International Journal of Engineering Research and Development
e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 10, Issue 12 (December 2014), PP.75-92

Robust Watermarking Using Hybrid Transform of DCT, Haar and Walsh and SVD

Dr. H. B. Kekre[1], Dr. Tanuja Sarode[2], Shachi Natu[3]
[1]*Senior Professor, Computer Engg. Dept., MPSTME, Vileparle, Mumbai, India.*
[2]*Associate Professor, Computer Dept. TSEC, Bandra, Mumbai, India.*
[3]*Ph. D. Research Scholar, MPSTME, Vileparle, Mumbai, India.*

Abstract:- In this paper a novel approach of watermarking using hybrid transform and SVD is proposed. Hybrid transform is generated from existing orthogonal transforms of different sizes by taking their kronecker product. DCT, Walsh, and Haar transforms are used to generate the hybrid transforms DCT-Walsh, Walsh-DCT, DCT-Haar, Haar-DCT, Walsh-Haar andHaar-Walsh. Each hybrid transform is applied column wise/row wise on host. Singular Value Decomposition of watermark is obtained and first few singular values of watermark are embedded in middle frequency band of hybrid column/row transformed host. Robustness of proposed approach is evaluated against image compression, cropping, noise addition, image resizing and histogram equalization attack. Performance of hybrid transform shows improvement against compression attack by 59%, against noise addition by 70% and against resizing by 32-56% when compared to hybrid wavelet transforms.

Keywords:- Watermarking, Singular Value Decomposition, Hybrid transform, Kronecker product, Hybrid wavelet transform

I. INTRODUCTION

Due to use of internet technology, vast amount of information is generated with a single click. Security of this information is equally important. Usually availability of various tools makes distribution and manipulation of digital information very easy. This may lead to claiming the digital information by someone else other than owner. To avoid this, some technique is required wherein the information of owner can be embedded in the digital information to be transmitted thus preventing illegal claim of ownership or can detect any alterations done in the digital information. Watermarking fulfils this need. Different types of information like identity of owner, logo of company etc. can be embedded in the information to be protected. The information to be protected is called host or cover and the secret information embedded in it is called as watermark. Depending on type of cover, watermarking can be classified as digital image watermarking, audio and video watermarking. In the proposed work focus is on watermarking of digital images. Depending on how the watermark is embedded in image, it is classified as spatial domain and frequency domain watermarking. Spatial domain watermarking directly deals with pixel intensities of image. Frequency domain watermarking first converts image into another form i.e. its frequency representation using transformation techniques and then changes those frequency coefficients in such a way that hidden watermark goes unnoticeable with host. Some more classifications of watermarking include visible and invisible watermarking. As the name suggests it either reveals or hides the existence of watermark in host image depending on the purpose for which it is used. Robust and fragile watermarking is yet another category of image watermarking. In robust watermarking, any change in the host will try to prevent destruction of hidden watermark. Thus attacker cannot easily change or remove hidden watermark to change the ownership information. In fragile watermarking, small change to image information will easily damage the hidden watermark thereby detecting the unauthorised changes in contents of host. Varieties of watermarking techniques available in literature are overviewed in the next section.

II. REVIEW OF LITERATURE

In literature many spatial domain techniques were initially introduced to hide the watermark. Though spatial domain techniques are not as robust as frequency domain techniques, due to their simplicity they are still attracting the researchers. Some such spatial domain techniques have been presented in [1], [2], [3] and [4] where LSB of host is used to hide MSB of watermark. To improve the robustness, instead of using LSB, 3rd or 4th LSB are preferred to hide the watermark. Also operations like shifting the watermark bits or embedding watermark bits multiple times at different positions in host are proposed.

To have robust watermarking where watermarks can survive the attacks on digital contents, we need to move to frequency domain watermarking. Transforms like DCT [5], [6], [7], Discrete wavelet transforms (DWT) [8], [9], [10], Singular Value Decomposition [11], [12] are some of the popularly used transformation techniques. Wavelet packet transform is also efficiently used for watermarking by Bhatnagar et al. in [13]. Using more than one transform has also shown a positive effect on robustness. Some popular pairs of such multiple transforms are DWT-DCT [14], DWT-SVD [15], DCT-SVD [16], DWT-DCT-SVD [17] etc.

Cox [18] first introduced a watermarking using DCT. Piva et al. proposed watermarking using DCT in [19] in which, a DCT domain watermarking of colour images is presented, which exploits the characteristics of the human visual system and the correlation between the RGB image channels.Bedi et al. proposed a SVD and DCT_DWT watermarking technique in [20]. The middle band DCT coefficients are chosen to achieve high robustness against JPEG compression. Robustness against other attacks is achieved by taking DWT of the DCT coefficients and the lowest frequency LL band of DWT is chosen for insertion. Chandra Mohan and Srinivas Kumar presented a SVD based watermarking method in which watermark embedding is carried out in left singular matrix U and diagonal matrix D [21]. Watermark image is embedded in the D component using Dither quantization. A copy of the watermark is embedded in the columns of U matrix using comparison of the coefficients of U matrix with respect to the watermark image. If extraction of watermark from D matrix is not complete, there is a fair amount of probability that it can be extracted from U matrix.

Rahman proposed a DWT-DCT-SVD based watermarking method in [22]. In their watermarking method, theoriginal image is rearranged using zigzag sequence and DWT is applied on rearranged image. Then DCT andSVD are applied on all high bands LH, HL and HH. Watermark is embedded by modifying the singularvalues of these bands. One more DWT-SVD based watermarking algorithm is proposed by Erkan Yavuz and Ziya Telatar. In their method [23], third level decomposition of host image is obtained. LL and HL sub bands obtained through this decomposition are used to embed singular values of watermark. In addition, components of U matrix of watermark are embedded into LH and HH sub band. While extracting, first the similarity of extracted U components are checked with the original one. If they are found similar, watermark is constructed by using extracted singular values and original U and V matrices of the watermark.

Kekre, Tanuja and Shachi presented a DWT-DCT-SVD based hybrid watermarking method for colour images in [24]. 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. In [25], 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. In [26] 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 [25]. In [27], other wavelet transforms like Hartley wavelet, Slant wavelet, Real Fourier wavelet and Kekre wavelet were explored by Kekre, Tanuja and Shachi. Performance of Slant wavelet and Real Fourier wavelet were proved better for histogram Equalization and Resizing attack than DCT wavelet based watermarking in [25] and Walsh wavelet based watermarking presented in [26].

III. HYBRID TRANSFORM AND SVD

Hybrid transform is generated by taking kronecker product of two different orthogonal transforms of different sizes. For example, DCT-Walsh hybrid transform is generated using DCT and Walsh transform matrix. DCT-Walsh hybrid transform matrix of size say 256x256 can be generated using DCT matrix of size 128x128 and Walsh matrix of size 2x2. Thus (128, 2) is one possible pair of component matrix size. Similarly other possible pairs are (64, 4), (32, 8), (16, 16), (8, 32) (4, 64) and (2,128). It comprises of the good characteristics of both the component transforms and hence is expected to shoe better performance than individual component transform. In the proposed approach component transforms of size 16x16 each is used to generate 256x256 hybrid transform matrix.

Using singular value decomposition, any real matrix A can be decomposed into a product of three matrices U, S and V as A=USVT, where U and V are orthogonal matrices and S is diagonal matrix. If A is mxn matrix, U is mxm orthonormal matrix whose columns are called as left singular vectors of A and V is nxn orthonormal matrix whose columns are called right singular vectors of A. Some properties of SVD which make it useful in image processing are:

- The singular values are unique for a given matrix.
- The rank of matrix A is equal to its nonzero singular values. In many applications, the singular values of a matrix decrease quickly with increasing rank. This property allows us to reduce the noise or compress the matrix data by eliminating the small singular values or the higher ranks [28].

- The singular values of an image have very good stability i.e. when a small perturbation is added to an image; its singular values don't change significantly [29].

IV. PROPOSED METHOD

In the proposed method, a hybrid watermarking approach using SVD and hybrid transform is proposed. Use of orthogonal transforms like DCT, DFT, and Haar with SVD is very popular. In this paper a concept of hybrid transforms generated from orthogonal transforms is used to perform watermarking. Strength of hybrid transform is increased by using SVD with it. Hybrid transform is applied to host image either column wise or row wise. Middle frequency band of transformed host is selected to embed the watermark. Watermark to be embedded in host is subjected to SVD. Since maximum of image energy is accumulated in only first few singular values, these values are sufficient to embed the watermark in host. In propose approach we find that for 128x128 size watermark image, first 30 singular values contain almost 99.99% of image energy and hence sufficient for embedding. Before embedding, singular values are adaptively scaled to match their energy with the energy of middle frequency region in which they are embedded. Inverse transform of host after embedding singular values in it gives watermarked image.

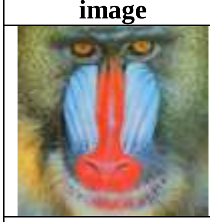
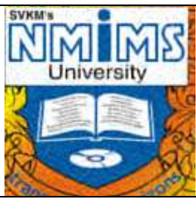
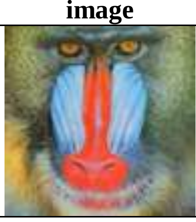
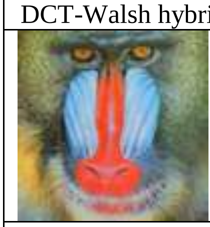
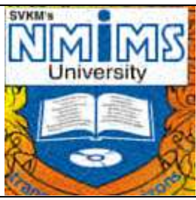
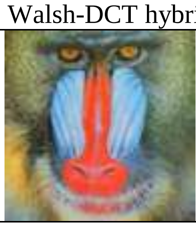
Extraction of watermark is followed exactly in reverse manner. Thus watermarked image is first column/row transformed using hybrid transform. From its middle frequency region, singular values of watermark are obtained. These singular values are scaled up to bring them back to their original strength. Inverse SVD of these scaled singular values gives us recovered watermark. Robustness of proposed approach is tested by comparing recovered watermark with embedded one. Comparison is done on the basis of average of absolute difference between pixels of two images known as Mean Absolute Error (MAE).

