



Robust Watermarking by Embedding Watermark in Sorted Mid-frequency Coefficients of Column Transform using DKT-DCT Wavelet

H. B. Kekre¹, Tanuja Sarode², Shachi Natu³

¹MPSTME, Department of Computer Engineering, NMIMS University, Mumbai, India
hbkekre@yahoo.com

²Department of Computer Engineering, TSEC, Mumbai University, India
tanuja_0123@yahoo.com

³Ph. D. Research Scholar, MPSTME, NMIMS University, Mumbai, India
shachi_natu@yahoo.com

ABSTRACT

In this paper we introduce a watermarking method which is based on hybrid wavelet transform generated from two orthogonal transforms namely Discrete Kekre Transform and Discrete Cosine transform. As introduced in our previous work, column transform of host and watermark is obtained to make the technique computationally efficient. Watermark is compressed and normalized before embedding to improve imperceptibility of watermarked image. Middle frequency host transform coefficients are used to embed the watermark. Instead of random (row wise) embedment of watermark coefficients into host coefficients, sorting is applied to both coefficients to have a maximum match or minimum difference between them while embedding. Sorting improves the performance of the technique when compared to previous work done without sorting.

Keywords

Watermarking; Sorting; DKT; DCT; Cropping; Compression; Run length noise; Resizing.

Council for Innovative Research

Peer Review Research Publishing System

Journal: INTERNATIONAL JOURNAL OF COMPUTERS AND TECHNOLOGY

Vol. 13, No. 7

editorijctonline@gmail.com

www.ijctonline.com, www.cirworld.com



INTRODUCTION

Increased use of network technology for communication has made information sharing a very routine part of life. Shared information can be in the form of digital data like images, videos, audio files and many more. Along with easy sharing of information, threats like tampering the information or unauthorised claiming of information are also increased. Sophisticated technology tools available for manipulation or edition of digital data are the major contributor in this. Obviously, secure transmission of data over network is the need arising out of it. Watermarking is one of the well-known techniques used to make digital data secure against such unauthorised alteration or claiming.

Digital Image Watermarking can be performed in spatial domain and in frequency domain.

In spatial domain pixel values of cover image are subjected to alteration by some mechanism so that it will carry the watermark information. Frequency domain watermarking first transforms image into frequency domain. These transform coefficients are then used to hide the watermark information. Hiding watermark in transform coefficients makes it less susceptible to various attacks and thus more robust than spatial domain watermarking. This makes frequency domain watermarking more popular over spatial domain watermarking. Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT) are few of widely used transforms in frequency domain watermarking. Recently, Singular Value Decomposition is also used and proved to be very effective when used in combination with other transforms as mentioned earlier.

Desirable characteristics of digital image watermarking focused in the work are robustness and imperceptibility. Imperceptibility refers to the degree of invisibility of embedded watermark and robustness refers to the survival of the watermark in the cover image after performing intentional or non-intentional attacks on watermarked image. A good watermarking technique should have high imperceptibility and should be highly robust. But most of the times it is difficult to achieve both the things together and hence always there is trade-off between the two. In the proposed watermarking technique, we have tried to achieve these properties with minimum compromise.

The proposed watermarking technique is frequency domain invisible blind watermarking technique. Instead of using the routine popular forms of wavelet transforms, a hybrid wavelet transform is used. This hybrid wavelet transform is generated using Discrete Kekre Transform (DKT) and Discrete Cosine Transform. The algorithm for generation of hybrid wavelet transform and DKT are proposed by Dr. Kekre in [1] and [2] respectively. Further, it is noticed that, using column transform instead of full transform reduces the computational complexity and also give better robustness and imperceptibility.

Details in the paper are organized as follows. Section 2 gives related work in the domain of image watermarking. Proposed watermarking technique is discussed in section 3. Results of the proposed technique under various attacks are presented in section 4. Section 5 concludes the paper.

