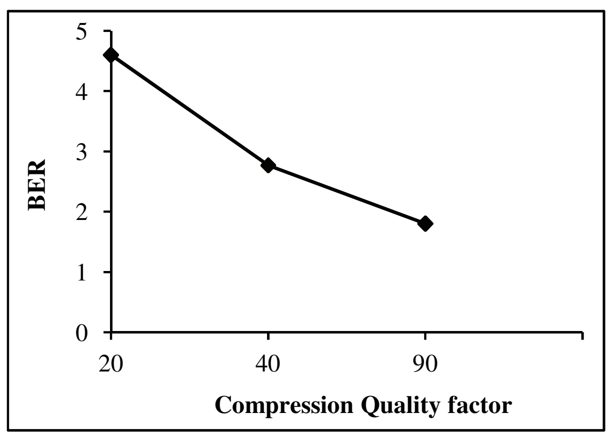


Fig.8. JPEG compression Quality factor (Qf) Vs. BER

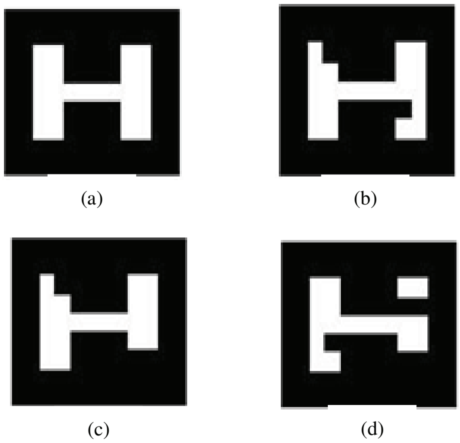


Fig.9. Watermarks recovered after JPEG Compression attacks – (a) Qf-80 (b) Qf-40 (c) Qf-30 (d) Qf-20

JPEG Compression - The watermarked images are compressed with both JPEG Lossy and Lossless Compression. With the case of lossless compression, the watermark is recovered perfectly with zero BER even when the quality factor (Qf) is varied from 90 to 10. But with lossy compression, the watermark is visible as long as the Qf is greater than 40. The results obtained for JPEG lossy compression is shown as a function of BER and compression quality in Fig.8. If the Qf is reduced further, there is slight disturbances in the recovered watermark and is shown in Fig.9.

4.2.2 Geometric Attacks

Scaling - For image scaling operations, the watermarked images are individually scaled by a factor (sf) of 1.5, 3 and 5 in each direction. Before watermark extraction, the watermarked image is rescaled back to its original size using bilinear interpolation because the proposed algorithm requires the pixels in the watermarked image to be in the corresponding location as the original host image in order to extract the watermark correctly. After scaling operations, the watermark embedded in the LL band is recovered successfully with zero BER from the scaled watermarked image and the watermarks recovered after scaling attacks with sf= 1.5, 3 and 5 are shown in Fig.10.

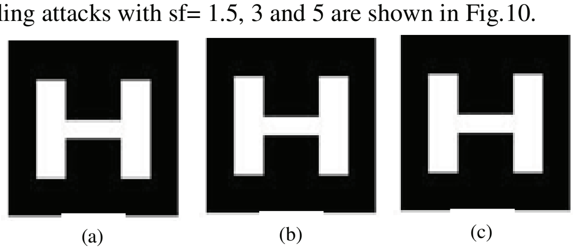


Fig.10. Watermarks recovered after scaling attacks (a) sf = 1.5 (b) sf = 3 (c) sf = 5

Rotation - Rotation attack is performed by rotating the watermarked image by a small angle, then scaling the rotated image and finally cropping the scaled image to the original image size. In a pixel based watermarking system, even if the image is rotated by a small degree, the positions of the pixels are shifted. Though, the rotation attack does not cause severe visual degradation it produces errors during watermark extraction.

