

Performance Comparison of Simple Orthogonal Transforms and Wavelet Transforms for Image Steganography

H. B. Kekre
Senior Professor,
SVKM's NMIMS,
Mumbai-56, India

Archana B. Patankar
Associate Professor
TSEC, Bandra,
Mumbai -50, India

Dipali Koshti
Assistant Professor
Fr. CRCE, Bandra,
Mumbai – 50, India

ABSTRACT

There are three major requirements for effective steganography: High embedding capacity, imperceptibility and robustness. It is very difficult to maximally satisfy all these requirements simultaneously. Transform domain techniques for steganography have been proved more robust against various attacks such as image filtering, noise, image cropping, compression etc. Using transform domain techniques it is possible to embed a secret message in different frequency bands of the cover. Embedding in the high frequency creates less impact on the perceivability of the media but provides low robustness to different attacks. In contrast, embedding in lower frequencies helps to withstand many attacks but creates perceptible impact on the media. The proposed image steganography scheme is based on transform domain. In the proposed system we have developed a steganography scheme using different wavelets that provide 56.25% of the embedding capacity as well as robustness against the attacks such as image cropping, addition of noise and changing the brightness of the stego. The paper compares steganography schemes that hide secret information into simple orthogonal transforms such as DCT and Walsh domain against their wavelet versions namely DCT Wavelet and Walsh wavelet domain. Our experimental results show that using wavelet transforms for steganography achieve much better robustness than the normal orthogonal transforms.

General Terms

Image Processing

Keywords

Steganography, Information hiding, DCT wavelet, Walsh wavelet

1. INTRODUCTION

An *image steganographic* scheme is one kind of steganographic systems, where the secret message is hidden in a digital image with some hiding method [1]-[3]. Some one can then use a proper embedding procedure to embed the secret message into the cover image in such a way that it is imperceptible to a human observer. The hidden message can then be recovered using appropriate extraction procedure. The original image is called the cover image and the message-embedded image is called a stego-image. There are a number of steganographic schemes that hide secret message in a digital image. These schemes can be classified according to method of hiding. We have two popular types of hiding methods: spatial domain embedding and transform domain embedding. The Least Significant Bit (LSB) substitution is

the most commonly used spatial domain technique. The basic idea in the LSB is the direct replacement of the LSBs of the cover image with the secret message bits. Hiding images using LSB substitution techniques can be found in [3]-[9]. But this method has low robustness to modifications made to the stego-image such as a low pass filtering and compression. The other type of hiding method is the transform domain techniques [1], [2], [10] which appeared to overcome the robustness and imperceptibility problem found in LSB substitution techniques. The most widely used transforms are Discrete Cosine Transform (DCT) [11], [12] and Walsh transform. Many researchers nowadays use Discrete Wavelet Transform (DWT) [13].

It is possible to generate wavelet from any simple orthogonal transform. For example Walsh Wavelet and DCT wavelet can be generated from orthogonal transforms Walsh and DCT respectively [14]. This paper compares the performance of simple orthogonal transforms with the performance of their wavelet counter parts with respect to robustness and embedding capacity for image steganography.

The main novelties of the proposed paper consist of (i) the extension of a previously published work for hiding secret information in Kekre's wavelet transform [15] by now hiding information in two more wavelet domains Walsh wavelet and DCT wavelet and (ii) Comparing the results of steganography using simple orthogonal transforms (Walsh and DCT) with steganography using wavelet (Walsh wavelet and DCT Wavelet) on the basis of their hiding capacity, imperceptibility and robustness against various attacks. The wavelet transform is applied on full cover image and the secret information is embedded into lower energy blocks of the transformed cover image. Before embedding, the system applies pre-processing step on the secret information. Secret information is first normalized and then embedded in to the cover. This will reduce the embedding error. In a normalized version, the pixel components take on values that span a range between 0.0 and 1.0 instead of integer ranges of [0-255]. Our experimental results show that the steganography using simple orthogonal transforms such as DCT and Walsh achieve 62.5% embedding capacity which is quite good but provides very poor robustness against the attacks such as image cropping, addition of noise and changing the brightness of the stego image, whereas steganography using wavelets provide excellent robustness against the above mentioned attacks at the cost of slightly reduced embedding capacity. Using wavelets we could achieve 56.25% of the embedding capacity of the cover image.