RELATED WORK

In Literature, lot of work has been done in the field of watermarking by using various transforms. SVD based image watermarking is proposed by Amrik Singh and Balpreet Kaur [3]. Adaptive histogram stretching is performed to improve the visibility of host image. This image is then subjected to singular value decomposition. Watermark is then added to singular values of host image by performing scaling of watermark. This modified singular value matrix is then used to reconstruct the watermarked image. Peak Signal to Noise Ratio (PSNR), Mean Squared Error (MSE) and Bit Error Rate (BER) are the parameters used to measure the robustness of the scheme against various attacks. S. S. Sudha and K. K. Rahini proposed a combination of cryptography and watermarking algorithm in order to secure image information in [4]. Original image is encrypted using AES encryption algorithm with 128 bit secret key. This encrypted image is then embedded into cover image by applying DCT to its blocks. Thapa, Sood and Sharma [5] proposed a singular Value Decomposition based watermarking technique for images. SVD decomposes an image I into three matrices as $I = USV^T$, where S is a diagonal matrix giving singular values on the diagonal. By exploring characteristics of S and V matrices and by using Pseudo random sequences, embedding of watermark is done. The largest singular value is quantized for each block of image using a predefined quantization coefficient. Using the mid frequency band of SVD transformed image and Pseudorandom sequences, watermark is embedded. Henri et. al. [6], proposed a watermarking scheme using DCT and Schur decomposition. Host image and watermark image are selected of same size. According to their scheme, DCT is applied to host image and watermark is subjected to Schur decomposition. The upper diagonal matrix obtained in Schur decomposition is added to DCT of host image using appropriate scaling factor. Using reverse procedure, upper diagonal matrix is retrieved from watermarked image using which watermark is reconstructed. Feature and transform based watermarking technique is developed by A. Umamaheshwari and K. Thanushkodi [7]. Primary features are detected by Harris Laplacian detector. These feature set is used to embed the watermark. Watermarked image obtained through this is found to be robust against known or introduced image processing attacks but not against noise attack and other unknown attacks. In order to make it robust against unknown image processing attacks, auxiliary feature set is detected using Knapsack algorithm and watermark is embedded into them. Robust image watermarking using Scale Invariant Feature Transform (SIFT) for image restoration is proposed by Haijun Luo, Xingming Soon, Hengfu Yang and Zhihua Xia [8]. Synchronization errors caused by geometric distortion attacks can be reduced by using Scale Invariant Feature Transform to reconstruct the image from feature points. Watermark is embedded in more than one sub-image in the middle region of the image. Watermark detection decision is based on match between reconstructed image using SIFT and original watermark. In [9] Hongtao Lu et.al proposed a feature extraction based watermarking technique. Using scale interactive model based filter, feature points of image are extracted. Based on these feature points, watermark is constructed and adaptively embedded into local regions of these points. By computing the statistical correlation between watermark and the embedded region, decision about existence of watermark is made.

H. B. Kekre, Tanuja Sarode, Shachi Natu presented a DWT-DCT-SVD based hybrid watermarking method for colour 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 4×4 Walsh 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 et.al. [14] presented a DCT wavelet transform based watermarking technique. Here DCT wavelet is generated from orthogonal DCT using algorithm of wavelet generation from orthogonal transforms given by Dr. Kekre in [15]. Watermark is compressed before embedding in host image. Various compression ratios are tried for compression of watermark so that watermark image quality is maintained with acceptable loss of information from image. Embedding compressed image also reduces the payload of information embedded in host image and thus causes good imperceptibility of watermarked image. Performance of the technique is evaluated under attacks like binary run length noise, Gaussian distributed run length noise, cropping for various compression ratios used in watermark compression. In [15], the work by Kekre et.al in [14] was extended for other attacks like resizing and compression. Also the compressed watermark is obtained using compression ratio 2.67 and strength of compressed normalized watermark is further increased using suitable scaling factor which was not done in [14]. Performance of full, column and row transform using DCT wavelet and DKT_DCT hybrid wavelet against various attacks is explored by Kekre et.al. in [16] and [17] respectively. Column transform was proved better performance wise as well as computational efficiency wise in both the cases. Further, DKT_DCT column wavelet was observed better than DCT column wavelet. Effect of embedding the watermark by maintaining its energy in some proportion of the host energy is proposed in [18] by Kekre et.al.