Proposed approach of watermarking is tested for its robustness against the attacks like image compression, image cropping, adding noise to watermarked images, resizing watermarked images and equalizing histogram of watermarked images. Fig. 1 shows five different host images and a watermark used to embed in host images.

(a) Lena **(b) Mandrill** **(c) Peppers** **(d) Face** **(e) Puppy** **(f) NMIMS**

Fig. 1: (a)-(e) host images (f) watermark image used for experimental work

Fig. 2 shows the watermarked image Mandrill using each of the column hybrid transforms mentioned and extracted watermark NMIMS from it without performing any attack. Below each watermarked image, MAE between host and watermarked image is displayed and below each extracted watermark, MAE between embedded and extracted watermark is shown.

Watermarked image	**Extracted watermark**	**Watermarked image**	**Extracted watermark**
			
MAE=0.337	MAE=0	MAE=0.265	MAE=0
DCT-Walsh hybrid column transform		Walsh-DCT hybrid column transform	
			
MAE=0.304	MAE=0	MAE=0.131	MAE=0
DCT-Haar hybrid column transform		Haar-DCT hybrid column transform	

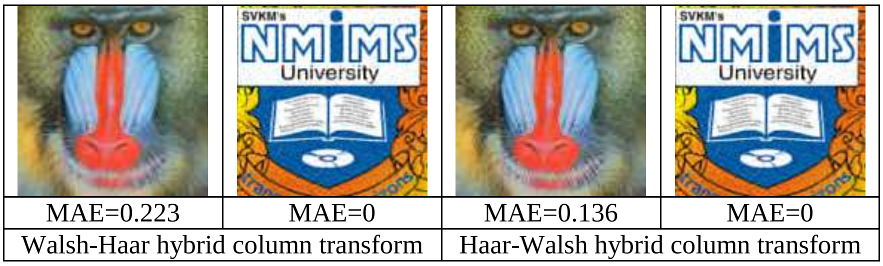


Fig. 2: watermarked image Mandrill and extracted watermark

V. RESULT ANALYSIS AGAINST ATTACKS

A. Compression attack

Compression of watermarked images is very obvious as its main aim is to save bandwidth. In proposed approach three types of compressions are performed. Compression using transforms like DCT, DST, Walsh, Haar and DCT wavelet, Compression using Vector quantization and JPEG compression. In compression using VQ, Kekre's Fast Codebook Generation (KFCG) algorithm [30] is used to generate codebook of size 256. JPEG compression includes compression using quality factor 100. One such compression results are shown here in Fig. 3. For each of the column hybrid transform mentioned, results of DCT compression are presented.

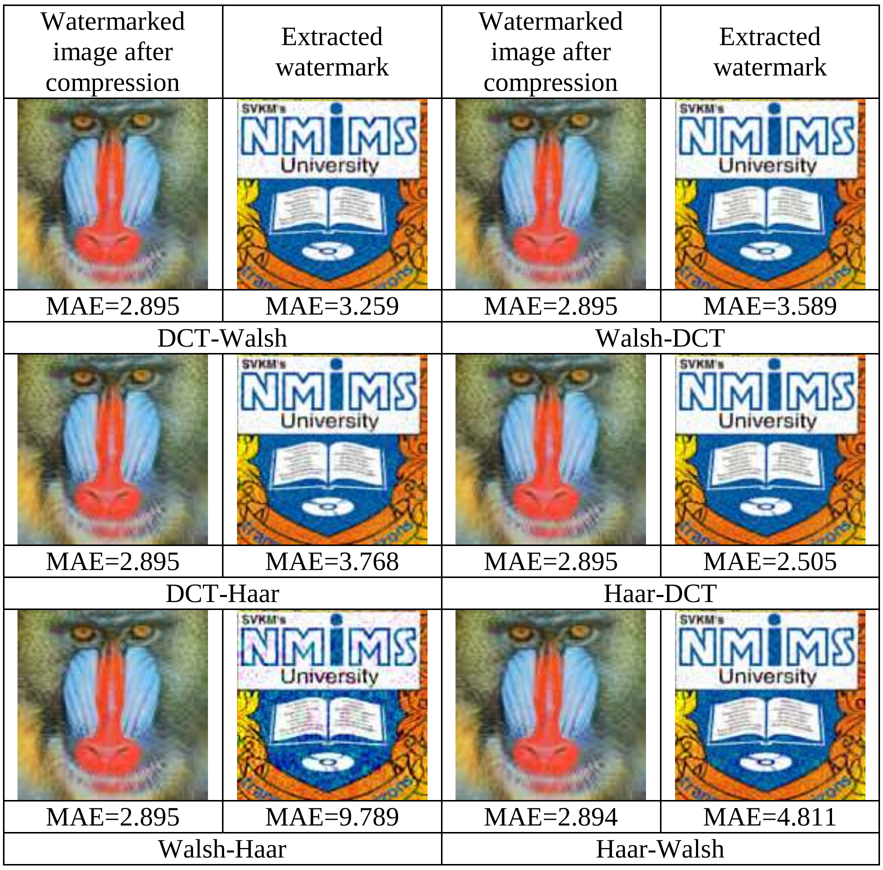


Fig. 3: Results of various hybrids transforms against compression using DCT

From Fig. 3 it can be seen that different hybrid transforms give different MAE values between embedded and extracted watermark and each of them is showing quite acceptable quality of extracted watermark. Table 1 shows average MAE between embedded and extracted watermark extracted from five different host images against compression attack when column and row version of hybrid transforms are used to embed the watermark.

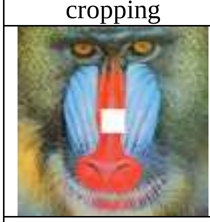
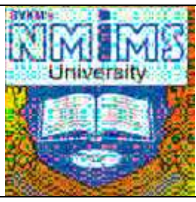
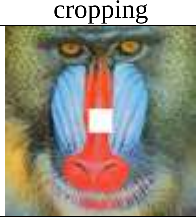
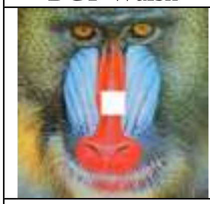
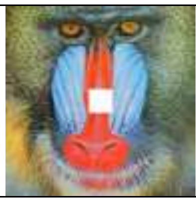
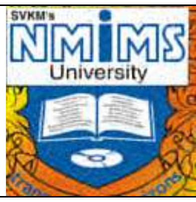
Table I: Average MAE between embedded and extracted watermark against compression attack using various hybrid transforms

Compression using	Column DCT-Walsh	Column Walsh-DCT	Column DCT-Haar	Column Haar-DCT	Column Walsh-Haar	Column Haar-Walsh
DCT	1.657	1.527	1.817	1.234	2.931	1.905
DST	1.677	1.537	1.840	1.265	2.980	1.980
Walsh	0	1.752	0.449	1.832	1.442	0.170
Haar	0.828	2.969	0.9	2.832	2.886	1.181
DCT Wavelet	7.182	2.015	7.716	1.407	8.569	8.082
JPEG	46.061	43.189	45.190	43.144	44.883	41.886
VQ	41.250	40.758	40.619	33.096	40.764	27.405
Compression using	**Row DCT-Walsh**	**Row Walsh-DCT**	**Row DCT-Haar**	**Row Haar-DCT**	**Row Walsh-Haar**	**Row Haar-Walsh**
DCT	2.197	1.482	3.312	2.230	1.981	3.449
DST	2.135	1.502	3.339	2.258	2.054	3.532
Walsh	0.327	2.010	2.062	2.253	1.136	1.660
Haar	3.131	2.756	4.057	3.491	1.110	2.690
DCT Wavelet	11.640	2.145	11.423	2.115	9.925	12.077
JPEG	47.069	44.216	45.964	39.436	45.100	40.968
VQ	39.648	40.637	39.832	30.429	40.897	34.998

From Table I it can be seen that except JPEG compression and VQ based compression, against all other types of compression attacks, all explored hybrid transforms show strong robustness.

B. Cropping Attack

Watermarked images are cropped at different regions: at corners and at centre. 16x16 size squares and 32x32 size squares are cropped at the corners of watermarked image to observe the effect of cropping more information. 32x32 size square is cropped at the centre where number of pixels cropped is same as in case of cropping 16x16 pixels at four corners. Fig. 4 shows the result images for cropping 32x32 at centre attack using column hybrid transforms.

Watermarked image after cropping	Extracted watermark	Watermarked image after cropping	Extracted watermark
			
MAE=1.856	MAE=61.781	MAE=1.856	MAE=165.969
DCT-Walsh		Walsh-DCT	
			
MAE=1.856	MAE=25.533	MAE=1.856	MAE=0
DCT-Haar		Haar-DCT	

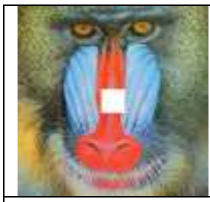
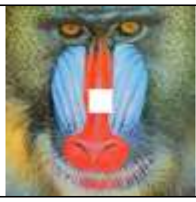
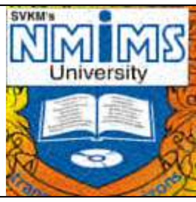
			
MAE=1.856	MAE=144.594	MAE=1.855	MAE=0
Walsh-Haar		Haar-Walsh	

Fig. 4: Results of various hybrid transforms against cropping 32x32 portion at centre.

From Fig. 4 it is observed that when Haar is used as base transform (first component) during generation of hybrid transform, highest robustness against cropping attack is obtained. Thus Haar-DCT and Haar-Walsh column hybrid transform show excellent robustness against cropping. On the other hand Walsh when used as base transform in the generation of hybrid transform cannot withstand the cropping attack. In case of row versions of hybrid transforms also transforms having Haar as base transform perform very well against cropping attack.