2. PROPOSED SYSTEM

2.1 Embedding into Simple Orthogonal Transform

Simple orthogonal transform (DCT or Walsh) is applied on full cover image. The entire transformed cover image is then divided into 16 non-overlapping blocks. Energy of each block is computed and the secret data is embedded into lesser energy blocks of the transformed cover image [16]. Energy of each block is computed by taking summation of square of each coefficient in the block. The blocks are numbered as shown in Figure 1. It has been observed that for DCT and Walsh transform blocks 16, 15, 11, 14, 13, 10, 7, 8, 4 (lower triangle) are having lesser energy. Figure 1 also shows the highlighted blocks where secret message is embedded.

1	5	9	13
2	6	10	14
3	7	11	15
4	8	12	16

Figure 1: Lesser energy blocks of the cover image (Shaded blocks)

Embedding Algorithm:

The algorithm embeds the secret image into the lowest energy block of the transformed cover image.

1. Apply Walsh/DCT on full cover image.
2. Normalize the secret image to be embedded. This can be done by finding the maximum pixel value of the secret image and then dividing each secret image pixel value by the maximum pixel value.
3. Select lowest energy block of the transformed cover image to embed the secret image.
4. Replace the selected block of the transformed cover by normalized secret image.
5. Apply inverse Walsh/DCT on the modified cover. This gives us the stego image.

Extraction Algorithm:

1. Apply Walsh/DCT on full stego-image.
2. Extract the lowest energy block where we embedded the secret image from the transformed stego-image.
3. De-normalize the extracted data (Multiply each extracted secret image value by its maximum pixel value). This gives us the recovered secret image.

2.2 Embedding into Wavelet Domain

In [14] the algorithm of generating wavelet from any orthogonal transform is presented. From any $N \times N$ orthogonal transform T , we can generate wavelet transform matrix of size $N^2 \times N^2$. For example, from orthogonal transform T of size 5×5 , we can generate corresponding wavelet transform matrix of size 25×25 . In general $M \times M$ wavelet transform matrix can be generated from $N \times N$ orthogonal basic transform T such that $M = N^2$. The following section illustrates the procedure of generating Walsh wavelet from Walsh transform.

2.2.1 Generating Wavelet from Simple Orthogonal Transform

The first step of the algorithm is to generate wavelet from simple orthogonal transform. The procedure of generating Walsh wavelet from simple Walsh transform is discussed in detail in [14]. Consider 4×4 Walsh transform matrix shown in Figure 2. Procedure of generating 16×16 Walsh transform from 4×4 Walsh transform is illustrated in Figure 3.

1	1	1	1
1	1	-1	-1
1	-1	-1	1
1	-1	1	-1

Figure 2: 4×4 Walsh Transform Matrix

	1 st column of W_4 Repeated $N=4$ times	2 nd column of W_4 repeated $N=4$ times	3 rd column of W_4 repeated $N=4$ times	4 th column of W_4 repeated $N=4$ times
1 to 4 rows	1 1 1 1	1 1 1 1	1 1 1 1	1 1 1 1
	1 1 1 1	1 1 1 1	-1 -1 -1 -1	-1 -1 -1 -1
	1 1 1 1	-1 -1 -1 -1	-1 -1 -1 -1	1 1 1 1
	1 1 1 1	-1 -1 -1 -1	1 1 1 1	-1 -1 -1 -1
5 to 8 rows	1 1 -1 -1	0 0 0 0	0 0 0 0	0 0 0 0
	0 0 0 0	1 1 -1 -1	0 0 0 0	0 0 0 0
	0 0 0 0	0 0 0 0	1 1 -1 -1	0 0 0 0
	0 0 0 0	0 0 0 0	0 0 0 0	1 1 -1 -1
9 to 12 rows	1 -1 -1 1	0 0 0 0	0 0 0 0	0 0 0 0
	0 0 0 0	1 -1 -1 1	0 0 0 0	0 0 0 0
	0 0 0 0	0 0 0 0	1 -1 -1 1	0 0 0 0
	0 0 0 0	0 0 0 0	0 0 0 0	1 -1 -1 1
13 to 16 rows	1 -1 1 -1	0 0 0 0	0 0 0 0	0 0 0 0
	0 0 0 0	1 -1 1 -1	0 0 0 0	0 0 0 0
	0 0 0 0	0 0 0 0	1 -1 1 -1	0 0 0 0
	0 0 0 0	0 0 0 0	0 0 0 0	1 -1 1 -1