PROPOSED WATERMARKING TECHNIQUE

Proposed Technique uses cover images of size 256×256 and watermark images of size 128×128 . For these images hybrid DKT_DCT transform of size 256×256 and 128×128 are needed respectively. From possible combinations of generating these transforms, we selected 16×16 size DKT transform matrix and 16×16 size DCT matrix to get 256×256 size DKT_DCT hybrid wavelet transform. 128×128 size DKT_DCT wavelet transform matrix for watermark image is generated from 32×32 DKT matrix and 4×4 DCT matrix. The colour bitmap images used for proposed work are shown in Fig. 1.



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

Embedding procedure

For embedding the watermark, first column transform of host image is obtained. Since column transform causes the energy of transformed image to be concentrated towards upper rows of image, middle frequency components of transformed host image are selected by choosing certain consecutive middle rows randomly. Coefficients from these rows are sorted in descending order. Similarly column DKT_DCT wavelet transform of watermark is obtained. By eliminating the lowermost rows which correspond to low energy elements, we compress the watermark such that distortion in compressed watermark will have acceptable level of imperceptibility. The compression ratio with which this acceptable distortion is obtained is 2.67. Compressed watermark is then normalized. Normalized watermark is further increased in strength by scaling it up with scaling factor ranging from 40 to 140 with the interval of 10. Coefficients of scaled up watermark are sorted in descending order. Middle rows of host are selected such that number of coefficients from these rows is equal in number of coefficients of scaled up watermark. Various groups of middle frequency rows selected for watermark in embedding are rows 233-256, 209-232, 185-208, 161-184, 137-160, 113-136, 108-131 and 89-112. Sorted coefficients of

transformed host image are replaced by sorted coefficients of scaled up watermark and positions where these coefficients are embedded are recorded. By sorting the coefficients we are trying to find the closest match for the watermark coefficient, thereby trying to maintain the energy of sub band selected for embedding the watermark. Inverse transform of host image is taken to get watermarked image.

Extraction procedure

For extraction of watermark, DKT_DCT column wavelet transform of watermarked image is obtained. From the middle frequency rows of this transformed image, transform coefficients of watermark are obtained. By using the recorded positions, these coefficients are placed at their appropriate places. Inverse column DKT_DCT transform is applied to these rearranged watermark coefficients to get the extracted watermark. To find the distortion caused by embedding watermark into host, Mean Absolute Error between host and watermarked image is calculated. Mean Absolute Error between embedded and extracted watermark is negligible.

RESULTS OF EMBEDDING AND EXTRACTION PROCEDURE

Watermarked image Lena and extracted watermark from it are shown in following Fig. 2. Since in [18] we have observed that higher value of scaling factor leads to better robustness, these results are for scaling factor 140 and for host rows 108-131 selected for watermark embedding. For comparison purpose, watermarked image and extracted watermark are also shown when embedding is done without sorting the transform coefficients. As we can see, there is very small increase in MAE between host and watermarked image in proposed technique and the technique proposed in our previous paper [18]. Though MAE is slightly higher, quality of watermarked image is better in sorting approach.


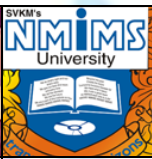
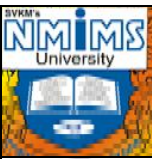
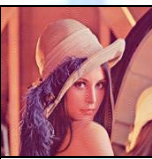



						
Host image	Watermark	MAE=15.404	MAE=3.374	Close to 0	MAE=3.364	Close to 0
(a)	(b)	(c)	(d)	(e)	(f)	(g)

Fig 2 (a) cover image ‘Lena’ (b) watermark ‘NMIMS’ (c) Compressed watermark (d) Watermarked image obtained when embedding is done by sorting transform coefficients (e) Extracted watermark when embedding is done by sorting transform coefficients (f) Watermarked image obtained when embedding is done without sorting transform coefficients (g) Extracted watermark when embedding is done without sorting transform coefficients

RESULTS OF PROPOSED WATERMARKING TECHNIQUE UNDER VARIOUS ATTACKS

Attacks performed on watermarked images are cropping, compression, noise addition, image resizing and histogram equalization.

