Effect of Weight Factor on The Performance of Hybrid Column Wavelet Transform used for Watermarking under Various Attacks

H. B. Kekre[1], Tanuja Sarode[2], Shachi Natu[3]

[1]MPSTME, Department of Computer Engineering, NMIMS University, Mumbai, India

hbkekre@yahoo.com

[2]Department of Computer Engineering, TSEC, Mumbai University, India

tanuja_0123@yahoo.com

[3]Ph. D. Research Scholar, MPSTME, NMIMS University, Mumbai, India

shachi_natu@yahoo.com

ABSTRACT

Digital image watermarking is aimed at copyright protection of digital images. Strength of embedded watermark plays an important role in robustness and invisibility of watermarking technique. In this paper, effect of two parameters namely, watermark strength and middle frequency coefficients of host image used for embedding watermark is studied. In the given watermarking technique, watermark is normalized before embedding. This reduces the strength of watermark so that there will be minimum possible distortion in watermarked image. However, it has been observed in our work proposed in previous paper that, such embedment responds poorly to various image processing attacks like compression, cropping, resizing, noise addition etc. Hence in this paper, an attempt has been made to increase the strength of embedded watermark by using suitable weight factor so that robustness of watermarking technique proposed in our previous paper is further increased with small acceptable decrease in imperceptibility. Also middle frequency elements of host image selected for embedding watermark are varied by selecting different rows of host such that slowly we move from middle frequency components towards high frequency components. For certain attacks like image cropping, selection of middle frequency coefficients affects the robustness achieved. Increase in weight factor significantly improves the performance of given watermarking technique by more than 50% as proposed in our previous paper where weight factor value was 25.

Keywords

Watermarking, Strength of watermark, Hybrid Wavelet Transform.

Introduction

In today's world due to use of fast growing internet technology, it has become easy to alter or to copy the digital contents. Digital watermarking is one of the popular security mechanisms which prevents illegal replication of digital data and thus provides copyright protection. Image watermarking is related to protection of digital images against tampering by hiding secret information in the form of another image into the images to be protected. It is carried out in two domains: spatial domain and frequency domain. In frequency domain, cover image and watermark are transformed into their frequency coefficients and appropriate coefficients of cover image are selected for hiding watermark coefficients. How much watermark information is to be hidden in which cover image coefficients decides the distortion caused in cover image and resistance of watermarked image to various image processing attacks. The amount of disturbance or alteration caused by watermark in the host medium is referred to as strength of watermark [1]. Thus strength of embedded watermark plays an important role in robustness and imperceptibility of watermarking technique. Generally, watermark strength is kept constant while embedding the watermark. In literature, lot of work has been done to study effect of watermark strength and to optimize the performance of watermarking technique by embedding appropriate watermark strength.

In [2] we proposed hybrid wavelet transform based watermarking technique. In that proposed technique, DKT-DCT wavelet transform generated using Kekre transform and DCT was used. DKT-DCT wavelet transform was applied column wise, row wise and as full transform.

In [2], watermark was first compressed with compression ratio 2.67. This was the maximum compression ratio observed for which image distortion is imperceptible. Watermark was then normalised and then using suitable weight factor, strength of watermark was increased to make it visually imperceptible after embedding it in host image. Selected weight factor was 25. This normalized and weighted watermark was then embedded in middle frequency coefficients. Middle frequency coefficients were selected on trial and error basis and they were selected as coefficients in rows 109 to 132 of 256x256 size transformed host image. Performance of technique was evaluated against various image processing attacks. Selection of weight factor was arbitrarily done.

In this paper, the method of watermarking remains same. However, an attempt is made to improve the performance of column DKT-DCT transform for various attacks by retrying different values of weight factor used to increase the strength of watermark. Also an attempt is made to select different mid frequency regions of host image to embed the watermark thereby replacing host energy by energy of watermark to be embedded. Thus host energy to be replaced by watermark energy is varied by selecting different range of rows from host for embedment. Watermark energy to be embedded is varied by changing the weight factor used to increase the strength of watermark. Thus aim of the work presented in paper is to study effect of weight factor selection and selection of mid frequency elements in host image on performance of various attacks using column DKT-DCT transform. In this paper, weight factor has been selected such that it corresponds to watermark energy embedded in host image to be minimum 60% of middle frequency elements selected for embedment and maximum 140% of middle frequency elements selected for embedment.

RELATED WORK

In [1], Muhammad Ishtiaq, Bushra Sikandar, M. Arfan Jaffar And Aziz Khan proposed a watermarking scheme in which strength selection problem has been solved using efficient swarm intelligence algorithm called Particle Swarm Optimization (PSO). PSO is a global optimization technique with good local search behaviour. The watermarking is performed in the DCT domain on the selected mid-band coefficients. The overall strength of the watermark is maintained above a specified threshold to obtain good robustness.

M. Jaymohan and K. Revathy proposed a hybrid image watermarking technique using fractal theory and wavelet transform in [3]. In their proposed technique, scaling factor value is selected depending on complexity of image portions. Image is partitioned into smooth and complex regions using fractal dimensions. A higher value of embedding strength is selected for complex regions and smaller embedding strength value for smooth regions. This results into imperceptible and robust watermarking technique.

In [4], pixelwise image watermarking proposed by Mauro Barni, Franco Bartolini, and Alessandro Piva is presented in spatial domain. Watermark is embedded by using Human Visual System characteristics to improve robustness and imperceptibility. Watermark strength is modulated according to local image characteristics. This is obtained through a mask which gives pixel by pixel measure of the sensibility of human eye to local image perturbations. Also a sophisticated mechanism derived from DWT coding studies is introduced to take into account several HVS phenomena, such as grey-level sensibility, isofrequency and nonisofrequency masking, noise sensibility around edges.

In [5], M. S. Keerthi, Nair Prithi and M. Jaymohan proposed wavelet domain watermarking technique with varying embedding strength. Since the texture complexity over an image is non-uniform, embedding watermark with same strength, all over the image, may cause distortions in watermarked image. In their proposed method, watermark information is embedded to selected approximation coefficients of host image wavelet coefficients. Wavelet coefficients are divided into four sets and four different strength values are used for each set. Highest strength value is used for the set of largest coefficients of host image; next higher strength value is used for next set of wavelet coefficients and so on. With varying strength value, better robustness and imperceptibility is observed than watermarking techniques proposed by Barni in [4] and by Nafornita in [6].