Figure 3: Generator of 16×16 Walsh wavelet transform from 4×4 Walsh transform

For 4x4 Walsh transform, first 4 rows of Walsh wavelet transform matrix is generated by repeating every column of Walsh transform 4 times. To generate next four rows i.e. row 5 to 8 second row of Walsh transform is used. Similarly to generate next four rows, 3rd row of Walsh transform is used. And to generate last four rows, last row of Walsh transform is used. Similar procedure can be used to generate DCT wavelet from DCT.

2.2.2 Applying Wavelet Transform on 2D Image

Any wavelet transform [WLT] on 2D image of size NxN is given by,

$$[F] = [WLT] [f] [WLT]^T$$

Where $[WLT]^T$ indicates transpose of [WLT]

The inverse is computed as follows:

First diagonal matrix [D] is computed,

$$[D] = [WLT] [WLT]^T$$

Figure 4 shows the diagonal matrix.

D ₁	0	0	0	0	0
0	D ₂	0	0	0	0
0	0	D ₃	0	0	0
0	0	0	...	0	0
0	0	0	0	...	0
0	0	0	0	0	D _N

Figure 4: Diagonal matrix

Inverse is calculated as

$$[f] = [WLT]^T [F_{ij} / D_{ij}] [WLT]$$

Where $D_{ij} = D_i * D_j$; $1 \leq i \leq N$ and $1 \leq j \leq N$

2.2.3 Selection of Blocks for Embedding Data in Wavelet Domain

The block selection technique for embedding secret data used in section 2.1 is applied here. It has been observed that for both Walsh and DCT wavelets blocks 16, 15, 11, 12, 7, 8, 10, 14 and (3 or 6) are lesser energy blocks. Figure 5 shows the blocks where secret message is embedded.

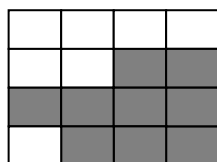


Figure 5: Lesser energy blocks of the cover transformed using Walshlet

2.2.4 Embedding in Wavelet Domain

The algorithm for embedding data into Walsh wavelet domain using Normalization technique is same as that of for KWT as discussed [15]. The only difference is the Walsh wavelet matrix of size C X C is generated from $\sqrt{C} \times \sqrt{C}$ Walsh

transform matrix where as in case of KWT, the KWT matrix of size C X C was generated from Kekre's Transform matrix of size $C/2 \times C/2$

Embedding Algorithm

1. Get the size of the Cover Image (say C X C).
2. Generate the wavelet transform (DCT wavelet or Walsh wavelet) of size C X C from $\sqrt{C} \times \sqrt{C}$ simple orthogonal transform matrix (DCT or Walsh). For example if cover image is of size 256x256 then Walsh wavelet is generated from 64x64 Walsh transform.
3. Apply Wavelet transform on full cover image.
4. Normalize the secret image. This can be done by finding the maximum pixel value of the secret image and then dividing each value of the secret image by its maximum value. Select lowest energy block of the transformed cover image to embed the secret image.
5. Replace the coefficients of the selected block of the transformed cover by normalized secret image.
6. Apply inverse Wavelet transform on the modified cover. This gives us the stego image.

Extraction Algorithm

1. Apply Wavelet transform on full stego-image.
2. Extract the lowest energy block where we embedded the secret image from the transformed stego-image.
3. De-normalize the extracted data (Multiply each value of the extracted secret data by its maximum value). This gives us recovered secret image.

3. RESULTS AND DISCUSSION

3.1 Comparing Embedding Capacity

Our experimental results show that using simple orthogonal transforms i.e. using Walsh and DCT transform achieve 62.5 % embedding capacity. Total seven secret images were embedded into the cover image of size 256 x 256. Figure 6 shows the secret images that were embedded into the cover image.