Result of cropping attack:

To perform cropping attack in three different ways, 16x16 and 32x32 size squares at corners of an image and 32x32 size square at the centre of an image is cropped. Watermarked images with 16x16 sizes square cropped at corners of image with and without sorting transforms coefficients during embedding process are shown in Fig. 3.


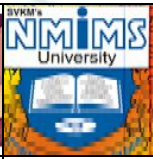


			
MAE=2.145	MAE=2.336	MAE=2.145	MAE=2.646
(a) With sorting		(b) Without sorting	

Fig. 3: Cropped watermark image and extracted watermark for 16x16 cropping attack using (a) sorted coefficients of host and watermark while embedding the watermark. (b) Without sorting coefficients of host and watermark while embedding the watermark.

In Fig. 4, watermarked image after cropping 32x32 size squares at corners and watermark extracted from it using sorting approach and without using sorting approach are shown.


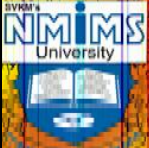


			
MAE=7.558	MAE=11.194	MAE=7.557	MAE=11.587
(a) With sorting		(b) Without sorting	

Fig. 4: Cropped watermark image and extracted watermark for 32x32 cropping attack using (a) sorted coefficients of host and watermark while embedding the watermark. (b) Without sorting coefficients of host and watermark while embedding the watermark.

From Fig. 3 and Fig. 4, it can be seen that the MAE between embedded and extracted watermark reduces when coefficients of both host image and watermark are sorted for embedding process. In this case, the MAE between watermarked image before and after attack remains same in both cases. Thus sorting makes it more robust.

Fig. 5 shows the watermarked image cropped at the centre, with and without sorting approach along with the extracted watermark from it.

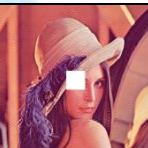
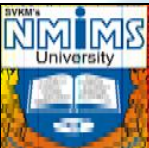
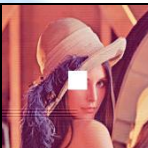
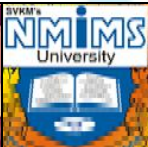
			
MAE=2.204	MAE=4.961	MAE=2.204	MAE=0.663
(a) With sorting		(b) Without sorting	

Fig. 5: Cropped watermark image and extracted watermark for 32x32 cropping attack at centre of an image using (a) sorted coefficients of host and watermark while embedding the watermark. (b) Without sorting coefficients of host and watermark while embedding the watermark.

However, for cropping an image at the centre does not improve the results by sorting the coefficients as shown in Fig. 5.

Results for compression attack:

Compression attack is performed by applying various column transforms to a watermarked image and then eliminating high frequency components from it. Various transforms used to perform compression attack are DCT wavelet transform, DCT, DST, Walsh and Haar. JPEG compression is also performed with quality factor 100. Results of watermarked image compression using orthogonal transforms DCT and DST are shown in Fig. 6. Similarly Fig. 7 and Fig. 8 show the compressed watermarked image and extracted watermark for compression using Walsh and Haar and DCT wavelet and JPEG compression.

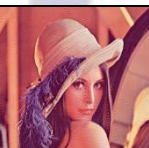
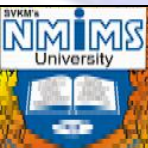
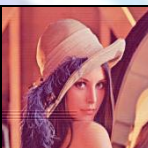
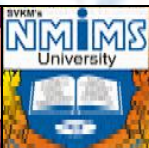
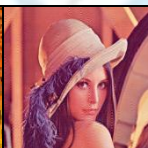
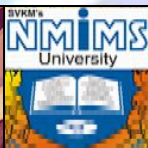
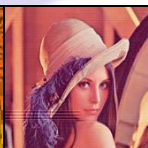
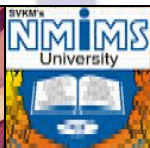
							
MAE=0.812	MAE=2.669	MAE=0.797	MAE=3.569	MAE=0.876	MAE=2.608	MAE=0.870	MAE=3.664
With sorting		Without sorting		With sorting		Without sorting	
(a) Compression using DCT				(b) Compression using DST			

Fig. 6: Compressed watermark image and extracted watermark using DCT and DST using (a) sorted coefficients of host and watermark while embedding the watermark. (b) Without sorting coefficients of host and watermark while embedding the watermark.