In [7], Cong Jin, and Shihui Wang proposed a neural network based watermarking technique, in which embedding strength is adaptively selected using neural network according to different textural features and luminance of each 8x8

block of cover image. In [8], Vesna Vuckovic embedded a watermark generated by adding Gaussian noise into grayscale image. Author has tried to find best embedding strength for robust watermarking in spatial and frequency domain, for short as well as longer messages and into whole image or into some of its coefficients.

Shao Ya-fei , Wu Guo-wei, Lin Xing-gang proposed a wavelet based adaptive watermarking algorithm in [9]. In their proposed technique, where to embed the watermark and how much should be the embedding strength is decided adaptively by local image characteristics. Second level of resolution is selected for watermarking. Frequency band with least variance is selected for embedding watermark. Watermark strength is selected based on image neighbourhood characteristics. For textured areas, which normally show high tolerance to modification in coefficients, larger strength value is selected and for smooth areas of image, small strength value is selected.

H. B. Kekre, Tanuja Sarode, Shachi Natu presented a DWT-DCT-SVD based hybrid watermarking method for color images in [10]. In their method, robustness is achieved by applying DCT to specific wavelet sub-bands and then factorizing each quadrant of frequency sub-band using singular value decomposition. Watermark is embedded in host image by modifying singular values of host image. Performance of this technique is then compared by replacing DCT by Walsh in above combination. Walsh results in computationally faster method and acceptable performance. Imperceptibility of method is tested by embedding watermark in HL2, HH2 and HH1 frequency sub-bands. Embedding watermark in HH1 proves to be more robust and imperceptible than using HL2 and HH2 sub-bands. In [11] and [12] Kekre, Sarode, and Natu presented DCT wavelet and Walsh wavelet based watermarking techniques. In [11], DCT wavelet transform of size 256*256 is generated using existing well known orthogonal transform DCT of dimension 128*128 and 2*2. This DCT Wavelet transform is used in combination with the orthogonal transform DCT and SVD to increase the robustness of watermarking. HL2 sub-band is selected for watermark embedding. Performance of this proposed watermarking scheme is evaluated against various image processing attacks like contrast stretching, image cropping, resizing, histogram equalization and Gaussian noise. DCT wavelet transform performs better than their previously proposed DWT-DCT-SVD based watermarking scheme in [10] where Haar functions are used as basis functions for wavelet transform. In [12] Walsh wavelet transform is used that is derived from orthogonal Walsh transform matrices of different sizes. 256*256 Walsh wavelet is generated using 128*128 and 2*2 Walsh transform matrix and then using 64*64 and 4*4Walsh matrix which depicts the resolution of host image taken into consideration. It is supported by DCT and SVD to increase the robustness. Walsh wavelet based technique is then compared with DCT wavelet based method given in [11]. Performance of three techniques is compared against various attacks and they are found to be almost equivalent. However, computationally Walsh wavelet was found preferable over DCT wavelet. Also Walsh wavelet obtained by 64*64 and 4*4 is preferable over DCT wavelet and Walsh wavelet obtained from corresponding orthogonal transform matrix of size 128*128 and 2*2. In [13], other wavelet transforms like Hartley wavelet, Slant wavelet, Real Fourier wavelet and Kekre wavelet were explored by H. B. Kekre, Tanuja Sarode and Shachi Natu. Performance of Slant wavelet and Real Fourier wavelet were proved better for histogram Equalization and Resizing attack than DCT wavelet based watermarking in [11] and Walsh wavelet based watermarking presented in [12].

KEKRE TRANSFORM AND HYBRID WAVELET TRANSFORM

Kekre Transform

Kekre's transform matrix [14] has the advantage that it need not be of size having integer power of 2. It can be of any size NxN. All diagonal and upper diagonal elements of Kekre transform are 1 whereas; all lower diagonal elements except the elements just below the diagonal are zero. Kekre transform matrix of size 5x5 is shown below for example.

1	1	1	1	1
-4	1	1	1	1
0	-3	1	1	1
0	0	-2	1	1
0	0	0	-1	1

Hybrid Wavelet Transform

H. B. Kekre, Tanuja Sarode and Sudeep Thepade introduced the concept of hybrid wavelet transform in [15]. An idea behind use of hybrid wavelet transform is to explore the good properties of two different transforms by combining them into hybrid wavelet transform. Use of hybrid wavelet transforms generated from Discrete Cosine Transform, Discrete Walsh Transform, Discrete Hartley transform and Discrete Kekre transform have been explored by authors very successfully for image compression. Hybrid wavelet transform is also proved better in other image processing applications like image retrieval in [16] and biometrics applications like palm print identification in [17].

PROPOSED TECHNIQUE

In proposed technique, DKT-DCT hybrid wavelet transform is generated using DKT and DCT of size 16x16 each to process host image. Also hybrid DKT-DCT transform of size 128x128 is generated using 32x32 size DKT and 4x4 size DCT matrix to process watermark. Column transform of host and watermark images is taken instead of full transform to reduce computational overhead as well as by noting its robustness as observed in [2] over full transform. Study of effect of

weight factor and selection of mid frequency elements of host is conducted using five color bitmap images of size 256x256 and a color bitmap watermark image of size 128x128. They are shown in Fig. 1.
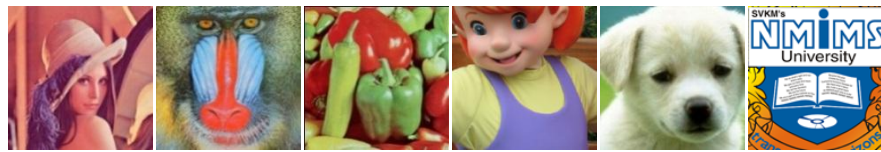
(a) Lena   (b) Mandrill   (c) Peppers   (d) Balls   (e) Puppy   (f) NMIMS

Fig. 1. Five Host images and a watermark image used for experimental work

Embedding Procedure

Step 1. Separate the host image into its Red, Green and Blue channel and apply column DKT_DCT wavelet transform to each channel.

Step 2. Separate the watermark into its Red, Green and Blue channel and apply column DKT_DCT wavelet transform to each channel.

Step 3. Compress the watermark by compression ratio 2.67. This is maximum compression ratio for which image distortion is imperceptible.

Step 4. Normalize and then weight the watermark by suitable weight factor so as it increases the watermark strength and makes it visually imperceptible after embedment into host image. Vary the weight factor such that the watermark energy to be embedded in mid frequency components of host image will vary from 60% of host energy to 140% of host energy.