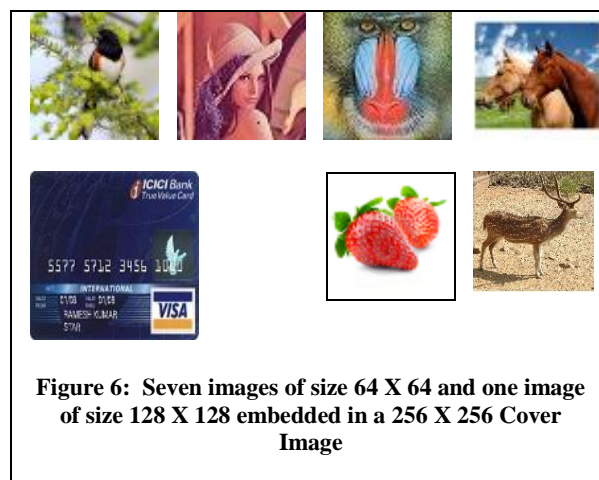


Figure 6: Seven images of size 64 X 64 and one image of size 128 X 128 embedded in a 256 X 256 Cover Image

For Walsh wavelet and DCT wavelet data is embedded into blocks 16,15,11,12,7,8,10,14 and 3 as illustrated in Figure 7. Total six images were embedded (Five of size 64x64 and one of size 128x128) thus achieving 56.25% embedding capacity.



Figure 7: Six secret images embedded into cover (Embedding capacity 56.25%)

Table I - Results obtained from Embedding into DCT, Walsh, DCT Wavelet and Walsh wavelet

Cover	DCT		Walsh		DCT wavelet		Walsh wavelet	
	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE
Rose	53.21	0.31	36.08	16.02	43.53	2.88	41.65	4.44
YellowLily	45.01	2.04	33.96	26.07	42.08	4.02	39.27	7.68
Horse	41.18	4.94	31.23	48.91	38.29	9.63	34.73	21.86
Nature	43.96	2.61	34.45	23.31	39.07	8.05	37.40	11.83
Temple	39.09	8.00	30.18	62.37	35.34	18.97	32.45	36.98
American Goldfinch	36.80	13.57	30.75	54.61	35.45	18.52	32.66	35.22
Ganapati	40.28	6.09	31.47	46.33	38.24	9.73	36.04	16.17
Puppy	35.63	17.78	32.50	36.56	35.33	19.05	34.39	23.69
PolarBear	33.21	30.99	32.08	40.27	33.33	30.16	32.97	32.80
Fern	33.64	28.08	30.86	53.82	33.02	32.40	31.80	42.90
Average	40.20	11.44	32.35	40.82	37.36	15.34	35.33	23.35

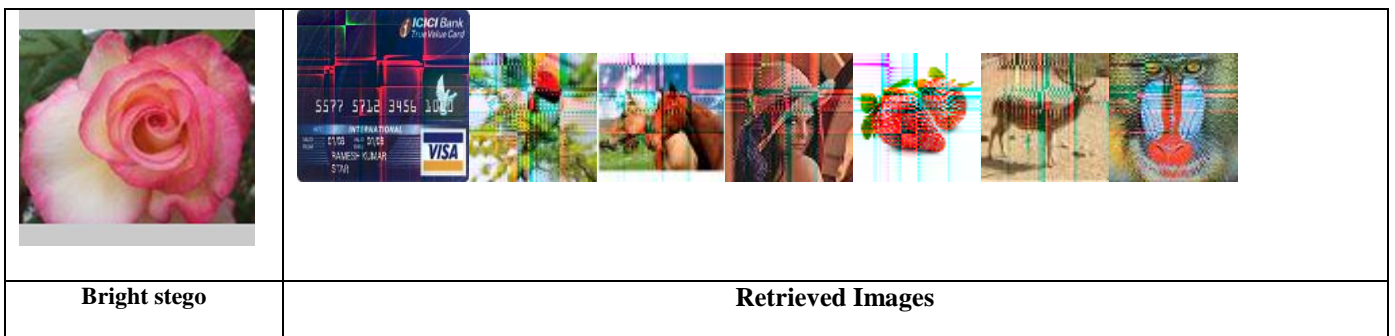
3.2 Testing for Robustness

Three types of attacks were applied on the stego image. (1) Changing the brightness of the stego (ii) Cropping the stego (iii) Adding salt and pepper noise to the stego. Our experimental results show that stego generated

from embedding into normal orthogonal transforms such as DCT and Walsh do not withstand these attacks. Figure 8, 9 and 10 shows the effect of applying all three attacks on the stego generated from normal DCT transform.