From Fig. 6, it can be clearly observed that extracted watermark has better correlation with the embedded one when embedding is done by sorting the coefficients of host and watermark.

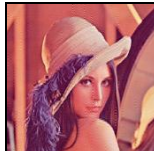
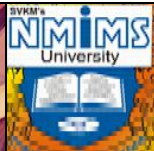
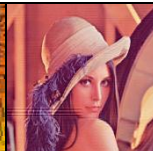
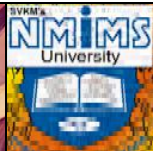
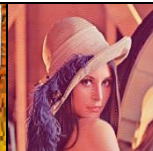
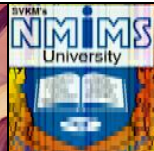
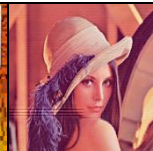
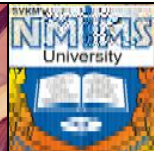
							
MAE=1.526	MAE=2.849	MAE=1.6	MAE=9.077	MAE=0.988	MAE=16.451	MAE=0.881	MAE=14.364
With sorting		Without sorting		With sorting		Without sorting	
(a) Compression using Walsh				(b) Compression using Haar			

Fig. 7: Compressed watermark image and extracted watermark using Walsh and Haar using (a) sorted coefficients of host and watermark while embedding the watermark. (b) Without sorting coefficients of host and watermark while embedding the watermark.

Fig. 7 shows that sorting results in better robustness for Walsh based compression attack. However, for Haar based compression, MAE between embedded and extracted watermark is slightly higher in case of sorting. But for lower values of scaling factors, sorting works better.

Fig. 8 shows the results of DCT wavelet based compression and JPEG compression with and without sorting transform coefficients.

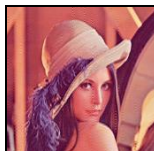
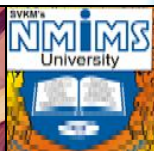
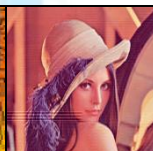
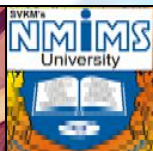
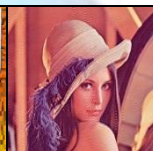
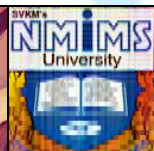
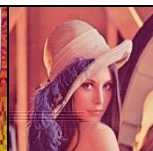
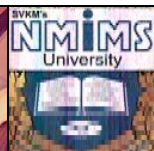
							
MAE=2.322	MAE=close to	MAE=2.322	MAE= close	MAE=0.011	MAE=22.833	MAE=0.003	MAE=26.099
With sorting		Without sorting		With sorting		Without sorting	
(a) Compression using DCT Wavelet				(b) JPEG Compression			

Fig. 8: Compressed watermark image and extracted watermark using DCT Wavelet and JPEG compression using (a) sorted coefficients of host and watermark while embedding the watermark. (b) Without sorting coefficients of host and watermark while embedding the watermark.

Fig. 8 shows that for DCT wavelet compression sorting and without sorting perform equally well. For JPEG compression, not only MAE value is reduced but also the quality of retrieved image is improved.

Results for Noise addition attack

Binary run length noise with magnitude 1 and -1 and binary distribution with different run lengths is added to watermarked image in noise addition attack. Addition of Gaussian distributed run length noise with magnitude between 2 and -2 is also tested. Results for noise added watermarked image and watermark extracted from it with corresponding MAE values are shown in Fig. 9 and Fig. 10.