Once the weight factor corresponding to range of 60% to 140% of host energy are identified, the closest weight factors in multiples of ten are selected for study. E.g. If weight factor 76 corresponds to 60% of host energy and weight factor 113 corresponds to 140% of host energy then weight factors selected are 76, 80, 90, 100, 110 and 113. These weight factors are selected for every chosen range of rows from host image where watermark is to be embedded.

Step 5. Embed this weighted normalized watermark in selected middle frequency band of corresponding channel of host image by replacing host image coefficients there.

Step 6. Take inverse column DKT_DCT wavelet to obtain watermarked image.

Step 7. Calculate average absolute pixel to pixel difference i.e. Mean Absolute Error (MAE) between host and watermarked image to measure the imperceptibility.

Extraction Procedure

The reverse of embedding procedure is followed to recover the watermark from watermarked image. The watermarked image may also be subjected to image processing attack like cropping, compression, resizing or noise attack. Steps of extraction procedure are as follows:

Step 1. Separate the watermarked image into its Red, Green and Blue channel and apply following steps to each channel.

Step 2. Take column DKT_DCT wavelet transform of each channel of watermarked image.

Step 3. Extract the middle frequency coefficients of each plane of watermark from corresponding planes of watermarked image.

Step 4. Weight and then denormalize these coefficients using same weight factor and normalization coefficients used in embedding procedure.

Step 5. Take inverse column DKT_DCT transform of these extracted coefficients to recover the compressed watermark embedded in host image.

Step 6. Calculate average absolute pixel to pixel difference i.e. Mean Absolute Error (MAE) between embedded and

Step 7. extracted watermark to measure the robustness.

RESULTS

Table 1 below show the resultant watermarked images and extracted watermark from them when energy of embedded watermark is 60% of host image coefficients. Rows of host images selected for embedding and weight factors corresponding to 60% energy are also shown in Table 1.

Table 1: Mean Absolute Error between original and extracted watermark when watermark energy is 60% of selected rows of host image with corresponding rows for embedding watermark and weight factor
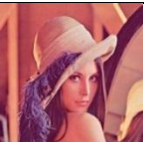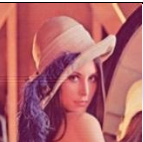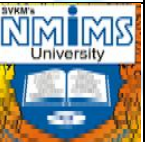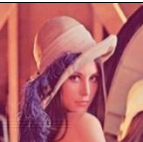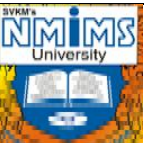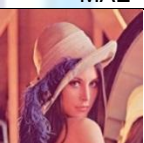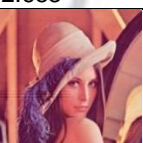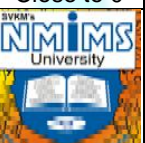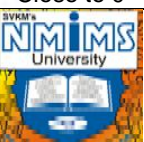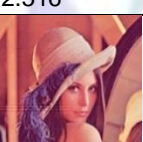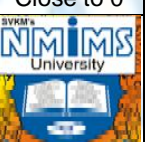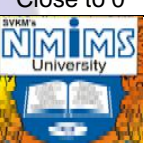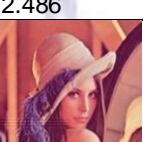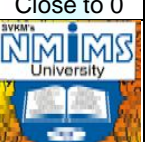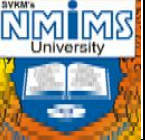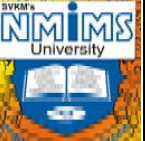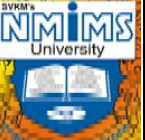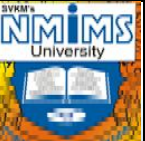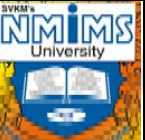
Selected rows for embedding watermark	Weight factor	Host image	Watermarked image	Extracted watermark	Selected rows for embedding watermark	Weight factor	Watermarked image	Extracted watermark
104-127	82				109-132	70		
		MAE= 2.722		Close to 0			MAE=2.333	Close to 0
105-128	80				110-133	67		
		MAE= 2.658		Close to 0			MAE=2.290	Close to 0
106-129	76				111-134	68		
		MAE= 2.516		Close to 0			MAE=2.315	Close to 0
107-130	74				112-133	68		
		MAE= 2.486		Close to 0			MAE=2.331	Close to 0
108-131	72							
		MAE= 2.421		Close to 0				

Table 2 below show the resultant watermarked images and extracted watermark from them when energy of embedded watermark is 140% of host image coefficients. Rows of host images selected for embedding and weight factors corresponding to 140% energy are also shown in Table 2.

Table 2: Mean Absolute Error between original and extracted watermark when watermark energy is 140% of selected rows of host image with corresponding rows for embedding watermark and weight factor

Selected rows for embedding watermark	Weight factor	Host image	Watermark ed image	Extracted watermark	Selected rows for embedding watermark	Weight factor	Watermark ed image	Extracted watermark
104-127	125				109-132	108		
		MAE=3.313		Close to 0			MAE=2.832	Close to 0
105-128	123				110-133	103		
		MAE= 3.248		Close to 0			MAE=2.769	Close to 0
106-129	116.5				111-134	103.5		
		MAE=3.062		Close to 0			MAE=2.788	Close to 0
107-130	113				112-133	104.5		
		MAE= 3.019		Close to 0			MAE=2.813	Close to 0
108-131	110							
		MAE=2.932		Close to 0				

From Table 1 and Table 2, it is observed that as energy of watermark embedded in host image is increased by increasing weight factor, MAE between original and extracted watermark remains close to zero but MAE between host and watermarked image increases.