Table II shows Average MAE between embedded and extracted watermark against cropping attack for column and row versions of hybrid transforms.

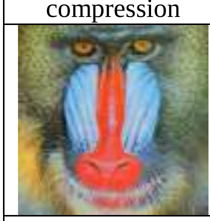
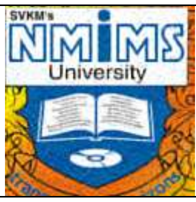
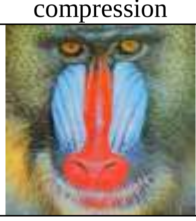
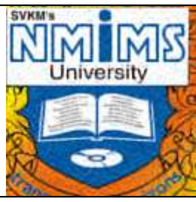
Table II: Average MAE between embedded and extracted watermark against cropping attack using various hybrid transforms

Cropping type	Column DCT-Walsh	Column Walsh-DCT	Column DCT-Haar	Column Haar-DCT	Column Walsh-Haar	Column Haar-Walsh
16x16 at corners	58.328	55.231	51.901	115.660	55.613	123.134
32x32 at corners	35.162	27.042	33.539	242.896	26.898	260.219
32x32 at centre	71.125	95.420	61.814	**0.749**	90.048	**0**
Cropping type	**Row DCT-Walsh**	**Row Walsh-DCT**	**Row DCT-Haar**	**Row Haar-DCT**	**Row Walsh-Haar**	**Row Haar-Walsh**
16x16 at corners	56.626	36.456	49.493	73.904	29.773	83.985
32x32 at corners	34.500	45.407	35.560	254.603	46.026	281.515
32x32 at centre	48.616	51.125	45.665	**1.885**	41.382	**3.048**

From Table 2 it can be concluded that for cropping at centre, hybrid transform column as well as row with Haar as the base transform shows strong robustness.

C. Noise addition attack

Two types of noises binary distributed run length noise and Gaussian distributed run length noise are added to watermarked images. Binary distributed noise is added with different run length like 1 to10, 5 to 50 and 10 to 100. Fig. 5 shows the watermarked images with Gaussian distributed noise added to them and watermark extracted from them when different hybrid transforms are used to embed the watermark.

Watermarked image after compression	Extracted watermark	Watermarked image after compression	Extracted watermark
			
MAE=0.746	MAE=1.968	MAE=0.746	MAE=2.213

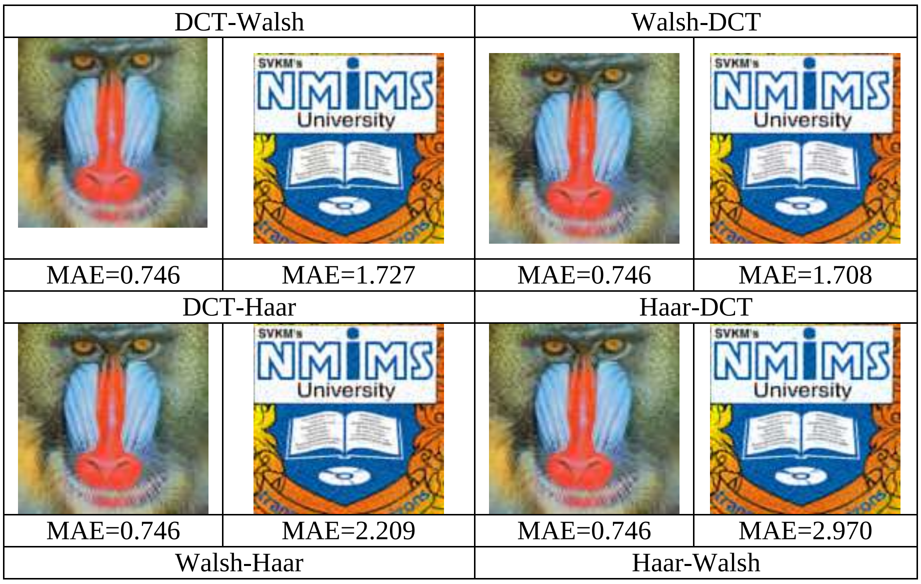


Fig. 5: Results of various hybrid transforms against Gaussian distributed run length noise.

From Fig. 5 it is observed that column hybrid transforms show excellent robustness against Gaussian distributed run length noise added to watermarked images. For binary distributed run length noise also, hybrid transforms shoe very well sustenance. Table 3 shows average MAE between embedded and extracted watermark from five different host images using column and row version of hybrid transforms.

Table III Average MAE between embedded and extracted watermark against noise addition attack using various hybrid transforms

Noise type	Column DCT-Walsh	Column Walsh-DCT	Column DCT-Haar	Column Haar-DCT	Column Walsh-Haar	Column Haar-Walsh
Binary distributed run length noise (1-10)	0	0	0	0	0	0
Binary distributed run length noise (5-50)	1.963	2.568	2.374	1.945	2.088	2.766
Binary distributed run length noise (50-100)	2.433	2.239	2.015	2.261	2.059	2.282
Gaussian distributed run length noise	2.087	2.207	2.037	**2.243**	2.109	2.413
Noise Type	**Row DCT-Walsh**	**Row Walsh-DCT**	**Row DCT-Haar**	**Row Haar-DCT**	**Row Walsh-Haar**	**Row Haar-Walsh**
Binary distributed run length noise (1-10)	5.755	4.897	4.036	3.840	6.381	3.961
Binary distributed run length noise (5-50)	5.411	4.702	4.676	4.316	4..140	4.234
Binary distributed run length noise (50-100)	3.656	3.430	3.512	3.011	3.101	3.632
Gaussian distributed run length noise	2.097	1.419	1.97	1.299	1.349	1.640

Table 3 shows that all hybrid transforms explored in proposed approach sustain noise addition attack very strongly. Column hybrid transforms show better robustness over row hybrid transforms against binary distributed run length noise attack.

D. Resizing attack

In resizing attack, watermarked image is first increased in size two times and then reduced to its original size. This is achieved by three different mechanisms: bicubic interpolation, transform based zooming [31] and grid based interpolation [32]. In transform based zooming, different transforms like DCT, DST, DFT, Real Fourier Transform and Hartley transform are used to zoom and reduce the watermarked image. Fig. 6 shows result images for bicubic interpolation based resizing for column hybrid transforms used for embedding the watermark.

Watermarked image after compression	Extracted watermark	Watermarked image after compression	Extracted watermark
			
MAE=3.770	MAE=18.886	MAE=3.766	MAE=20.349
DCT-Walsh		Walsh-DCT	
			
MAE=3.769	MAE=18.159	MAE=3.763	MAE=21.340
DCT-Haar		Haar-DCT	
			
MAE=3.768	MAE=19.437	MAE=3.762	MAE=20.842
Walsh-Haar		Haar-Walsh	

Fig. 6: Results of various hybrid transforms against resizing using bicubic interpolation

Table IV shows average MAE between embedded and extracted watermark when different hybrid transforms (column and row versions) are used to embed watermark.

Table IV Average MAE between embedded and extracted watermark against resizing attack using various hybrid transforms

Resizing type	Column DCT-Walsh	Column Walsh-DCT	Column DCT-Haar	Column Haar-DCT	Column Walsh-Haar	Column Haar-Walsh
Bicubic Interpolation	19.371	18.479	19.200	17.661	19.015	17.731
DFT	0.619	0.689	0.627	0.644	0.679	0.692
Grid based Interpolation	6.061	6.567	5.900	3.708	8.425	4.935
Resizing Type	**Row DCT-Walsh**	**Row Walsh-DCT**	**Row DCT-Haar**	**Row Haar-DCT**	**Row Walsh-Haar**	**Row Haar-Walsh**
Bicubic Interpolation	20.412	17.767	20.340	15.980	19.321	18.403
DFT	0.950	0.727	0.927	0.979	0.732	1.013
Grid based Interpolation	6.699	5.826	6.173	3.660	8.105	5.089

From Table IV, it is observed that column as well as row hybrid transforms show excellent robustness against resizing using DFT. For other transforms used to resize the watermarked image, MAE between embedded and extracted watermark is found to be zero. Thus we can conclude that proposed watermarking approach is strongly robust against transform based image resizing attack. Next high level robustness is obtained against resizing using grid based interpolation as shown in Table 4. For resizing using bicubic interpolation the quality of extracted watermark is acceptable. Similar results are obtained for row hybrid transforms also.

E. Histogram Equalization

Fig. 7 shows result images of Mandrill after equalizing its histogram for various column hybrid transforms.