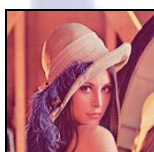
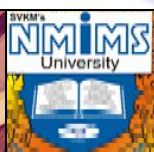
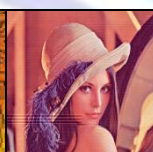
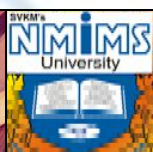
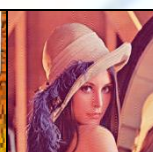
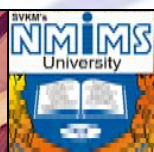
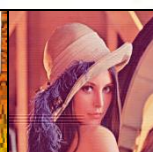

							
MAE=1	MAE=close to	MAE=1	MAE=close to	MAE=1	MAE=2.370	MAE=1	MAE=7.581
With sorting		Without sorting		With sorting		Without sorting	
(a) Binary distributed run length noise with run 1-10				(b) Binary distributed run length noise with run 5-50			

Fig. 9: watermarked image after adding binary distributed run length noise of run length 1 to 10 and 5 to 50 and extracted watermark from it using (a) sorted coefficients of host and watermark while embedding the watermark. (b) Without sorting coefficients of host and watermark while embedding the watermark.

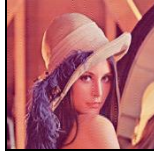
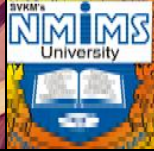
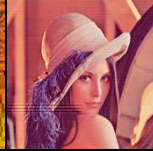
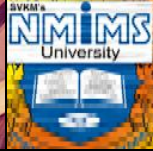

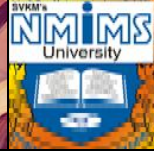
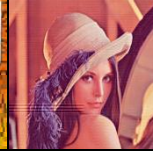
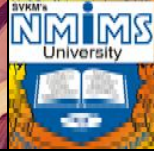
							
MAE=1	MAE=3.307	MAE=1	MAE=8.378	MAE=0.746	MAE=0.165	MAE=0.746	MAE=0.445
With sorting		Without sorting		With sorting		Without sorting	
(a) Binary distributed run length noise with run 10-100				(b) Gaussian distributed run length noise			

Fig. 10: watermarked image after adding binary distributed run length noise of run length 10 to 100 and Gaussian distributed run length noise and extracted watermark from it using (a) sorted coefficients of host and watermark while embedding the watermark. (b) Without sorting coefficients of host and watermark while embedding the watermark.

From Fig. 9 it is visible that though for small run length of binary distributed run length noise, performance of sorting and without sorting the coefficients is equal, for increased run length, sorting gives better robustness than without sorting the coefficients. From Fig. 10, we can see that sorting improves the performance for Gaussian distributed run length noise also.

Results for Resizing attack:

Image resizing is done by using bicubic interpolation. Two cases of resizing are applied. First, by doubling image in size and reducing it to its original size and second, by expanding image to four times its size and reducing it to original size. Results are shown in Fig. 11.









							
MAE=1.7	MAE=42.671	MAE=1.315	MAE=13.732	MAE=1.657	MAE=41.503	MAE=1.280	MAE=13.288
With sorting		Without sorting		With sorting		Without sorting	
(a) Resizing by doubling and reducing back to original				(b) Resizing by doubling and reducing back to original			

Fig. 11: watermarked image after resizing it to double the size and four times of its size and extracted watermark from it using (a) sorted coefficients of host and watermark while embedding the watermark. (b) Without sorting coefficients of host and watermark while embedding the watermark.

From Fig. 11 it is clear that sorting in case of resizing attack, does not prove better than without sorting.

COMPARISON OF PERFORMANCE UNDER VARIOUS ATTACKS WHEN TRANSFORM COEFFICIENTS OF HOST USED ARE SORTED AND UNSORTED FOR EMBEDDING PROCESS