Performance against various attacks
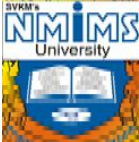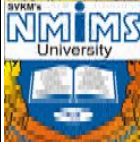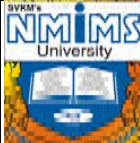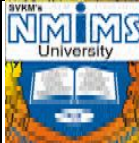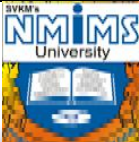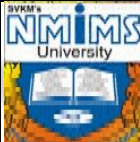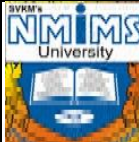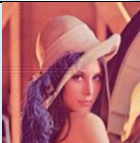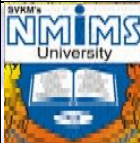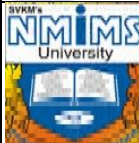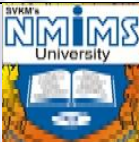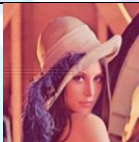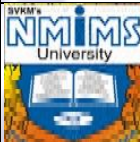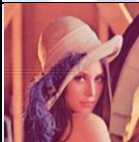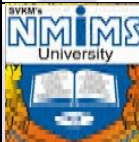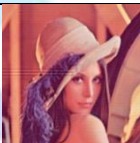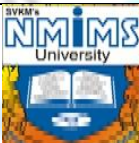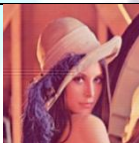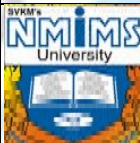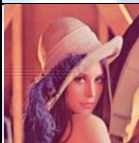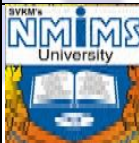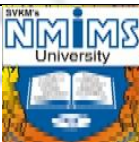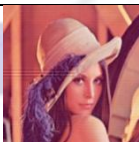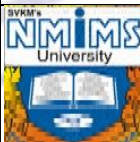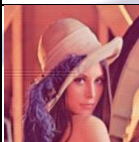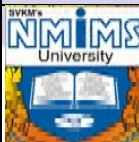
Various attacks performed on watermarked images are compression, cropping, noise addition, and resizing of watermarked image.

In compression attack, watermarked image is compressed using transforms like DCT wavelet (compression ratio 1.95), DCT, DST, Walsh, Modified Haar using compression ratio 1.14 and JPEG compression using 100% quality factor.

Effect of weight factor and mid-frequency components of host image selected for embedding watermark on extracted watermark from various image processing attacks is given below.

Table 3 below shows watermark extracted from compressed watermarked image 'Lena' along with MAE values between original and extracted watermark for compression attack when watermark is embedded in mid frequency elements of host from rows 104 to 127. These resultant images are obtained with varying weight factors and corresponding watermark energy percentage. Energy of embedded watermark is increased from 60% to 140% of mid frequency elements of host image using different weight factors.

Table 3. Resultant watermarked images and extracted watermark from compression attack performed using DCT wavelet, DCT and DST

Weight factor	Watermark energy in % of host energy	DCT Wavelet		DCT		DST	
		Compressed watermarked image	Extracted watermark	Compressed watermarked image	Extracted watermark	Compressed watermarked image	Extracted watermark
82	60						
		2.322	Close to 0	0.734	5.232	0.808	5.399
90	73						
		2.322	Close to 0	0.742	4.873	0.815	5.019
100	90						
		2.322	Close to 0	0.753	4.515	0.825	4.639
105	100						
		2.322	Close to 0	0.758	4.364	0.830	4.479
110	109						
		2.322	Close to 0	0.763	4.228	0.836	4.335
120	130						
		2.322	Close to 0	0.775	3.996	0.846	4.089
125	140						
		2.322	Close to 0	0.781	3.896	0.852	3.982

From Table 3 it can be observed that when host rows selected for watermark embedding are kept fixed and energy of watermark to be embedded is increased by increasing the value of weight factor, MAE between original and extracted watermark remains close to zero using DCT wavelet for compression. For compression using DCT, DST increasing weight factor results in decrease in MAE value between embedded and extracted watermark. Thus increase in weight factor leads to more robustness against DCT based and DST based compression attack.

Table 4 shows extracted watermarks and MAE values between original and extracted watermark for compression attack using transforms Walsh, Modified Haar and JPEG compression when watermark is embedded in middle frequency components of host lying in rows 104 to 127. Table also shows the weight factors used to vary watermark energy percentage from 60 to 140 and corresponding percentage of watermark energy.

Table 4. Resultant watermarked images and extracted watermark from compression attack performed using Walsh, Modified Haar and JPEG compression

Weight factor	Watermark energy in % of host energy	Walsh		Modified Haar		JPEG Compression	
		Compressed watermarked image	Extracted watermark	Compressed watermarked image	Extracted watermark	Compressed watermarked image	Extracted watermark
82	60						
		1.510	14.825	0.830	16.513	0.0051	27.23
90	73						
		1.523	13.821	0.837	15.541	0.00551	26.680
100	90						
		1.541	12.819	0.846	14.564	0.00552	26.117
105	100						
		1.550	12.399	0.850	14.154	0.00552	25.837
110	109						
		1.559	12.022	0.855	13.785	0.000402	25.647
120	130						
		1.578	11.379	0.865	13.510	0.00351	25.454
125	140						
		1.588	11.102	0.870	12.874	0.00702	25.374

Table 4 also shows increased robustness for increased watermark energy embedded in host for all compression attacks i.e. using Walsh, modified Haar. For JPEG compression though the MAE values between embedded and extracted watermark are higher as compared to Walsh and Haar transform based compression, these MAE values also show gradual decrease after increase in watermark energy embedded in middle frequency coefficients of host. Also though the MAE is higher, there is no loss of information except color has been changed with less contents of red color.