3.2.1 Testing Against Various Attacks for DCT

3.2.1.1 Testing for brightness attack



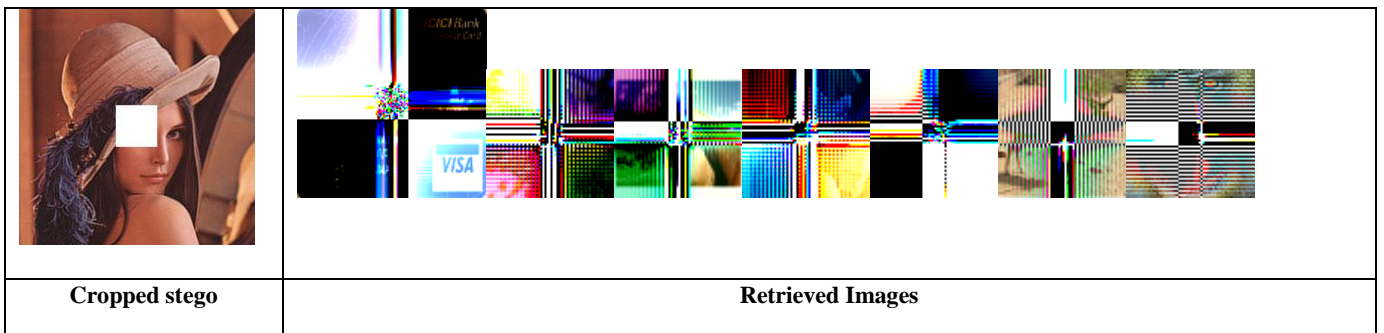
Brightness increased by 10



Brightness increased by 20

Figure 8: Effect of brightness attack on stego generated using DCT

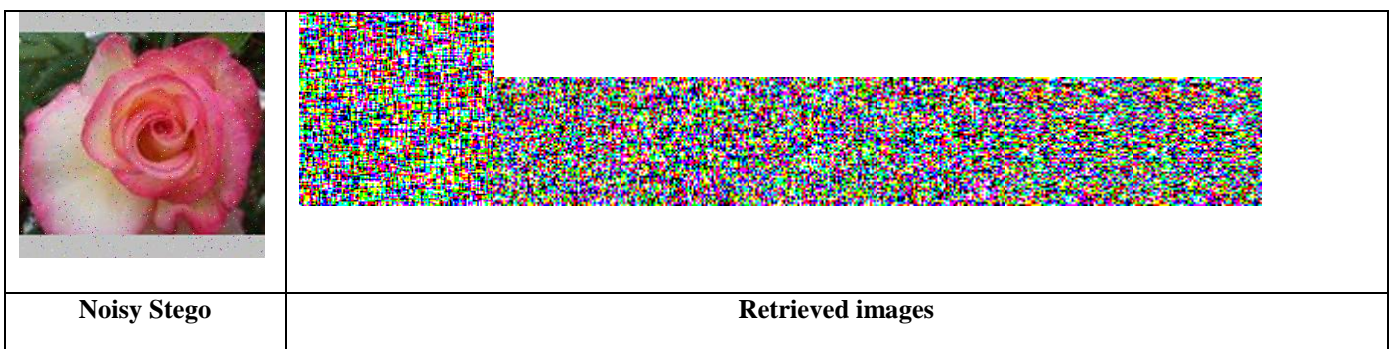
3.2.1.2 Testing against cropping attack



Cropped by 3%

Figure 9: Effect of cropping the stego image generated by using DCT

3.2.1.3 Testing Against Noise Attack



0.1 % noise has been added

Figure 10: Effect of cropping the stego image generated by using DCT


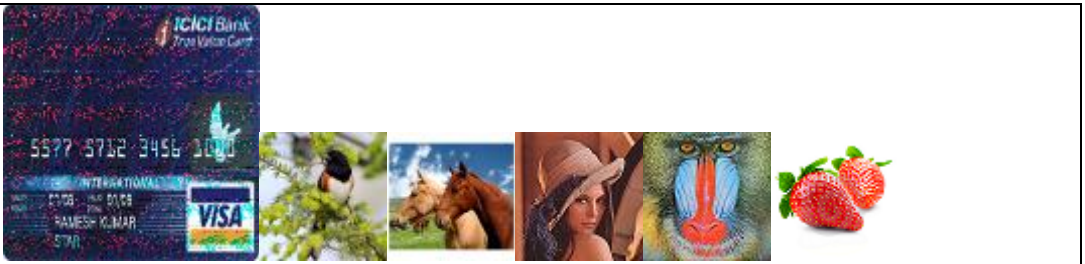
3.2.2 Testing against various attacks for DCT wavelet

Figure 11, Figure 12 and Figure 13 shows the results of applying brightness, cropping and noise attack on the stego generated by using DCT wavelet respectively.