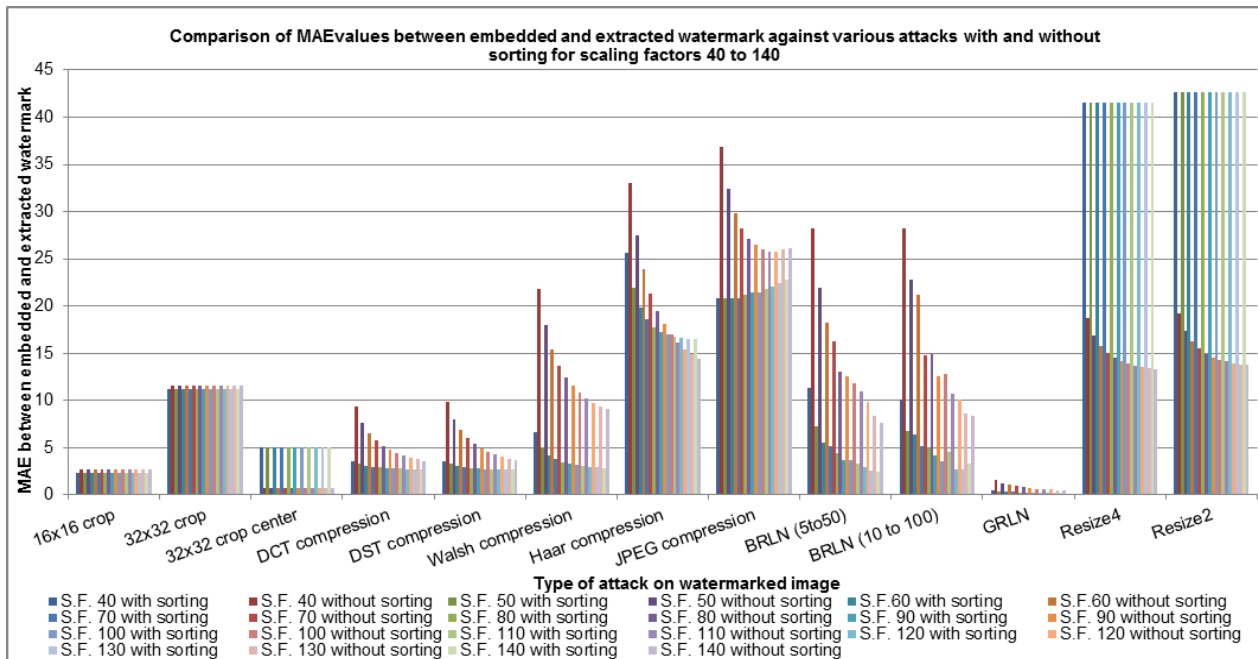


Fig. 12: Performance comparison of MAE values between embedded and extracted watermark against various attacks in proposed watermarking technique with and without sorting the transform coefficients of host and watermarked image while embedding the watermark (scaling factor values taken from 40 to 80 with the interval of 10)

From Fig. 12 above, it can be clearly seen that for attacks like 16x16 cropping and 32x32 cropping at corners of a watermarked image, sorting of host transform coefficients for embedding process gives lesser MAE values between embedded and extracted watermark. Though this difference is small it is observable. However, this does not hold true for 32x32 cropping at the centre of an image.

For all types of compression attacks i.e. using DCT, DST, Walsh, Haar transforms for compression of watermarked image and Jpeg compression, significant improvement is observed in the quality of watermark extracted from compressed watermarked image. Thus use of sorted coefficients of host as well as watermark in embedding process makes it more robust.

For, binary distributed run length noise and Gaussian distributed run length noise added to watermarked image also, the extracted watermark is observed to be closer to the embedded watermark when sorting of host and watermark coefficients is done. Only for binary distributed run length noise with less run length (run length 1 to 10) performs almost equal for sorted and unsorted coefficients of host and watermark.

CONCLUSION

The proposed method uses sorted host and watermark coefficients to embed the watermark. Thus for every watermark coefficient embedded in host image, we try to replace the closest host transform coefficient. This reduces the error introduced while embedding i.e. between host and watermarked image as well as the error between embedded and extracted watermark. For various attacks like 16x16 cropping, sorting of coefficients results into 1.13 times better performance than using unsorted coefficients and replacing them by watermark coefficients row by row. For DCT based compression it shows that similarity between embedded and extracted watermark is 1.3 times improved. For DST, Walsh, Haar based compression and JPEG compression this improvement is 1.4, 3.18, 0.87 and 1.14 times respectively. For binary distributed run length noise of length 5 to 50 and 10 to 100, quality of extracted watermark improves by 3.19 times and 2.53 times respectively. For Gaussian distributed run length noise attack, it is observed to be 2.7 times. Watermarking without sorting frequency coefficients of host and watermark better sustains against resizing attack.