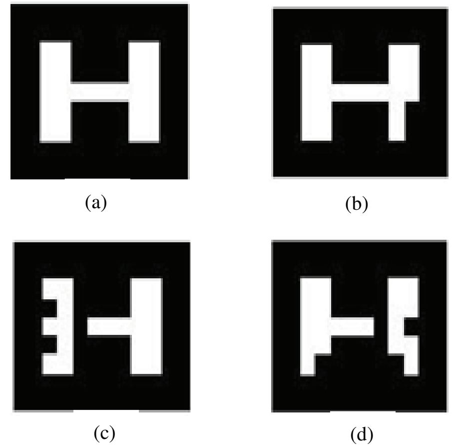


Fig.11. Watermarks recovered after additive noise for variance v (a) v=1 (b) v=2 (c) v=3 (d) v=4

Additive noise - The watermarked images are distorted by additive Gaussian noise with zero mean and a variance (v) which is varied from 1 to 4. The watermark is however recognizable as long as the variance is less than equal to 4 and this is shown in Fig.11. Beyond that, the proposed schemes can recover the watermark with much degradation. The BER obtained for the noise added with various levels of variances are shown in Fig.12.

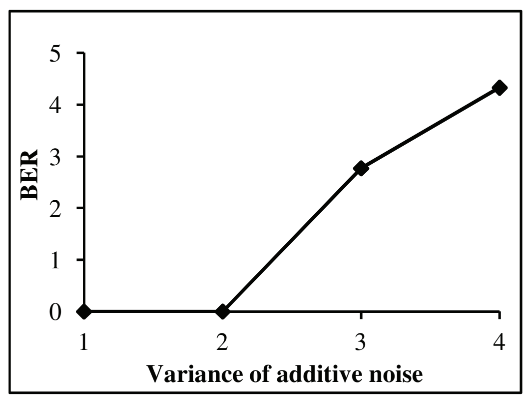


Fig.12. Impact of variance of additive noise Vs. BER

4.3 COMPARISON OF THE PROPOSED SCHEMES AGAINST SCDFT BASED APPROACH

The proposed schemes appear similar in the way the chrominance contents are utilized for watermarking in the SCDFT approach proposed by Tsz Kin Tsui et al. [13]. The use of wavelets for watermarking has considerably increased the PSNR of the watermarking approach to 57 dB on an average as shown in Table 1. But for the SCDFT approach when the Logo shown in Fig.5 (b) is embedded, the PSNR is between 40 and 45 dB. Also, the proposed approaches are resistant to scaling even by a factor of 5 whereas the SCDFT results in some errors during watermark recovery. Also, the SCDFT approach is not resistant to JPEG compression especially for a low compression factor. The proposed schemes on the other hand, guarantee perfect extraction of the watermark when the quality factor is $40<Qf<90$and with minimal BER even when the quality factor is as low as 20. This is shown in Fig.9.

4.4 COMPARISON OF THE PROPOSED SCHEMES AGAINST DWT BASED APPROACH

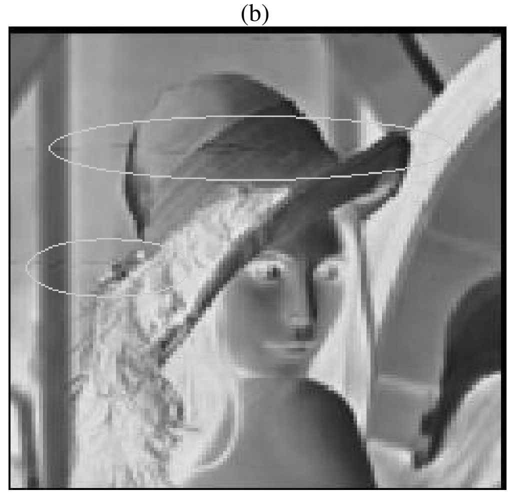
The DWT based approach proposed by Ramana et al. [10] shows resistance to additive noise and salt and pepper noise only for a small variance. But the proposed schemes can resist additive noise even when the variance is 4. All the other attacks on the DWT scheme do not guarantee the recovery of the embedded watermark. Also, the PSNR of the watermarked images using this DWT approach is on an average 42 dB. On the other hand, the proposed schemes are resistant to a variety of attacks as discussed earlier with a PSNR of 57 dB on an average.