For each retrieved image, retrieval Accuracy (RA) values are given. If RA is 100 means image is retrieved 100%. RA is measured as,

$$RA = \frac{\text{No. of correct bytes}}{\text{Total No. of bytes in actual data}} * 100$$



3.2.2.1 Testing Against Brightness Attack

	 <p>RA=75.27 RA = 100 RA = 100 RA=100 RA=100 RA=100</p>
<p>Bright stego</p>	<p>Retrieved images</p>

Brightness increased by 50

Figure 11: Effect of increasing the brightness of the stego generated from DCT wavelet



3.2.2.2 Testing Against Cropping Attack

	 <p>RA=75.27 RA = 100 RA = 100 RA=100 RA=100 RA=100</p>
<p>Bright stego</p>	<p>Retrieved images</p>

Cropped by 10%

Figure 12: Effect of cropping the stego generated from DCT wavelet

3.2.2.3 Effect of Noise Attack

	 <p>RA=75.27 RA = 100 RA = 100 RA=100 RA=100 RA=100</p>
<p>Noisy stego</p>	<p>Retrieved images</p>

40% noise has been added

Figure 13: Effect of cropping the stego generated by DCT wavelet

Table III: Comparison of DCT Wavelet and Walsh wavelet against brightness attack

Brightness increased by	RA for Card.bmp	
	DCT wavelet	Walsh Wavelet
30	89.71	90.48
50	75.27	79.92
70	46.42	63.41
100	35.32	53.64
120	28.89	47.72

Table IV: Comparison of DCT Wavelet and Walsh wavelet against cropping attack

% of cropping	RA for Card.bmp	
	DCT wavelet	Walsh Wavelet
3	93.77	94.44
5	90.67	92.23
10	86.40	87.58
20	74.72	78.86

Table IV: Comparison of DCT Wavelet and Walsh wavelet against salt and pepper noise attack

% of Noise added	RA for Card.bmp	
	DCT wavelet	Walsh Wavelet
10	9.93	10.54
20	1.45	2.32
40	0.45	1.02
50	0.48	0.77

Table III, IV and V compares the results of DCT wavelet and Walsh wavelet for various attacks. Our experimental results clearly show that steganography using DCT wavelet provides more robustness against the above mentioned three attacks (brightness, cropping and noise attack) than the simple DCT. For a wavelet, only the image that is embedded into fourth quadrant (card.bmp) is not retrieved fully. This is because embedding in high frequency (blocks with lower energies) creates less impact on the perceivability of the media but provides low robustness to different attacks. Rest all five images that are embedded into middle frequency band are retrieved fully with RA = 100. Figure 13 shows that if we add noise to the stego generated from DCT wavelet then the card.bmp cannot be retrieved but rest five images can be retrieved successfully.

4. CONCLUSION

This paper proposes a novel and robust image steganography technique using wavelets. DCT wavelet and Walsh wavelet are generated from DCT and Walsh transform respectively. Image steganography using DCT wavelet and Walsh wavelet have been implemented. The paper also compress the results of simple DCT and Walsh transform with their wavelet counter parts DCT wavelet and Walsh Wavelet respectively. Our experimental results prove that steganography using DCT and Walsh achieve 62.5% embedding capacity but provide very poor robustness to attacks such as changing the brightness of the stego, cropping the stego and adding noise to

the stego. On the other hand steganography using DCT wavelet and Walsh wavelet achieve 56.25% embedding capacity which is slightly lesser than the DCT and Walsh transform but provide excellent robustness against the above mentioned three attacks. Thus steganography using wavelet provides excellent robustness at the cost of slightly reduced embedding capacity. The proposed method provides a good balance of imperceptibility, embedding capacity and robustness for the application where robustness is essential.