Table 5 below shows MAE between original and extracted watermark when embedded watermark energy is 60% of middle frequency components of host energy but the position of embedding watermark is changed from host rows 104-127 to 112-135 for compression attack.
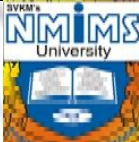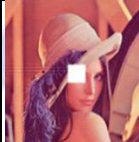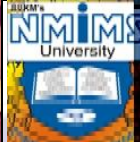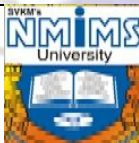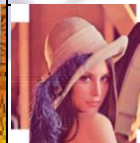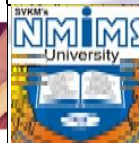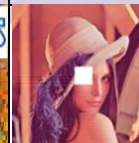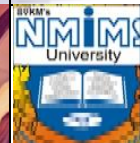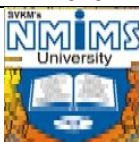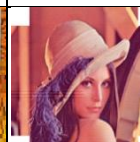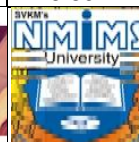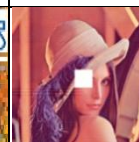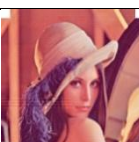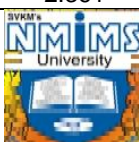
Table 5. MAE between embedded and extracted watermark for compression attack performed using DCT wavelet, DCT, DST, Walsh, Modified Haar and JPEG compression when embedded watermark energy is 60% of embedded rows and varying embedding position
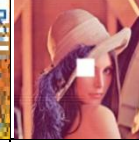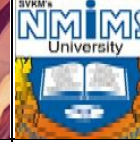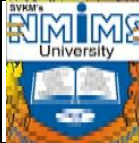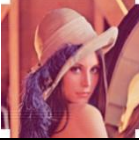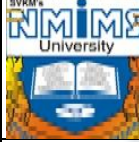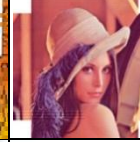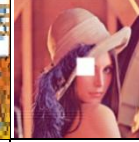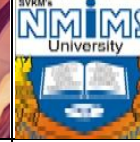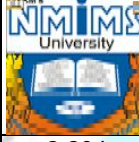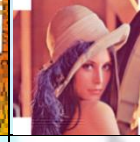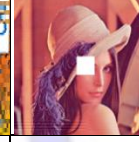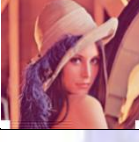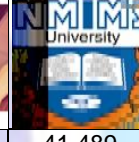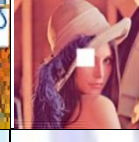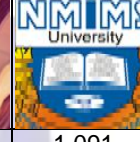
Host rows used for embedding watermark	Weight factor	Watermark energy (% of host energy)	Transform used for Compression Attack					
			DCT Wavelet	DCT	DST	Walsh	Modified Haar	JPEG
104-127	82	60	Close to 0	5.232	5.398	14.82	16.513	27.230
105-128	80	60	Close to 0	5.314	5.534	15.028	19.037	27.916
106-129	76	60	Close to 0	5.415	5.622	14.743	20.909	28.134
107-130	74	60	Close to 0	5.544	5.747	13.82	20.365	28.342
108-131	72	60	Close to 0	5.597	5.837	13.41	20.90	27.844
109-132	70	60	0.783	5.717	5.950	13.538	53.472	28.823
110-133	67	60	3.37	6.019	6.019	12.829	54.470	29.406
111-134	68	60	4.24	6.063	6.213	12.299	53.957	29.167
112-135	68	60	5.68	5.952	6.320	9.219	51.706	29.102

From Table 5, it can be seen that when amount of watermark energy embedded in host image is constant and as we move towards higher frequency component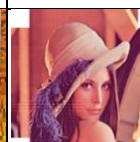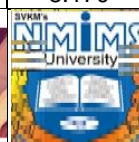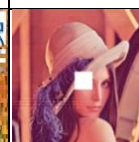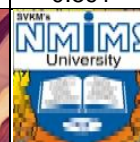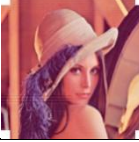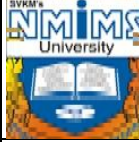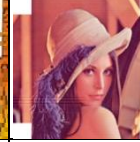s of host image for embedding watermark, MAE between embedded and extracted watermark shows slight increase for compression using DCT Wavelet, DCT, DST, Modified Haar and JPEG compression which means decreased robustness. Only Walsh transform based compression attack shows better robustness as we go on selecting rows of host image containing lower energy components.

Table 6 below shows cropped watermarked images and watermark extracted from it for three types of cropping attacks. These images are obtained by embedding watermark energy that is 60% of middle frequency components of host images and by changing the position of embedment in host image.

Table 6: Watermarked images and extracted watermark for various cropping attacks with different rows of host selected for embedment and weight factor corresponding to 60% energy of embedded rows
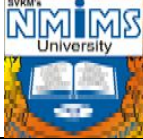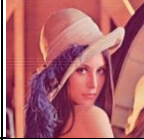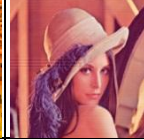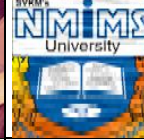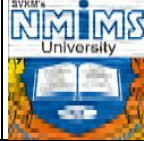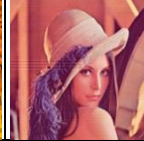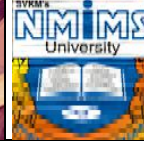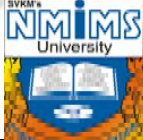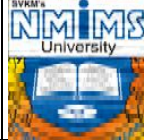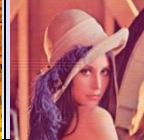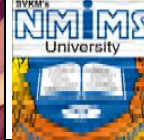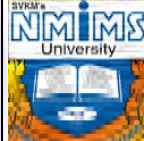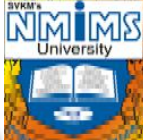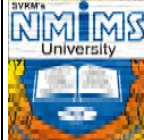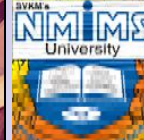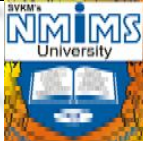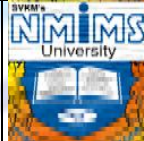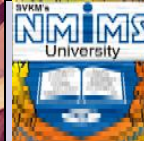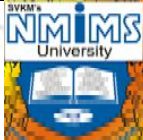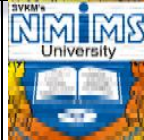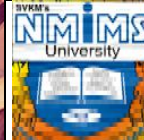
Host rows used for embedding watermark	Weight factor	Watermark energy (% of host energy)	Cropping Attack					
			16x16 crop		32x32 crop		32x32 crop at centre	
			Cropped watermarked image	Extracted watermark	Cropped watermarked image	Extracted watermark	Cropped watermarked image	Extracted watermark
104-127	82	60						
		MAE=		0.987		4.948		18.183
105-128	80	60						
				1.020		6.894		17.659
106-129	76	60						
				2.361		8.170		0.591
107-130	74	60						
				3.179		10.151		0.715

108-131	72	60						
				2.645		11.587		0.663
109-132	70	60						
				2.623		9.716		0.681
110-133	67	60						
				2.275		9.424		0.701
111-134	68	60						
				2.204		42.324		0.968
112-135	68	60						
				19.938		41.489		1.091