4.5 RESISTANCE TO COLLUSION ATTACK

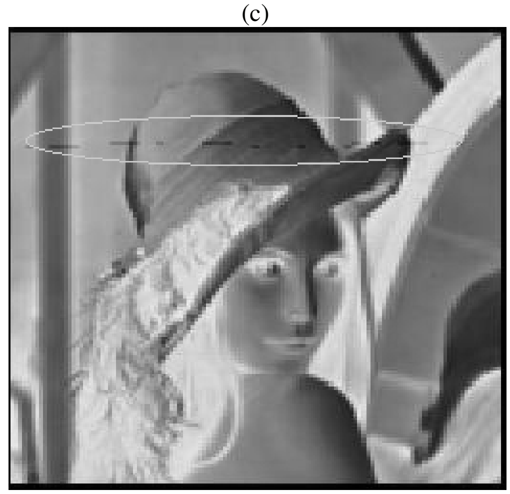
Conventional watermarking techniques are concerned with robustness against a variety of attacks such as filtering but do not always address robustness to attacks mounted by a coalition of users with the same content that contains different marks. These attacks, which are known as collusion attacks, can provide a cost effective approach to removing watermark. Linear collusion is one of the most feasible collusion attacks against watermarking. When users come together with a total of K differently watermarked copies of the same multimedia content, these users can simply linearly combine the K signals to produce a colluded version. Since normally no colluder is willing to take more of a risk than any other colluder, the watermarked signals are usually averaged with an equal weight for each user. This averaging reduces the power of each contributing watermark. As the number of colluders increases, the embedded watermark becomes weaker. In fact, the colluded signal can have better perceptual quality in that it can be more similar to the host signal than the watermarked image.

(a)

(b)



(c)



(d)

Fig.13. Colluded Lena images – (a) with β=0.2 for 5 users (b) with β=0.2 for 2 users (c) with β=0.02 for 5 users (d) with β=0.02 for 2 users

With the proposed approaches, as the geometry of each copy is distorted independently (embedding is done in LL band at randomly chosen coefficients), a collusion attack yields a low quality signal. According to Tanmoy Kanti Das et al. [16], for an image of size 256 ×256 or 512× 512, for a successful collusion attack, a large number of watermarked images may be required, depending on the size of the key information. They also state that this is not practical. But it is not true with our schemes. We show that collusion even with only two copies results in disturbing distortions as shown in Fig.13 by marked area and visual quality does not improve when the number of copies is increased. More degradation encounters with increased number of colluders as shown in Fig.13 (a) and (c) where collusion is done with 5 users. High quality colluded image can be obtained only with special software and with substantial computational resources, but this is not feasible. Also, it is observed from our previous work that the embedding strength β has an impact on the collusion strength [17]. Hence, in the proposed work the embedding strength is increased further and is seen that an increase in β from 0.02 to 0.2 produces disturbing distortions in the visual quality of the colluded images as shown in Fig.13 for collusion with 2 users and 5 users.

5. CONCLUSION

In this paper, we have proposed non-blind watermarking schemes that utilize the luminance and chrominance contents for watermarking in the L*a*b* space. It is based on DWT and the watermark is scrambled before embedding. Watermarking is done on the approximation band on selected coefficients decided by the random function. As a result, the watermark is robust to a wide variety of attacks. In the proposed schemes, the PSNRs of the watermarked images are on an average 57dB. The schemes can effectively resist common image processing attacks especially JPEG compression (with a quality factor up to 20), filtering (mean, median, average and Weiner) by a mask of size 3×3, 5×5 and 7×7, blurring, sharpening, histogram equalization and intensity adjustment. Also, it is resistant to geometric attacks like scaling and Gaussian noise with a variance less than 4. After undergoing all these attacks, the extracted watermark is still recognizable. The scheme is superior in the way it resists collusion attacks. The watermark embedding strength and the location is shown to have an impact on the resistance of the proposed schemes to collusion attacks. Also, the scheme can resist collusion even for a minimum of two colluders and with increasing number of colluders, there is much distortion in the visual quality. Both DWTC and DWTLC schemes find their application in image authentication, copy control and content tracking. Future work is to concentrate on the attacks like color grayscale conversion, cropping that have not been considered yet.