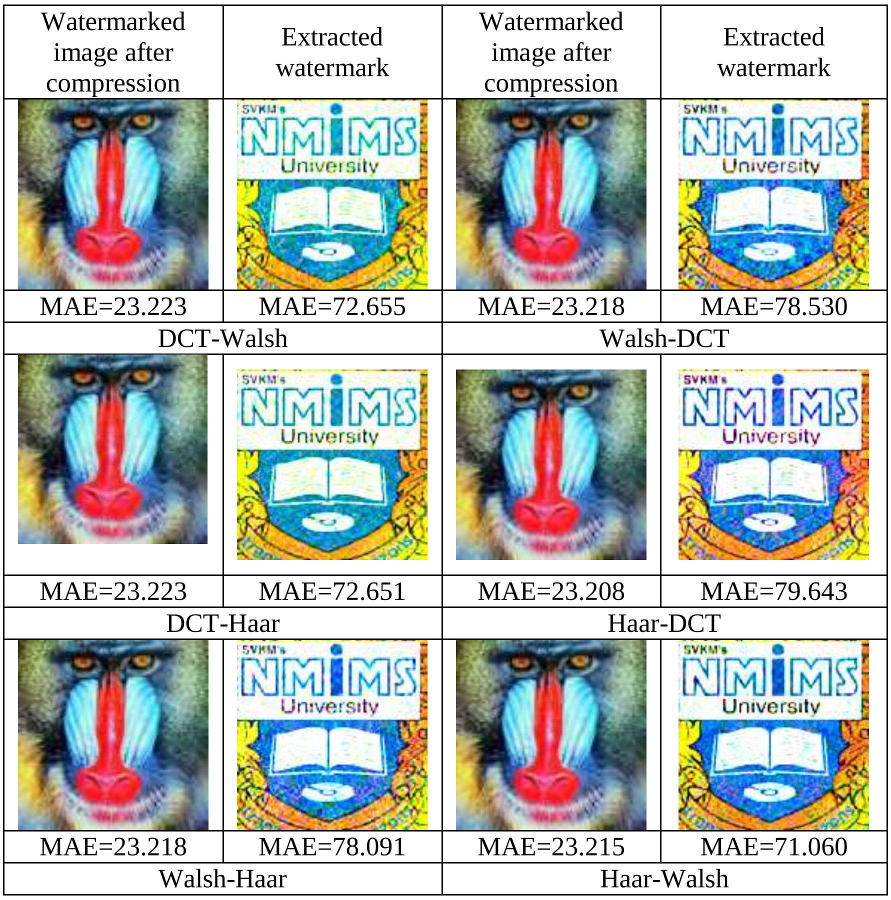


Fig. 7: Results of various hybrid transforms against histogram equalization

As can be seen from Fig. 7, MAE values between embedded and extracted watermark are higher due to changes in their pixel intensity values. Similar behaviour is depicted by row versions of hybrid transforms.

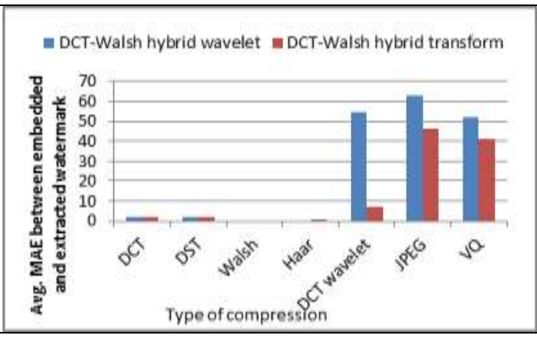
VI. PERFORMANCE COMPARISON WITH HYBRID WAVELET TRANSFORMS

Performance of proposed approach using hybrid transforms is compared with our previous work of hybrid wavelet transforms.

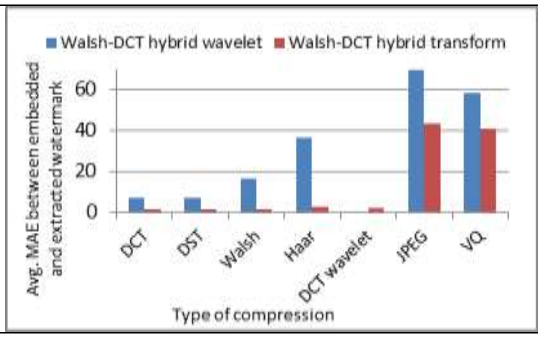
A. Compression attack:

1) Column hybrid wavelet vs. Column hybrid transform

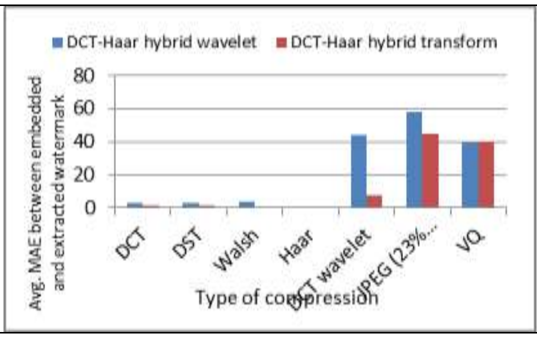
Fig. 8 shows comparison of column hybrid wavelet transforms and column hybrid transforms against compression attack.



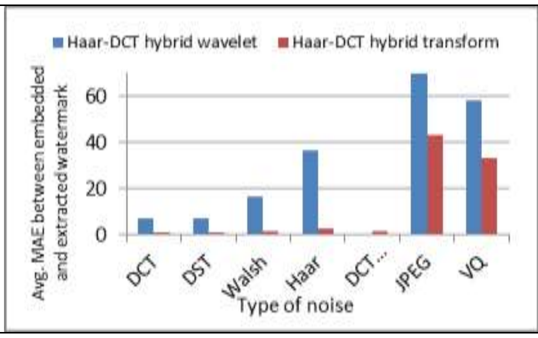
(a)DCT-Walsh hybrid wavelet vs. DCT-Walsh hybrid transform



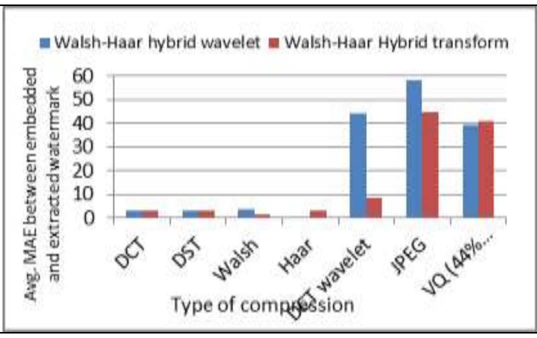
(b)Walsh-DCT hybrid wavelet vs. Walsh-DCT hybrid transform



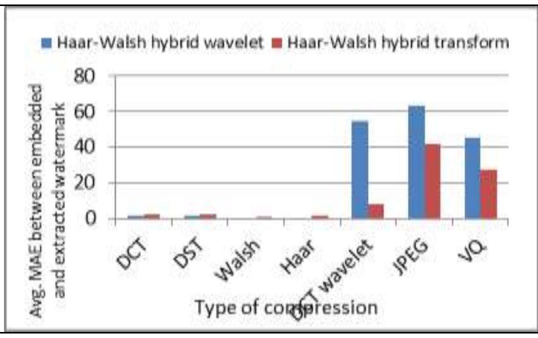
(c)DCT-Haar hybrid wavelet vs. Haar-DCT hybrid transform



(d)Haar-DCT hybrid wavelet vs. Haar-DCT hybrid transform



(e)Walsh-Haar hybrid wavelet vs. Walsh-Haar hybrid transform



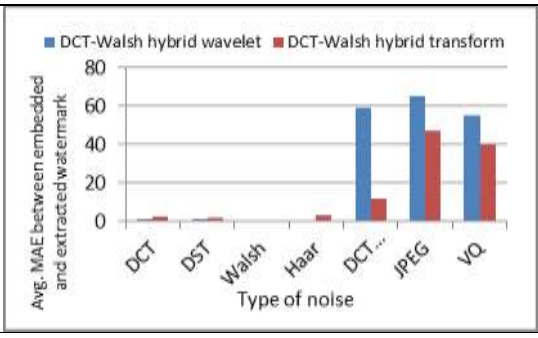
(f)Haar-Walsh hybrid wavelet vs. Haar-Walsh hybrid transform

Fig. 8: Column hybrid wavelet transforms vs. column hybrid transforms against compression attack.

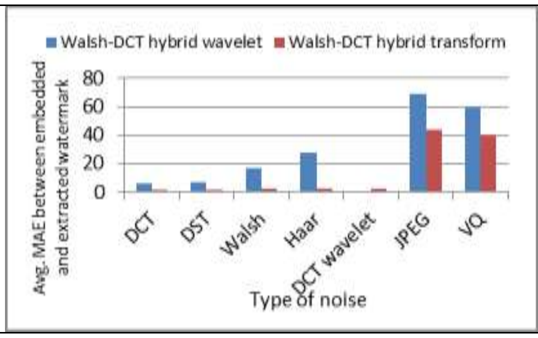
From Fig. 8 it can be observed that hybrid transforms perform better than hybrid wavelet transforms. For transform based compression this improvement is from 6% to 95%. For JPEG compression it is 23% to 38% better. For VQ based compression the improvement in robustness by hybrid transforms is 20% to 44%.

2) Row hybrid wavelet transforms vs. row hybrid transforms

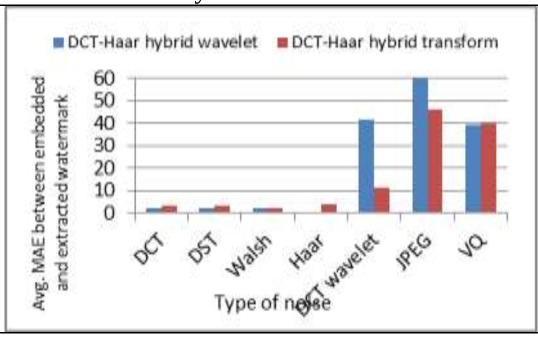
Fig. 9 shows comparison of row hybrid wavelet transforms and row hybrid transforms against compression attack. Similar to column hybrid transforms, row hybrid transforms improve the robustness against compression attack by more or less similar range.