For cropping attack, when 16x16 size squares and 32x32 size squares are cropped at four corners of watermarked image, MAE between embedded and extracted watermark is observed to remain same irrespective of scaling factor when host rows selected for embedment are kept fixed. However, when the position of watermark embedment is varied from middle frequency elements towards higher frequency elements, change in MAE between embedded and extracted watermark is observed. For 16x16 cropping attack, this MAE increases slowly for host rows 104-127 to 107-130 selected for embedding watermark. As we go towards higher frequency elements further from rows 108-131 to 111-134, gradual decrease in MAE is observed. After that, this MAE value drastically increases showing reduction in robustness. For 32x32 cropping attack, MAE between embedded and extracted watermark are higher than in 16x16 cropping attack. As we move from middle frequency components towards higher frequency components for embedding watermark, this MAE value initially increases from rows 104-127 of host to 108-131 rows and then slowly decreases till 110-133 rows beyond which it suddenly raises to higher MAE values showing unsuitability of host rows beyond rows 110-133 for embedment. However for 32x32 size square cropped at centre at image, as we move from middle frequency components towards higher frequency components for embedding watermark, initially for rows 104-127 and 105-128 of host, higher MAE values (18.183, 17.659) are observed and then it drastically reduces and shows minor fluctuation for lower rows selected from host. Thus for 32x32 cropping at centre is more robust than 16x16 and 32x32 cropping at corners of image.

Table 7 below shows the result images obtained for Binary distributed run length noise with different run lengths i.e. run length 1 to 10, run length 5 to 50 and run length 10 to 100. These result images are obtained for watermark embedded in host rows 104-127 by varying the percentage of watermark energy embedded using different weight factors.

Table 7. Watermarked images and extracted watermark after adding binary run length noise with different run length

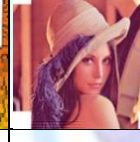| Host rows selected for embedding watermark	Weight factor	Watermark energy (% of host rows energy)	Binary run length noise					
			Run length 1 to 10		Run length 5 to 50		Run length 10 to 100	
			Attacked image	Extracted watermark	Attacked image	Extracted watermark	Attacked image	Extracted watermark
104-127	82	60						
			1	Close to 0	1	13.99	1	13.20
	90	73						
			1	Close to 0	1	12.08	1	12.08
	100	90						
			1	Close to 0	1	11.12	1	11.12
	105	100						
			1	Close to 0	1	11.11	1	12.09
	110	109						
			1	Close to 0	1	10.56	1	10.56
	120	130						
			1	Close to 0	1	9.77	1	9.77
	125	140						
			1	Close to 0	1	8.93	1	9.21

From Table 7 above, it is clearly seen that for binary distributed run length noise with run length 1 to 10, MAE between embedded and extracted watermark remains close to 0 irrespective of watermark energy embedded in host image when it is embedded in the same rows of host image. As we increase the run length of noise added to watermarked image to the range 5 to 50 and 10 to 100, there is significant increase in these MAE values. With increase in weight factor, this MAE decreases. Thus more is the percentage of watermark energy embedded in host rows; more robust is the performance against binary distributed run length noise

When the watermark energy embedded in host is kept same 60% of mid frequency components of host and position of watermark embedding is varied from 104-127 to 112-135, result images obtained from noise attack are shown in Table 8.
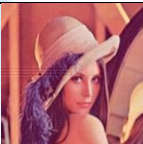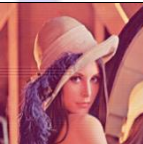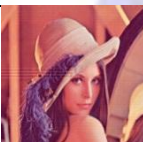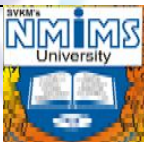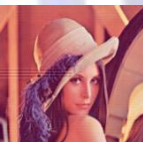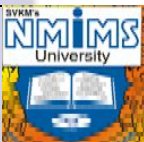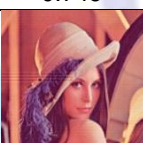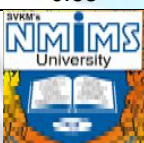
Table 8. Watermarked images and extracted watermarks from Binary run length noise added images with watermark energy 60% of embedded rows and varying embedding positions

Host rows selected for embedding watermark	Binary run length noise					
	Run length 1 to 10		Run length 5 to 50		Run length 10 to 100	
	Attacked image	Extracted watermark	Attacked image	Extracted watermark	Attacked image	Extracted watermark
104-127						
	1	Close to 0	1	14.748	1	13.055
105-128						
	1	Close to 0	1	13.749	1	15.464
106-129						
	1	Close to 0	1	13.800	1	15.232
107-130						
	1	Close to 0	1	14.898	1	15.951
108-131						
	1	Close to 0	1	16.507	1	14.906
109-132						
	1	Close to 0	1	16.264	1	16.847
110-133						
	1	Close to 0	1	17.556	1	17.638
111-134						
	1	Close to 0	1	17.565	1	17.092
112-135						
	1	Close to 0	1	16.194	1	19.415

From Table 8, it can be observed that, changing the position in host image to embed watermark, does not significantly result into increase or decrease in MAE between embedded and extracted watermark. Thus effect on MAE between embedded and extracted watermark is only due to weight factor selected to increase or decrease the embedded energy of watermark.

Table 9 shows Gaussian noise added watermarked image and watermark extracted out of it for varying weight factors with host rows 104-127 selected for embedding watermark. Here weight factors correspond to watermark energy ranging from 60% to 140% of host rows selected for embedding.

Table 9. Watermarked images after adding Gaussian distributed noise and extracted watermark from them with watermark energy ranging from 60% to 140% of host rows selected for embedding watermark.

Weight factor	Watermark energy (% of host rows energy)	Gaussian distributed noise		Weight factor	Watermark energy (% of host rows energy)	Gaussian distributed noise	
		Attacked image	Extracted watermark			Attacked image	Extracted watermark
82	60			110	109		
		0.746	0.82			0.746	0.61
90	73			120	130		
		0.746	0.75			0.746	0.56
100	90			125	140		
		0.746	0.68			0.746	0.54
105	100						
		0.746	0.64				

From Table 9, once again it has been observed that increasing the weight factor and hence the energy of watermark embedded in host image middle frequency elements results in more robustness against Gaussian distributed run length noise attack. Also varying the embedment position does not significantly affect the robustness against attack.

Table 10 shows results for resizing attack of two types: first in which image is enlarged four times of its original size and then reduced to original size again (Type 1) and second in which image is enlarged two times of its original size and then reduced to original size (Type 2).