REFERENCES

[1] Arvind Kumar Parthasarathy, Subash Kak, 2007, "An Improved Method of Content Based Image Watermarking", IEEE Trans. Broadcasting, Vol. 53, No. 2, pp. 468-479.

[2] Elham Salahi, M. Shahram Moin and Ahmed Salahi, 2008, "A New Visually Imperceptible and Robust Image Watermarking Scheme in the Contourlet Domain". Proc. of Int. Conf. Intelligent Information Hiding and Multimedia Signal Processing: pp. 457-460.

[3] P.S. Huang, C S Chiang, C P Chang and T M Tu, 2005, "Robust Spatial Watermarking Technique for Color Images via Direct Saturation Adjustment". IEEE Proc. on Vision, Image and Signal Processing, Vol. 152, No. 5, pp. 561-574.

[4] Amit Phadikar, Bhupendra Verma and Sanjeev 2007, "Region Splitting Approach to Robust Color Image Watermarking Scheme in the Wavelet Domain". Asian Journal of Information Management, Vol. 1, No.2, pp. 27-42.

[5] Shang-Lin Hsieh, Jh-Jie Jian, I-Ju Tsai and Bin-Yuan Huang. 2008, "Protecting Copyrights of Color Images using a Watermarking Scheme Based on Secret Sharing and Wavelet Transform". Journal of Multimedia, Vol. 3, No. 4, pp. 42-49.

[6] Jiang-Bin Zheng and Sha Feng, 2008, "A Color Image Multi Channel DWT Domain Watermarking Algorithm for Resisting Geometric Attacks". Proc. of Int. Conf. on Machine Learning and Cybernetics, Vol. 2, pp. 1046-1051.

[7] Deyu Hu, Jun Wang, Hong Peng and Xun Wang, December 2008, "A Color Image Watermarking Scheme in the Wavelet Domain based on Support Vector Machine". Proc. of Pacific Asia Workshop on Computational Intelligence and Industrial Application, Vol. 1, pp. 404-407.

[8] Peter Foriš and Dušan Levický, 2009, "Adaptive Digital Image Watermarking Based on Combination of HVS Models". Radio Engineering, Vol. 18, No. 3, pp. 317-323.

[9] Qiujuan Liang and Zhizhong Ding, 2008, "Spread Spectrum Watermark for Color Image Based on Wavelet Tree Structure". Proc. of Int. Conf. on Computer Science and Software Engineering, Vol. 3, pp. 692-695.

[10] P.Ramana Reddy, Munaga, V.N.K.Prasad and D. Sreenivasa Rao, May 2009, "Robust Digital Watermarking of Color Images under Noise attacks". International Journal of Recent Trends in Engineering, Vol.1, No. 1, pp.334-338.

[11] Tao Peining and Eskicioglu, Ahmet M, 2004, "A Robust Multiple Watermarking Scheme in the Discrete Wavelet Transform Domain". Proc. of the SPIE 5601, pp. 133-144.

[12] Rafael C. Gonzalez and Richard Eugene Woods, 2004, "Digital Image Processing", Second Edition.

[13] Tsz Kin Tsui, Xiao-Ping Zhang and Androutsos D, 2008, "Color Image Watermarking Using Multidimensional Fourier Transforms". IEEE Trans. on Information Forensics and Security, Vol. 3, No.1, pp.16 – 28.

[14] USC-SIPI Image Database, available at website: http://sipi.usc.edu/services/database/Database.html.

[15] Shijun Xiang, Hyoung Joong Kim and Jiwu Huang, 2008, "Invariant Image Watermarking based on Statistical Features in the low Frequency Domain". IEEE Trans. on Circuits and Systems for Video Technology, Vol. 18, No.6, pp. 777-790.

[16] Tanmoy Kanti Das, Subhamoy Maitra, and Joydip Mitra, 2005, "Cryptanalysis of Optimal Differential Energy Watermarking (DEW) and a Modified Robust Scheme". IEEE Trans. on Signal Processing, Vol. 53, No. 2, pp. 768-775.

[17] Dejey and R S Rajesh. 2010. An improved Wavelet domain Digital Watermarking for image protection. Int. Journal of Wavelets and Multiresolution Information Processing, Vol.8, No.1, pp. 19-31.