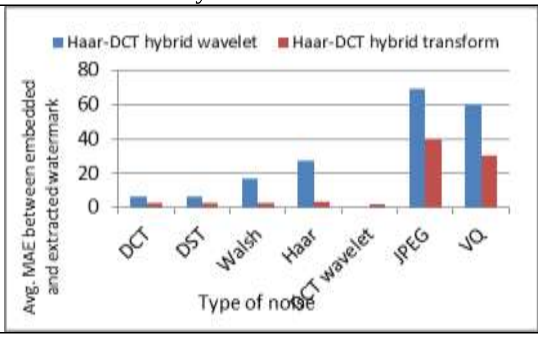
(a)DCT-Walsh hybrid wavelet vs. DCT-Walsh hybrid transform



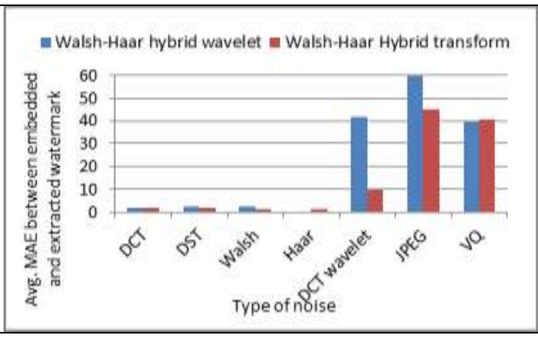
(b)Walsh-DCT hybrid wavelet vs. Walsh-DCT hybrid transform



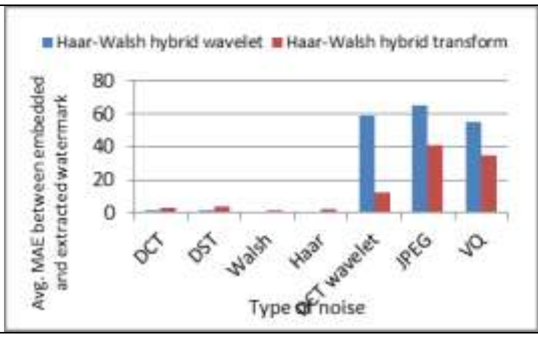
(c)DCT-Haar hybrid wavelet vs. Haar-DCT hybrid transform



(d)Haar-DCT hybrid wavelet vs. Haar-DCT hybrid transform



(e)Walsh-Haar hybrid wavelet vs. Walsh-Haar hybrid transform



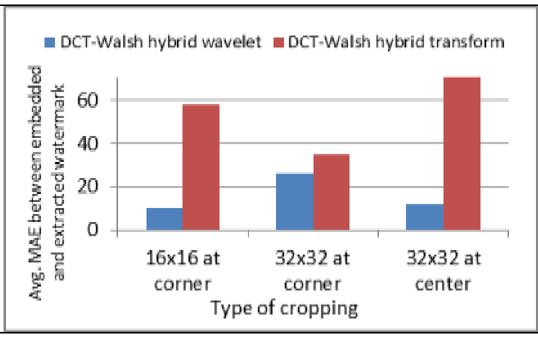
(f)Haar-Walsh hybrid wavelet vs. Haar-Walsh hybrid transform

Fig. 9: Row hybrid wavelet transforms vs. row hybrid transforms against compression attack.

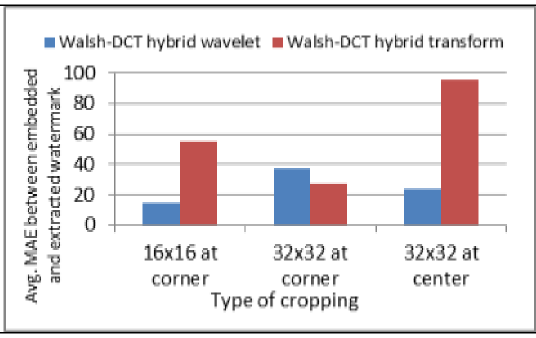
B. Cropping attack

1) Column hybrid wavelet transforms vs. column hybrid transform

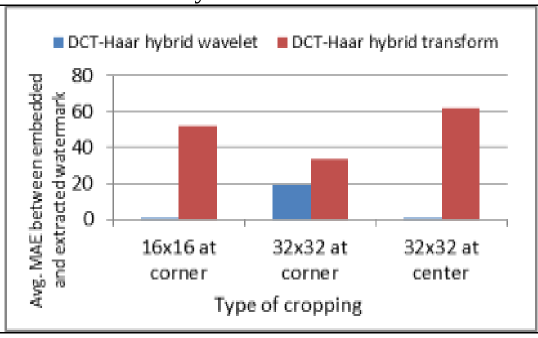
Fig. 10 shows comparison of column hybrid wavelet transform and column hybrid transforms against cropping attack. From Fig. 10 it is observed that hybrid transforms cannot perform better than hybrid wavelet transforms in column version against compression attack. Hybrid wavelet transforms are much better in robustness.



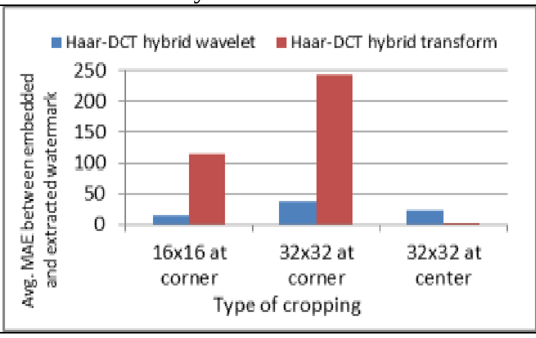
(a)DCT-Walsh hybrid wavelet vs. DCT-Walsh hybrid transform



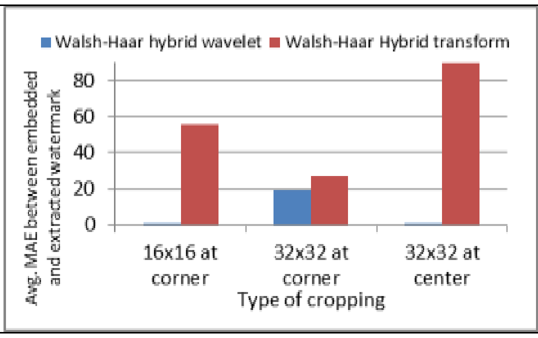
(b)Walsh-DCT hybrid wavelet vs. Walsh-DCT hybrid transform



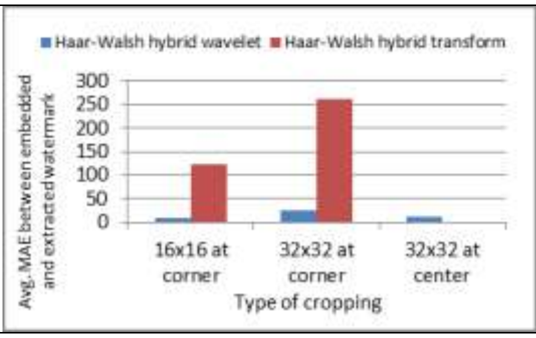
(c)DCT-Haar hybrid wavelet vs. Haar-DCT hybrid transform



(d)Haar-DCT hybrid wavelet vs. Haar-DCT hybrid transform



(e)Walsh-Haar hybrid wavelet vs. Walsh-Haar hybrid transform

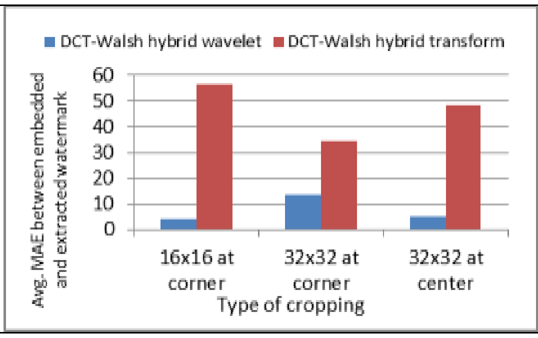


(f)Haar-Walsh hybrid wavelet vs. Haar-Walsh hybrid transform

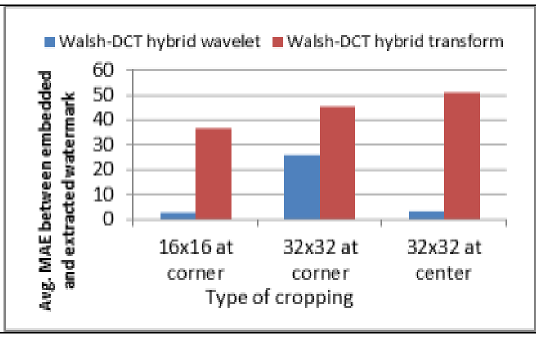
Fig. 10: Column hybrid wavelet transforms vs. column hybrid transforms against cropping attack.

2) Row hybrid wavelet transforms vs. row hybrid transforms

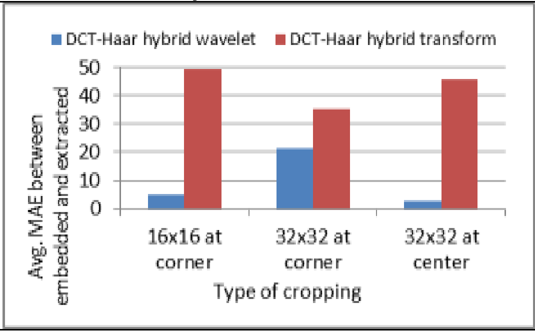
Fig. 11 shows comparison of row hybrid wavelet transforms and row hybrid transforms against cropping attack. Observations for row hybrid wavelet transforms and hybrid transforms are similar to that of column transforms. Hybrid wavelet transforms better sustain against cropping attack than hybrid transforms.