Table 10. Resultant watermarked images and extracted watermark from Resize Type 1 and Resize Type 2 attack for varying watermark energy from 60% to 140% of host rows

Weight factor	Watermark energy (% of host rows energy)	Resize Type 1 attack		Resize Type 2 attack	
		Attacked image	Extracted watermark	Attacked image	Extracted watermark
82	60				
		1.226	14.308	1.259	14.774
90	73				
		1.231	13.993	1.265	14.452
100	90				
		1.239	13.694	1.272	14.147
105	100				
		1.242	13.574	1.276	14.024
110	109				
		1.246	13.468	1.280	13.916
120	130				
		1.255	13.294	1.289	13.738
125	140				
		1.259	13.222	1.293	13.664

Table 10 indicates decrease in MAE values between embedded and extracted watermark upon increasing the watermark strength i.e. increase in embedded watermark energy and gradual increase in MAE between watermarked and resized watermarked image. Thus robustness increases and imperceptibility slightly decreases on increased strength of watermark.

Comparison with previous work:

In [2], we used column DKT_DCT transform with weight factor 25 and watermark is embedded within rows 109 to 132 of host image. This corresponds to watermark energy which is 3% of middle frequency elements of host in which it is embedded. When performance of watermarking technique with weight factor 25 against various attacks is compared with the work presented in this paper with weight factors corresponding to 60% to 140% of middle frequency components of host image for same rows selected for embedment, better robustness is achieved for most of the attacks. This comparison is shown in following Table 11. Wherever applicable, the percentage reduction in MAE for corresponding weight factor value is also shown in the table.

Table 11. Performance comparison of watermarking for scaling factor 25 and scaling factors 70, 91 and 108 which are corresponding to watermark energy 60%, 100% and 140% of host rows 109-132 selected for embedding

Weight Factor ->		25	70	91	108
Corresponding % energy of Watermark		3.36	60	100	140
MAE between host and Watermarked Image		1.864	2.334	2.603	2.832
MAE between embedded and extracted watermark		Close to 0	Close to 0	Close to 0	Close to 0
DCT wavelet compression	MAE between watermarked and attacked watermarked image	2.300	2.302	2.303	2.305
	MAE between embedded and extracted watermark	0.783	0.783	0.783	0.783
16x16 crop	MAE between watermarked and attacked watermarked image	2.550	2.145	2.145	2.145
	MAE between embedded and extracted watermark	2.623	2.623	2.623	2.623
32x32 crop	MAE between watermarked and attacked watermarked image	7.557	7.557	7.557	7.557
	MAE between embedded and extracted watermark	9.717	9.717	9.717	9.717
32x32 crop center	MAE between watermarked and attacked watermarked image	2.203	2.203	2.203	2.203
	MAE between embedded and extracted watermark	0.681	0.681	0.681	0.681
DCT	MAE between watermarked and attacked watermarked image	0.687	0.718	0.739	0.758
	MAE between embedded and extracted watermark	14.557	5.717	4.681	4.167
	(% reduction in MAE between embedded and extracted watermark)	-	61	68	71
DST	MAE between watermarked and attacked watermarked image	0.762	0.793	0.813	0.831
	MAE between embedded and extracted watermark	15.271	5.950	4.846	4.295
	(% reduction in MAE between embedded and extracted watermark)	-	61	68	72
Walsh	MAE between watermarked and attacked watermarked image	1.441	1.485	1.514	1.539
	MAE between embedded and extracted watermark	33.021	13.539	11.332	10.255
	(% reduction in MAE between embedded and extracted watermark)	-	59	66	69
M Haar	MAE between watermarked and attacked watermarked image	0.810	0.918	0.982	1.037
	MAE between embedded and extracted watermark	78.848	53.472	51.503	50.688
	(% reduction in MAE between embedded and extracted watermark)	-	32	35	36
JPEG Compression	MAE between watermarked and attacked watermarked image	0.011	0.001	0.006	0.007
	MAE between embedded and extracted watermark	98.975	28.824	27.014	26.435
	(% reduction in MAE between embedded and extracted watermark)	-	71	73	73.29
Binary Run length Noise (Run length 1 to 10)	MAE between watermarked and attacked watermarked image	1.000	1.000	1.000	1.000
	MAE between embedded and extracted watermark	0.000	0.000	0.000	0.000
Binary Run length Noise (Run length 5 to 50	MAE between watermarked and attacked watermarked image	1.000	1.000	1.000	1.000
	MAE between embedded and extracted watermark	41.227	16.264	11.924	9.800
	(% reduction in MAE between embedded and extracted watermark)	-	61	71	76
Binary Run length	MAE between watermarked and attacked watermarked image	1.000	1.000	1.000	1.000

Noise (Run length 10 to 100)	MAE between embedded and extracted watermark	41.103	16.848	12.426	11.301
	(% reduction in MAE between embedded and extracted watermark)	-	59	70	72.5
Gaussian Distributed Run Length Noise	MAE between watermarked and attacked watermarked image	0.746	0.746	0.746	0.746
	MAE between embedded and extracted watermark	2.296	0.820	0.631	0.532
	(% reduction in MAE between embedded and extracted watermark)	-	64	73	77
Resize attack (Type 1)	MAE between watermarked and attacked watermarked image	1.200	1.222	1.237	1.251
	MAE between embedded and extracted watermark	24.584	15.113	14.267	13.887
	(% reduction in MAE between embedded and extracted watermark)	-	39	42	44
Resize (Type 2)	MAE between watermarked and attacked watermarked image	1.232	1.255	1.270	1.285
	MAE between embedded and extracted watermark	25.300	15.600	14.735	14.347
	(% reduction in MAE between embedded and extracted watermark)	-	38	42	43

CONCLUSION:

From the work done to study effect of weight factor selection and selection of middle frequency components in host image, we reach to the following conclusion.

As we increase the weight factor and hence the energy of watermark embedded in host image, from 60% of middle frequency elements of host to 140%, the middle frequency components of host image are altered to greater extent. This causes more distortion in host image and MAE between host and watermarked image increases. This leads to less imperceptibility of watermarked image. The MAE between original and extracted watermark remains almost 0 for increased value of weight factor.

For compression using DCT wavelet transform, cropping 16x16 square at four corners, 32x32 squares at four corners and 32x32 square at the centre of host image attacks, MAE between embedded and extracted watermark as well as MAE between watermarked and attacked watermarked image is unaffected by change in weight factor. However, for cropping, selection of middle frequency components gives better robustness than as we move towards high frequency elements.