5. REFERENCES

- [1] Chin-Chen Chang, Tung-Shou Chen, Hsien-Chu Hsia, "An Effective Image Steganographic Scheme Based on Wavelet Transformation and Pattern-Based Modification," *iccnmc*, pp.450, 2003 International Conference on Computer Networks and Mobile Computing (ICCNMC'03), 2003. .
- [2] R.O.EI Safy, H.H. Zayed and A. EI Dessouki, "An Adaptive Steganographic Technique Based on Integer Wavelet Transform," International Conference on Networking and Media Convergence, 2009 (ICNM 2009) on 24-25 March.
- [3] Wu, H.-C.; Wu, N.-I.; Tsai, C.-S.; Hwang, M.-S ,” Image steganographic scheme based on pixel-value differencing and LSB replacement methods,” *Vision, Image and Signal Processing*, IEE Proceedings - Volume 152, Issue 5, 7 Oct. 2005.
- [4] C.K Chan and L.M Cheng,” Hiding data in images by simple LSB substitution,” *Pattern Recognition*, pp. 469-474, Mar. 2004.
- [5] Wu, H.-C.; Wu, N.-I.; Tsai, C.-S.; Hwang, M.-S ,” Image steganographic scheme based on pixel-value differencing and LSB replacement methods,” *Vision, Image and Signal Processing*, IEE Proceedings - Volume 152, Issue 5, 7 Oct. 2005.
- [6] C.K Chan and L.M Cheng ,” Hiding data in images by simple LSB substitution ,” *Pattern Recognition* , pp. 469-474, Mar. 2004.
- [7] Dr. H. B. Kekre, Ms. Archana Athawale and Ms. Pallavi N. Halarnkar, “Increased Capacity of Information Hiding in LSBs Method for Text and Image”, *International Journal of Electrical, Computer and Systems Engineering*, Volume 2 Number 4. <http://www.waset.org/ijecse/v2.html>.
- [8] Dr. H. B. Kekre, Ms. Archana Athawale, “Information Hiding using LSB Technique with Increased Capacity” *International Journal of Cryptography and Security*, Vol-I, No.2, Oct-2008
- [9] Dr. H. B. Kekre, Ms. Archana Athawale and Ms. Pallavi N. Halarnkar, “Polynomial Transformation To Improve Capacity Of Cover Image For Information Hiding In Multiple LSB’s ”, *International Journal of Engineering Research and Industrial Applications (IJERIA)*, Ascent Publications, Volume II, March 2009, Pune.
- [10] Faisal Alturki , Russell Mersereau, “ Secure Blind Image Staganographic Technique using Discrete Fourier Transformation”, *Image Processing*, 2001, Proceedings 2001 International Conference Volume : 2.
- [11] Dr. H. B. Kekre, Ms. Archana Athawale and Ms. Pallavi N. Halarnkar, “Increased Capacity and High Security for

Embedding Secret Message in Transform Domain using Discrete Cosine Transform”, Accepted in Technopath.

- [12] Dr. H. B. Kekre, Ms. Archana Athawale, Ms. Pallavi N. Halarnkar and Mr. Varun Banura, “Performance Comparison of DCT and Walsh Transform for Steganography”, Accepted for ICWET
- [13] Radomir S. Stankovi and Bogdan J. Falkowski, “ The Haar Wavelet Transform : Its status and Achievements,” Computer and Electrical Engineering, Volume 29 , Issue 1, January 2003, Pages 25-44
- [14] Dr. H.B. Kekre, Ms. Archana Athawale and Ms. Dipali Sadavarti, “Algorithm to Generate Wavelet Transform from an Orthogonal Transform” , International Journal

Of Image Processing (IJIP), Volume (4): Issue (4) 444,2009

- [15] Dr. H.B. Kekre , Ms. Archana Athawale and Ms. Dipali Sadavarti ,” Algorithm to Generate Kekre’s Wavelet Transform from Kekre’s Transform”, International Journal of Engineering Science and Technology Vol. 2(5), 2010, 756-767,2009.
- [16] Dr. H.B. Kekre, Ms. Archana Athawale and Dipali Sadavarti,”A Novel Steganographic Scheme Using Discrete Sine Transform based upon energy distribution”, International conference on contours of computing technology, Thinkquest-2010, held on 13th, 14th March, 2010, Mumbai.