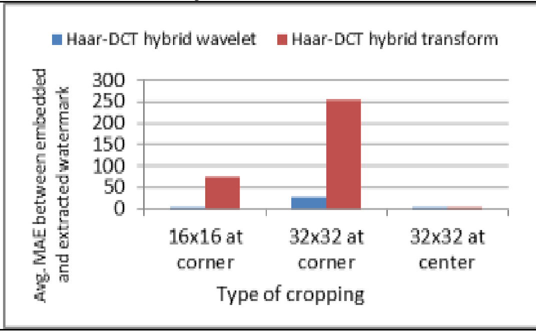
(a)DCT-Walsh hybrid wavelet vs. DCT-Walsh



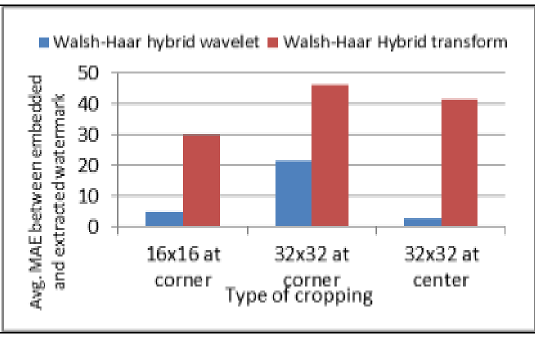
(b)Walsh-DCT hybrid wavelet vs. Walsh-DCT hybrid transform | hybrid transform



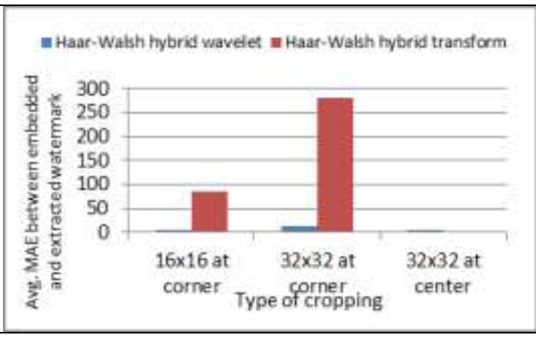
(c)DCT-Haar hybrid wavelet vs. Haar-DCT hybrid transform



(d)Haar-DCT hybrid wavelet vs. Haar-DCT hybrid transform



(e)Walsh-Haar hybrid wavelet vs. Walsh-Haar hybrid transform



(f)Haar-Walsh hybrid wavelet vs. Haar-Walsh hybrid transform

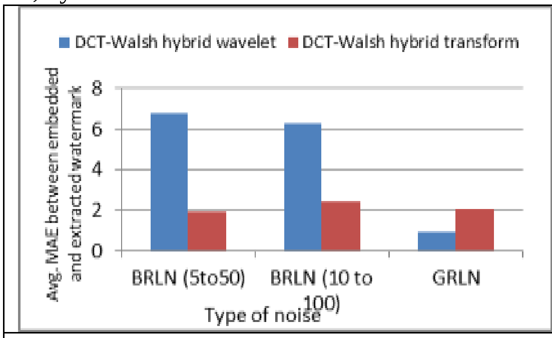
Fig. 11: Row hybrid wavelet transforms vs. row hybrid transforms against cropping attack.

C. Noise addition attack

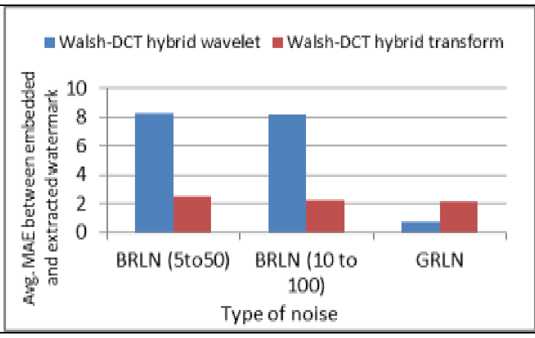
1) Column hybrid wavelet transform vs. column hybrid transform

Fig. 12 compares column hybrid transforms with column hybrid wavelet transforms against noise addition attack. In column version of hybrid transforms and hybrid wavelet transforms, MAE obtained for smaller run length (1 to 10) of binary distributed run length noise is zero. Therefore it is not shown in the graph. However, for row transforms, it is nonzero and hence can be compared.

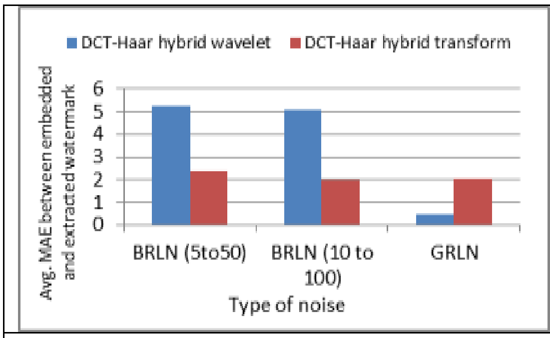
From Fig. 12 it is observed that all hybrid transforms show up to 70% improved robustness against binary distributed run length noise with run length 5 to 50 and 10 to 100. But for Gaussian distributed run length noise, hybrid wavelet transforms are more robust.



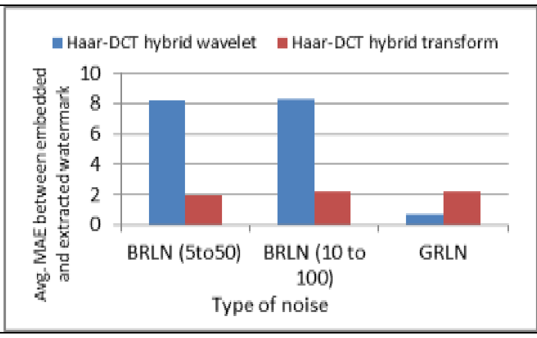
(a)DCT-Walsh hybrid wavelet vs. DCT-Walsh hybrid transform



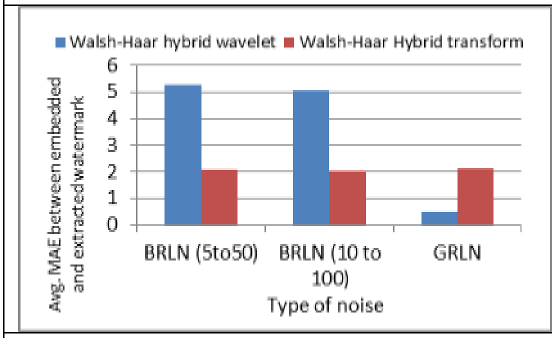
(b)Walsh-DCT hybrid wavelet vs. Walsh-DCT hybrid transform



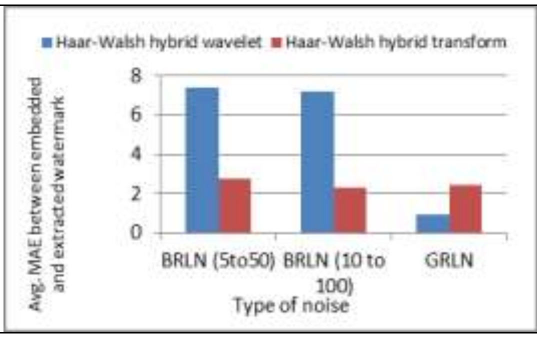
(c)DCT-Haar hybrid wavelet vs. Haar-DCT hybrid transform



(d)Haar-DCT hybrid wavelet vs. Haar-DCT hybrid transform



(e)Walsh-Haar hybrid wavelet vs. Walsh-Haar hybrid transform

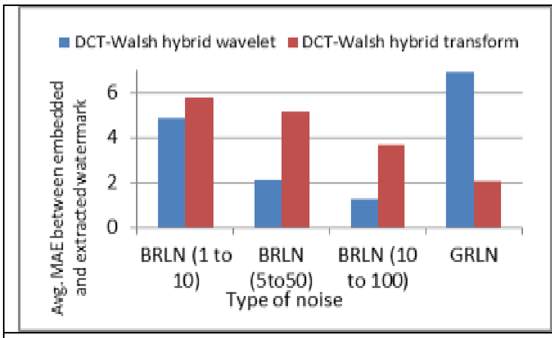


(f)Haar-Walsh hybrid wavelet vs. Haar-Walsh hybrid transform

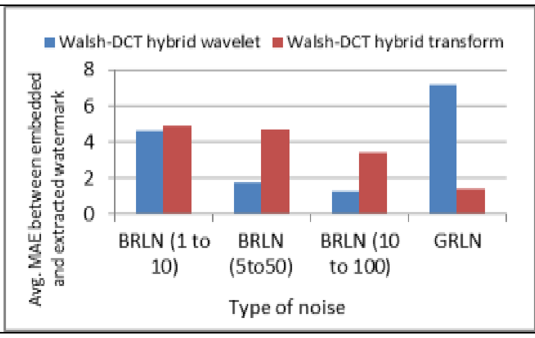
Fig. 12: Column hybrid wavelet transforms vs. column hybrid transforms against noise addition attack.

2) Row hybrid wavelet vs. row hybrid transforms

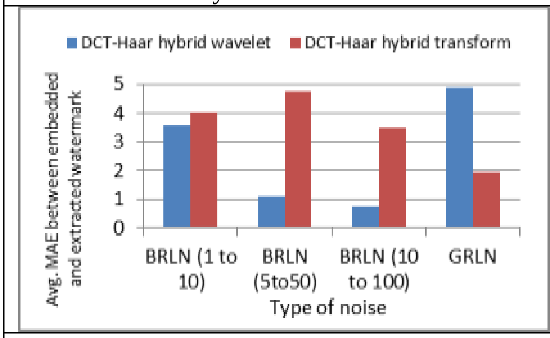
Fig. 13 compares row hybrid transforms with row hybrid wavelet transforms. Behaviour of row hybrid transforms and row hybrid wavelet transforms is opposite to that of column transforms. Thus in row version, hybrid transforms perform better than hybrid wavelet transform against Gaussian distributed run length noise. For Binary distributed run length noise, hybrid wavelet transform show better robustness than hybrid transforms.