For compression using DCT, DST, Walsh and Modified Haar and JPEG Compression, significant decrease is observed in MAE between embedded and extracted watermark with slight increase in MAE between watermarked and attacked watermarked image. Thus more robustness is achieved by increasing the weight factor but with small decrease in imperceptibility of watermarking technique.

For binary distributed run length noise with run length 1 to 10, MAE between embedded and extracted watermark remains very close to zero. However, as run length is increased between 5 to 50 and then 10 to 100, significant improvement in robustness is observed. For Gaussian distributed run length noise added to host image, though the MAE between embedded and extracted watermark is less (2.296) for weight factor 25 as observed in [2], it is further reduced to 0.532 with increased weight factor up to 108.

For resizing attack both of type 1 and type 2, better robustness is clearly observed with increased weight factor. Improvement in robustness for all above mentioned attacks are obtained with very little decrease in imperceptibility which is affordable.

REFERENCES

[1] Muhammad Ishtiaq, Bushra Sikandar, M. Arfan Jaffar And Aziz Khan, "Adaptive Watermark Strength Selection Using Particle Swarm Optimization", ICIC Express Letters Icic International 2010, Volume 4, Number 5, October 2010, pp. 1-6.

[2] Dr. H. B. Kekre, Dr. Tanuja Sarode, Shachi Natu, "Robust Watermarking Technique using Hybrid Wavelet Transform Generated from Kekre Transform and Discrete Cosine Transform", International Journal of Scientific and Research Publications, Volume 4, Issue 2, February 2014, pp. 1-13.

[3] M. Jayamohan and K. Revathy, "A hybrid fractal-wavelet digital watermarking technique with localized embedding strength", Communication in Computer and Information Science, Proc. of International Conference on Information Processing, Vol. 292, Part 7, , Springer-Velarge, 2012, pp. 584-591.

[4] Mauro Barni, Franco Bartolini, and Alessandro Piva, "Improved wavelet-based watermarking through pixel-wise masking", IEEE Transactions On Image Processing, Vol. 10, No. 5, May 2001, pp.783-791.

[5] M. S. Keerthi, Nair Prithi and M. Jaymohan, "An improved wavelet domain image watermarking with varying embedding strength", World Congress on Information and Communication Technologies (WICT), 2012, pp. 404-407.

[6] C. Nafornita, "Contributions to digital watermarking of still images in the wavelet transform", Ph. D Thesis, Technical university of Cluj-Napoca, Romania, 2008.

[7] Cong Jin, and Shihui, "Applications of a Neural Network to Estimate Watermark Embedding Strength", Eighth International Workshop on 2007, page 68.

[8] Vesna Vuckovic, "Embedding strength criteria for AWGN Watermark, robust against expected Distortion", Computing and Informatics, Vol. 29, 2010, pp. 357–387.

[9] Shao Ya-fei , Wu Guo-wei, Lin Xing-gang, "A Wavelet Based Adaptive Watermarking Algorithm", 2001, pp. 384-389.

[10] Dr. Kekre H. B. and Thepade Sudeep D., "Image Retrieval using Non-Involutional Orthogonal Kekre's Transform", International Journal of Multidisciplinary Research And Advances in Engineering, IJMRAE, Vol.1, No. I, November 2009, pp. 189-203.

[11] H. B. Kekre, Tanuja Sarode, Sudeep Thepade, "Inception of Hybrid Wavelet Transform using Two Orthogonal Transforms and its use for Image Compression", International Journal of Computer Science and Information Security, vol. 9. No. 6, 2011, pp. 80-87.

[12] H. B. Kekre, Kavita Sonawne, "Query based Image Retrieval using Kekre's, DCT and Hybrid wavelet Transform over 1st and 2nd Moment", International Journal of Computer Applications, Vol. 32, No. 4, 2011, pp. 13-18.

[13] H. B. Kekre, Tanuja Sarode, Rekha Vig, Pranay Arya, Saurabh Bisani, Aashita Irani, "Identification of Multi-spectral Palm prints using Energy Compaction by Hybrid Wavelet", 2012, pp.433-438.

Author's biography with Photo

Dr. H. B. Kekre has received B.E. (Hons.) in Telecomm. Engg. from Jabalpur University in 1958, M.Tech (Industrial Electronics) from IIT Bombay in 1960, M.S.Engg. (Electrical Engg.) from University of Ottawa in 1965 and Ph.D. (System Identification) from IIT Bombay in 1970. He has worked Over 35 years as Faculty of Electrical Engineering and then HOD Computer Science and Engg. at IIT Bombay. After serving IIT for 35 years, he retired in 1995. After retirement from IIT, for 13 years he was working as a professor and head in the department of computer engineering and Vice principal at Thadomal Shahani Engg. College, Mumbai. Now he is senior professor at MPSTME, SVKM's NMIMS University. He has guided 17 Ph.Ds., more than 100 M.E./M.Tech and several B.E. / B.Tech projects, while in IIT and TSEC. His areas of interest are Digital Signal processing, Image Processing and Computer Networking. He has more than 450 papers in National / International Journals and Conferences to his credit. He was Senior Member of IEEE. Presently He is Fellow of IETE, Life Member of ISTE and Senior Member of International Association of Computer Science and Information Technology (IACSIT). Recently fifteen students working under his guidance have received best paper awards. Currently eight research scholars working under his guidance have been awarded Ph. D. by NMIMS (Deemed to be University). At present   seven research scholars are pursuing Ph.D. program under his guidance.

Dr. Tanuja K. Sarode has received M.E. (Computer Engineering) degree from Mumbai University in 2004, Ph.D. from Mukesh Patel School of Technology, Management and Engg. SVKM's NMIMS University, Vile-Parle (W), Mumbai, INDIA. She has more than 11 years of experience in teaching. Currently working as Assistant Professor in Dept. of Computer Engineering at Thadomal Shahani Engineering College, Mumbai. She is member of International Association of Engineers (IAENG) and International Association of Computer Science and Information Technology (IACSIT). Her areas of interest are Image Processing, Signal Processing and Computer Graphics. She has 137 papers in National /International Conferences/journal to her credit.

Ms. Shachi Natu has received M.E. (Computer Engineering) degree from Mumbai University in 2010. Currently pursuing Ph.D. from NMIMS University. She has 08 years of experience in teaching. Currently working as Assistant Professor in Department of Information Technology at Thadomal Shahani Engineering College, Mumbai. Her areas of interest are Image Processing, Database Management Systems and Operating Systems. She has 19 papers in International Conferences/journal to her credit.