REFERENCES

- [1] 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.
- [2] Dr. Kekre H. B. and Thepade Sudeep, "Image Retrieval using Non-Involutorial Orthogonal Kekre's Transform", International Journal of Multidisciplinary Research And Advances in Engineering, IJMRAE, Vol.1, No. 1, November 2009, pp. 189-203.
- [3] Amrik Singh, Balpreet Kaur, "Evaluating the performance of integrated SVD and visibility restoration digital watermarking", IPASJ, International Journal of Computer Science, Vol. 2, Issue 1, January 2014, pp. 16-22.
- [4] S.S. Sudha, K.K. Rahini, "Prevention of watermarking attacks using cryptography method", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 2, Feb 2014, pp. 5050-5053.
- [5] Manjit Thapa, Sandeep Kumar Sood, Meenakshi Sharma, "Digital image watermarking technique based on different attacks", International journal of advanced computer science and applications, Vol. 2., No. 4, 2011, pp. 14-19.
- [6] Henri Bruno Razafindrada, Nicolas Raft Razafindrakoto, Paul Auguste Randriamitantoa, "Improved watermarking scheme using discrete cosine transform and schur decomposition", International Journal of Computer Science and Network, Vol. 2, Issue 4, August 2013, pp. 25-31.
- [7] A. Umaamaheshvari, K. Thanushkodi, "A robust digital watermarking technique based on feature and transform method", Academic Journals, Vol. 8(32), August 2013, pp. 1584-1593.
- [8] Haijun Luo, Xingming Soon, Hengfu Yang, Zhihua Xia, "A robust image watermarking based on image restoration using SIFT", Radio Engineering, Vol. 20, No. 2, June 2011, pp. 525-532.
- [9] Wei Lu, Hongtao Lu, Fu-Lai Chung, "Feature based watermarking using watermark template match", Applied Mathematics and Computation, Elsevier publication, 2005.
- [10] 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, 2013, pp. 131-141.
- [11] Dr. H. B. Kekre, Dr. Tanuja Sarode, Shachi Natu, "Hybrid Watermarking of Colour Images using DCT-Wavelet, DCT and SVD", International Journal of Advances in Engineering and Technology, vol.6, Issue 2. May 2013.
- [12] 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, May 2013.
- [13] 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, July 2013, pp. 1139-1152.
- [14] Dr. H. B. Kekre, Dr. Tanuja Sarode, Shachi Natu, "Performance of watermarking system using wavelet column transform under various attacks", International Journal of Computer Science and Information Security, Vol. 12, No. 2, Feb 2014, pp. 30-35.
- [15] Dr. H. B. Kekre, Dr. Tanuja Sarode, Shachi Natu, "Robust watermarking scheme using column DCT wavelet transform under various attacks", International Journal on Computer Science and Engineering, Vol. 6, No. 1, Jan 2014, pp. 31-41.
- [16] Dr. H. B. Kekre, Dr. Tanuja Sarode, Shachi Natu, "Performance evaluation of watermarking technique using full, column and row DCT wavelet transform", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 3, Issue 1, Jan 2014.
- [17] Dr. H. B. Kekre, Dr. Tanuja Sarode, Shachi Natu, "Robust watermarking technique using hybrid wavelet transform generated from Kekre transform and DCT", International Journal of Scientific Research Publication, vol. 4, Issue 2, Feb 2014, pp. 1-13.
- [18] Dr. H. B. Kekre, Dr. Tanuja Sarode, Shachi Natu, "Effect of weight factor on the performance of hybrid column wavelet transform used for watermarking under various attacks", International Journal of Computer and Technology, Vol. 12, No. 10, March 2014, pp. 3997-4013.



Author' 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 17 papers in International Conferences/journal to her credit.