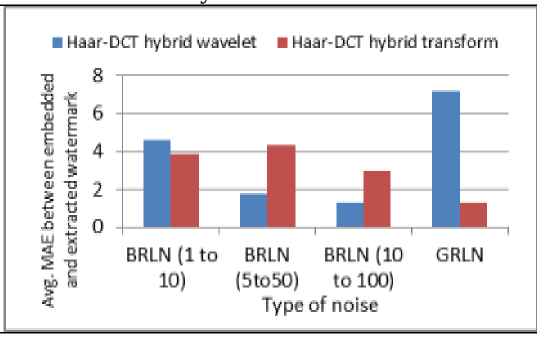
(a)DCT-Walsh hybrid wavelet vs. DCT-Walsh hybrid transform



(b)Walsh-DCT hybrid wavelet vs. Walsh-DCT hybrid transform



(c)DCT-Haar hybrid wavelet vs. Haar-DCT hybrid



(d)Haar-DCT hybrid wavelet vs. Haar-DCT hybrid

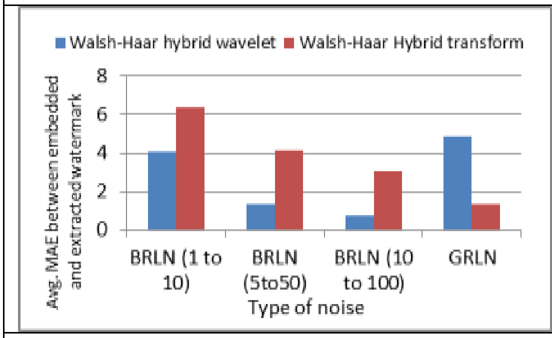
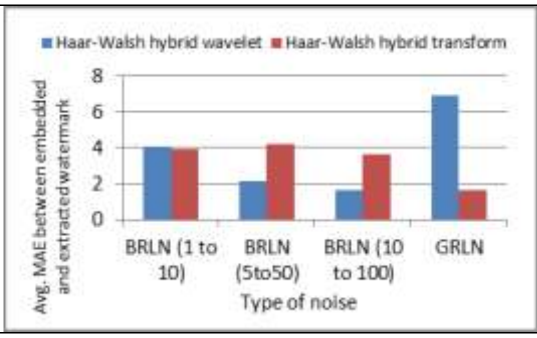
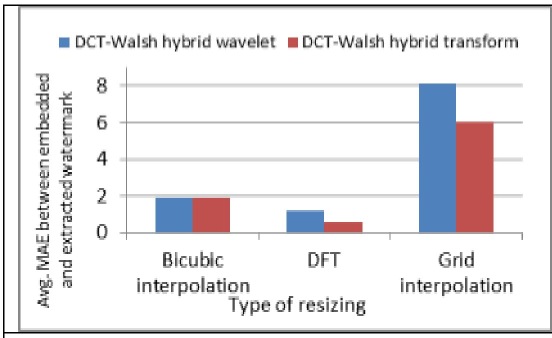
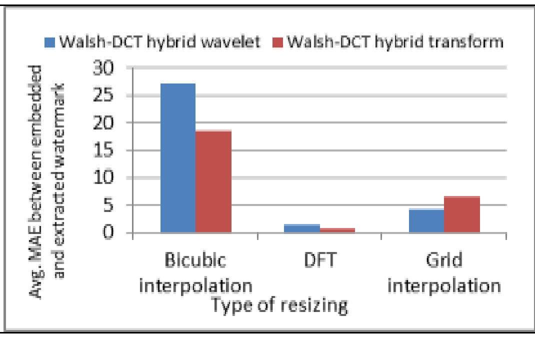
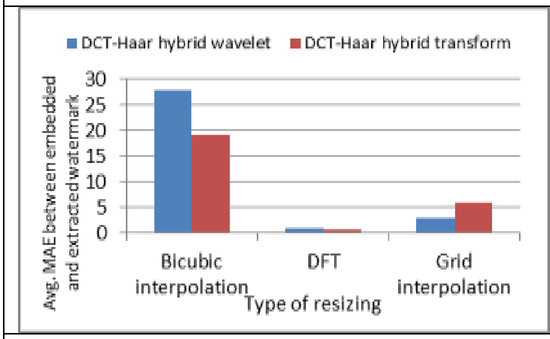
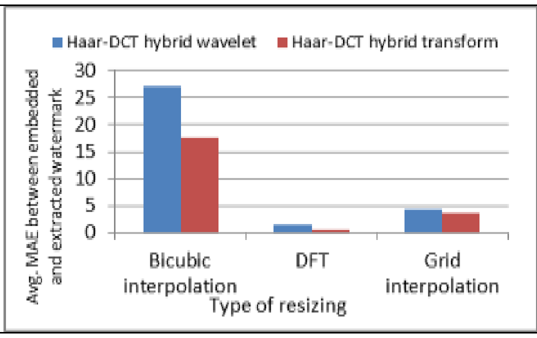
transform	transform
	
(e)Walsh-Haar hybrid wavelet vs. Walsh-Haar hybrid transform	(f)Haar-Walsh hybrid wavelet vs. Haar-Walsh hybrid transform

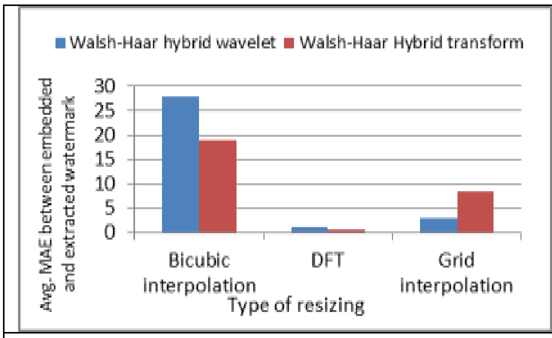
Fig. 13: Row hybrid wavelet transforms vs. row hybrid transforms against noise addition attack.

D. Resizing attack

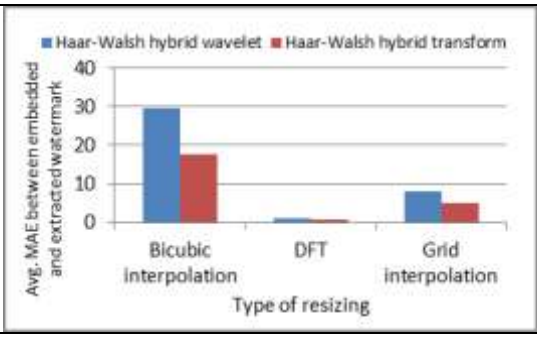
1) Column hybrid wavelet transforms vs. column hybrid transforms

Fig. 14 compares column versions of hybrid wavelet and hybrid transforms against resizing attack. Hybrid transforms improve the robustness significantly up to 32% against bicubic interpolation based resizing and up to 56% against resizing using DFT. For the combination of Walsh-DCT, Haar-DCT and Walsh-Haar, hybrid wavelet transforms are more robust than hybrid transforms against resizing using grid interpolation.

	
(a)DCT-Walsh hybrid wavelet vs. DCT-Walsh hybrid transform	(b)Walsh-DCT hybrid wavelet vs. Walsh-DCT hybrid transform
	
(c)DCT-Haar hybrid wavelet vs. Haar-DCT hybrid transform	(d)Haar-DCT hybrid wavelet vs. Haar-DCT hybrid transform



(e)Walsh-Haar hybrid wavelet vs. Walsh-Haar hybrid transform

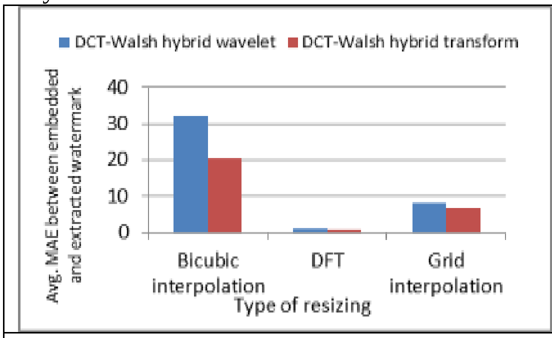


(f)Haar-Walsh hybrid wavelet vs. Haar-Walsh hybrid transform

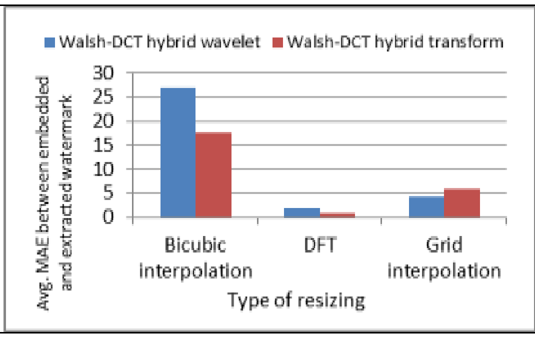
Fig. 14: Column hybrid wavelet transforms vs. column hybrid transforms against resizing attack.

2) Row hybrid wavelet transforms vs. row hybrid transforms

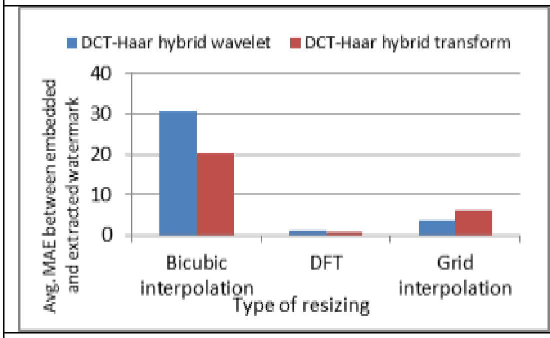
Fig. 15 compares hybrid wavelet transforms and hybrid transforms against resizing attack in their row versions. Performance of row versions is similar to that of column versions. Hybrid transforms are more robust than hybrid wavelet transforms.



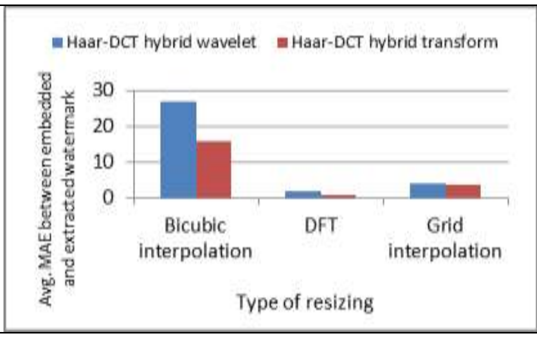
(a)DCT-Walsh hybrid wavelet vs. DCT-Walsh hybrid transform



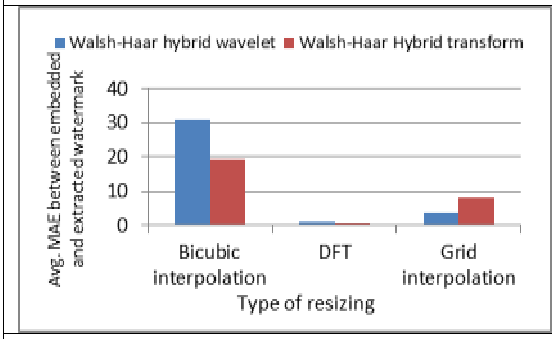
(b)Walsh-DCT hybrid wavelet vs. Walsh-DCT hybrid transform



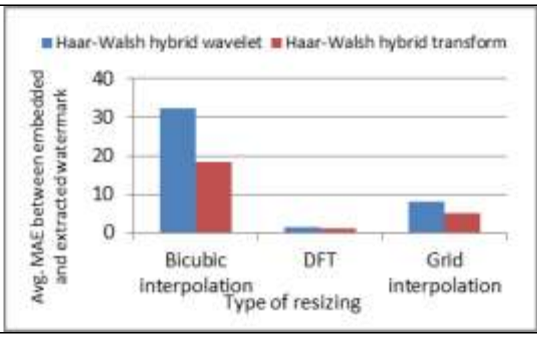
(c)DCT-Haar hybrid wavelet vs. Haar-DCT hybrid transform



(d)Haar-DCT hybrid wavelet vs. Haar-DCT hybrid transform



(e)Walsh-Haar hybrid wavelet vs. Walsh-Haar hybrid transform



(f)Haar-Walsh hybrid wavelet vs. Haar-Walsh hybrid transform

Fig. 15: Row hybrid wavelet transforms vs. row hybrid transforms against resizing attack.

VII. CONCLUSIONS

In the proposed approach of watermarking using hybrid transforms, desirable characteristics of two transforms are clubbed in one transform by taking their kronecker product. Hybrid transforms in their column and row versions improve the performance of individual component transforms. At the same time they also show significant improvement in robustness against various attacks over hybrid wavelet transforms. For different attacks percentage improvement shown by hybrid transforms is given in following Table V.

Table V Performance improvement by hybrid transforms over hybrid Wavelet transforms against various attacks.

Attack	Percentage improvement over hybrid wavelet transforms
Compression	59%
Cropping	No improvement
Noise addition	70%
Resizing	32-56%

REFERENCES

[1]. Abhay Sharma, Rekha Chaturvedi, Naveen Hemrajani, Dinesh Goyal, "New improved and robust watermarking technique based on third LSB substitution method", International journal of scientific and research publication, vol. 2, issue 3, pp. 1-4, 2012.

[2]. Rajani Verma, Archana Tiwari, "Copyright Protection for Watermark Image Using LSB Algorithm in Colored Image", Advance in Electronic and electric engineering, vol. 4, No. 5, pp. 499-506, 2014.

[3]. V.Madhu Viswanatham, Jeswanth Manikonda, "A novel technique for embedding data in spatial domain", International Journal on Computer Science and Engineering, Vol. 2, No. 2, pp. 233-236, 2010.

[4]. Abdullah Bamatraf, Rosziati Ibrahim and Mohd. Najib Mohd. Salleh, "A New Digital Watermarking Algorithm UsingCombination of Least Significant Bit (LSB) and Inverse Bit", Journal of computing, volume 3, Issue 4, pp. 1-8, 2011.

[5]. Wai Chu, "DCT-Based Image Watermarking Using Subsampling", IEEE transactions on multimedia, vol. 5, no. 1, pp. 34-38, March 2003.

[6]. Adrian G. Bor_s and Ioannis Pitas, "Image watermarking using block site selection and DCT domain constraints", Optics Express, Vol. 3, No. 12, pp.512-523, 1998.

[7]. Rajesh Kannan Megalingam, Mithun Muralidharan Nair, Rahul Srikumar, Venkat Krishnan Balasubramanian and Vineeth Sarma Venugopala Sarma, "A Comparative Study on Performance of Novel, Robust Spatial Domain Digital Image Watermarking with DCT Based Watermarking", International Journal of Computer Theory and Engineering, Vol. 2, No. 4, pp. 647-653, August 2010.

[8]. Dr. B. Eswara Reddy, P. Harini, S. Maruthu Perumal & Dr. V. Vijaya Kumar, "A New Wavelet Based Digital Watermarking Method for Authenticated Mobile Signals", International Journal of Image Processing (IJIP), Volume (5): Issue (1), pp. 13-24, 2011.

[9]. Nagaraj V. Dharwadkar & B. B. Amberker, "Determining the Efficient Sub band Coefficients of Biorthogonal Wavelet for Grey level Image Watermarking", International Journal of Image Processing Volume (4): Issue (2), pp. 89-105.

[10]. Yiwei Wang, , John F. Doherty, and Robert E. Van Dyck, "A Wavelet-Based Watermarking Algorithm for Ownership Verification of Digital Images", IEEE transactions on image processing, vol. 11, no. 2, pp.77-88, February 2002.

[11]. Ruizhen Liu and Tieniu Tan, "An SVD-Based Watermarking Scheme for Protecting Rightful Ownership", IEEE transactions on multimedia, vol. 4, no.1, pp. 121-128, March 2002.

[12]. Kapre Bhagyashri, Joshi, M.Y., "Robust image watermarking based on singular value decomposition and discrete wavelet transform", in Proc. of 3rd IEEE International Conference on Computer Science and Information Technology, pp.337-341, 2010.

[13]. G. Bhatnagar, B. Raman, Q. M. J. Wu, " Robust watermarking using fractional wavelet packet transform", IET Image Processing, vol. 6, issue 4, pp. 386-397, 2012.

[14]. Ahmed Abdulfetah, Xingming Sun, Hengfu Yang and Nur Mohammad, "Robust adaptive image watermarking using visual models in DWT and DCT domain", Information Technology journal 9(3), pp. 460-466, 2010.

[15]. Mohsen Kariman Khorasani, Mohammad Mojtaba Sheikholeslami, "An DWT-SVD Based Digital Image Watermarking Using a Novel Wavelet Analysis Function", Fourth International Conference on Computational Intelligence, Communication Systems and Networks, pp. 254-256, 2012.

[16]. A. Sverdlov, S. Dexter and A. M. Eskicioglu, "Robust DCT-SVD domain image watermarking for copyright protection : Embedding data in all frequencies, in proc. the 2004 Multimedia and Security Workshop, ACM press, pp. 166-174, Sep. 2004.
[17]. Navas, K.A., Ajay, M.C., Lakshmi M., Archana T.S., Sasikumar, M., "DWT-DCT-SVD based watermarking", 3rd International Conference on Communication Systems Software and Middleware and Workshops,pp.271-274, 2008.
[18]. Cox, Ingemar J., Joe Kilian, F. Thomson Leighton, and Talal Shamoon,"Secure spread spectrum watermarking for multimedia", Image Processing, IEEE Transactions on 6, no. 12, 1673-1687, 1997.
[19]. Piva, Alessandro, F. Bartolinin, V. Cappellini, and M. Barni,"Exploiting the cross-correlation of RGB-channels for robust watermarking of color images",inproc. IEEE of International Conference on Image Processing, pp. 306-310, 1999.
[20]. Bedi, S. S., Ashwani Kumar, and Piyush Kapoor, "Robust secure SVD based DCT–DWT oriented watermarking technique for image authentication", In International Conference on IT to celebrate S. Charmonman's 72nd birthday, pp. 46-1. 2009.
[21]. Mohan, B. Chandra, and S. Srinivas Kumar,"A robust image watermarking scheme using singular value decomposition", Journal of Multimedia 3, no. 1, 7-15, 2008.
[22]. Rahman, Md, "A dwt, dct and svd based watermarking technique to protect the image piracy", arXiv preprint arXiv:1307.3294 (2013).
[23]. Erkan Yavuz, ziya telatar, "Improved SVD-DWT Based Digital Image Watermarking against Watermark Ambiguity", Proceedings of the 2007 ACM symposium on applied computing, pp. 1051-1055, 2007.
[24]. H. B. Kekre, Tanuja Sarode, Shachi Natu, "Performance Comparison of DCT and Walsh Transforms for Watermarking using DWT-SVD", International Journal of Advanced Computer Science and Applications, Vol. 4, No. 2, pp. 131-141, 2013.
[25]. Dr. H. B. Kekre, Dr. Tanuja Sarode, Shachi Natu, "Hybrid Watermarking of Color Images using DCT-Wavelet, DCT and SVD", International Journal of Advances in Engineering and Technology, vol.6, Issue 2.pp. 769-779, May 2013.
[26]. Dr. H. B. Kekre, Dr. Tanuja Sarode, Shachi Natu, "Robust watermarking using Walsh wavelets and SVD", International Journal of Advances in Science and Technology, Vol. 6, No. 4, pp.8-23, April 2013.
[27]. Dr. H. B. Kekre, Dr. Tanuja Sarode, Shachi Natu," Performance Comparison of Wavelets Generated from Four Different Orthogonal Transforms for Watermarking With Various Attacks", International Journal of Computer and Technology, Vol. 9, No. 3, pp. 1139-1152, July 2013.
[28]. Cao, Lijie. "Singular value decomposition applied to digital image processing, "Division of Computing Studies" , Arizona State University Polytechnic Campus, Mesa, 2006.
[29]. Ruizhen Liu, Tieniu Tan, "A SVD based watermarking scheme for protecting rightful ownership",IEEE transactions on multimedia, vol. 4, pp.121-128, 2002.
[30]. Kekre, H. B., and Tanuja K. Sarode,"Fast Codebook Generation Algorithm for Color Images using Vector Quantization", International Journal of Computer Science and Information Technology 1.1: 7-12, 2009.
[31]. Dr. H. B. Kekre, Dr. Tanuja Sarode, Shachi Natu, "Image Zooming using Sinusoidal Transforms like Hartley, DFT, DCT, DST and Real Fourier Transform", International journal of computer science and information security Vol. 12 No. 7, 2014.
[32]. H. B. Kekre, Tanuja Sarode, Sudeep Thepade, "Grid based image scaling technique", International Journal of Computer Science and Applications, Volume 1, No. 2, pp. 95-98, 2008.