# Robust Watermarking Scheme using Column DCT Wavelet Transform under Various Attacks

H. B. Kekre,

Senior Professor
MPSTME, Department of Computer Engineering,
NMIMS University,
Mumbai, India
Email: hbkekre@yahoo.com

Tanuja Sarode,

Asssociate Professor
Thadomal Shahani Engineering College, Computer Engg. Department,
Mumbai, India
Email: tanuja_0123@yahoo.com

Shachi Natu,

Ph.D. Scholar
MPSTME, Department of Computer Engineering,
Mumbai, India
Email: shachi_natu@yahoo.com

***Abstract*— A novel watermarking scheme for color images has been proposed using column DCT wavelet transform. To improve the robustness of watermarking scheme, compressed watermark with tolerable fidelity is embedded into host image. Middle frequency coefficients are selected for embedding watermark so that the proposed scheme can sustain attacks like lossy image compression where high frequency coefficients are eliminated from watermarked image. Performance of proposed scheme is evaluated against image resizing, varieties of cropping, compression and noise attacks like binary distributed and Gaussian distributed run length noise. Due to column transform instead of full transform, proposed scheme also gives computational efficiency.**

***Keywords- Watermarking; DCT wavelet transform; binary;Gaussian;Runlength noise***

## I. INTRODUCTION

With rapid growth of internet usage, access to digital data has become quite easier. It has also made manipulation of digital contents easy. Hence there is a need to protect the copyright of digital contents against unauthorized alteration. Watermarking is the solution arisen through this need. Watermarking allows hiding the information of owner of digital data like image, audio or video into the data itself thereby providing protection of copyright of digital data. Digital image watermarking can be done in spatial domain or frequency domain. Though the spatial domain watermarking is easier to perform, it does not withstand attacks that can alter the digital data. It also directly affects the pixel values of an image. Hence requirement of robustness and perceptual quality of watermarked image has opened new gateways for frequency domain watermarking. In frequency domain watermarking, transforms like DCT, DFT, Wavelet transforms, Singular Value Decomposition are more popular. Mix of multiple transforms has also proved more robust. Selection of proper frequency bands is of utmost importance for embedding the watermark. In literature, it has been observed that embedding watermark in high frequency sub bands will cause minimal loss of information from host image. But this causes loss of watermark information when watermarked contents are subjected to attacks like lossy image compression. Embedding watermark in low frequencies degrades the perceptual quality of watermarked image and this makes detection of watermark very easy. Hence normally watermark is embedded in middle frequency components of host images. However, in literature there are many methods by which watermark can be embedded in low frequencies and still better imperceptibility and robustness can be achieved.

In this paper a novel robust watermarking scheme using DCT wavelet transform generated using Kekre's algorithm [1] is proposed. Instead of decomposing host image into various levels of wavelet coefficients, only column wise transform is applied to host and watermark image. This prevents the loss of image contents due to

multilevel wavelet decomposition of an image and makes the scheme computationally efficient. Instead of embedding all frequency coefficients, compressed watermark is embedded into host image which causes less distortion in host image and hence gives better imperceptibility. Proposed scheme is evaluated against various attacks such as: cropping, lossy image compression achieved using DCT, DST and Walsh transforms, JPEG compression, binary distributed run length noise, Gaussian distributed run length noise and image resizing.

Rest of the paper is organized as follows. Section II briefly explains related work in the field of digital image watermarking. Proposed scheme is presented in section III. Section IV presents the results of performance of proposed scheme under various attacks. Finally section V concludes the paper.

## II. RELATED WORK

Kaushik Deb, Md. Sajib Al-Seraj, Md. Moshiul Hoque and Md. Iqbal Hasan Sarkar in [2] have proposed a wavelet and DCT based watermarking technique in which watermark is embedded as a bit stream in low frequency DCT coefficients of HL frequency components. Two uncorrelated pseudorandom sequences are generated to embed watermark bit 1 and watermark bit 0 using a key. Weighted correction is used to improve the invisibility of the watermark. The technique is proved to be robust for JPEG compression, contrast adjustment, cropping and noise attacks. In [3], Gil-Je Lee, Eun-Jun Yoon, Kee-Young Yoo proposed a multiple digital watermarking scheme. The proposed scheme is divided into two phases, Grayscale watermark phase and binary watermark phase. In first phase, grayscale watermark is embedded in original image by dividing it into blocks and calculating average of each block. In second phase, binary watermark is embedded by generating polarity matrices from original image and grayscale watermark. Reverse procedure is followed to extract the watermarks.

Wei Wang, Aidong Men, Bo Yang and Xiaobo Chen in [4] proposed DWT-SVD based watermarking scheme. Single level wavelet decomposition is applied to image. SVD is applied to LL sub-band. Origin of LL sub band, height and width of LL sub band and U and V matrices obtained from Singular Value Decomposition of LL sub band are concatenated into a bit stream. Chaotic sequence is generated using initial value i and then converted into binary. Bit stream and this binary sequence are then hashed to generate a key. These secrete key and initial value i are registered in a third party intellectual property for copyright protection.

Haohao Song, Zihua Qiu, Jian Gu in [5], proposed a semi-fragile watermarking scheme based on wavelets. Image is decomposed into wavelet frequency sub bands up to third level. Watermark is generated from wavelet coefficients of LL frequency band by condition judgment based on the mean value. Watermark is then embedded into predetermined bit plane of LH2, HL2 and HH3 frequency bands. Ouazzane Hana, Mahersia Hela, Hamrouni Kamel in [6] proposed wavelet based robust multi-watermarking scheme. In this scheme, host image is wavelet decomposed up to desired level n. A binary watermark image is embedded into LL and HH frequency bands by modifying it with appropriate scaling factor. In [7], Muhammad Imran, Abdul Ghafoor, Muhammad Rizwan Khokher proposed a non-blind color image watermarking scheme using Principle Component Analysis (PCA), DWT and SVD. R, G, B color channels are uncorrelated using PCA. The first Principle component which contains most of the image information is selected for watermark embedding. Second level wavelet of this principle component is performed. Singular values of each sub band are obtained and then modified to embed the watermark. Reverse process is applied to extract the watermark. Dr. M. A. Dorairangaswamy, B. Padhmavathi in [8], proposed an invisible blind watermarking scheme. Mean of each non-overlapping 2x2 block of host image is calculated and divided by embedding strength. This value is then used along with two different functions for embedding bit 1 and 0 of watermark. Every pixel of binary watermark is embedded into 2x2 size block of host image. Taha Jassim and Raed Abd-Alhameed and Hussain Al-Ahmad in [9] proposed robust and fragile watermarking scheme for color images captured by mobile phones. Robust watermarking is used for copyright protection whereas fragile watermarking is used for image authentication. The mobile phone number including its international code is used as robust watermark and is embedded in frequency domain. Hash numbers are used as fragile watermark and are embedded in spatial domain of R G B channels. These hash values are calculated using rows of host image except first row and inserted in the first row of host image. Robust watermarking survives against several attacks whereas fragile watermarking detects any tampering to an image. Chun-Yu Lin and Chung-Yen Su proposed an improved wavelet tree based watermarking scheme in [10]. According to their scheme, image is divided into four level sub bands and grouped the sub band coefficients into many wavelet trees. N bit watermark is embedded in first N shuffled trees. Changing only one coefficient of each tree is proposed to embed the watermark.

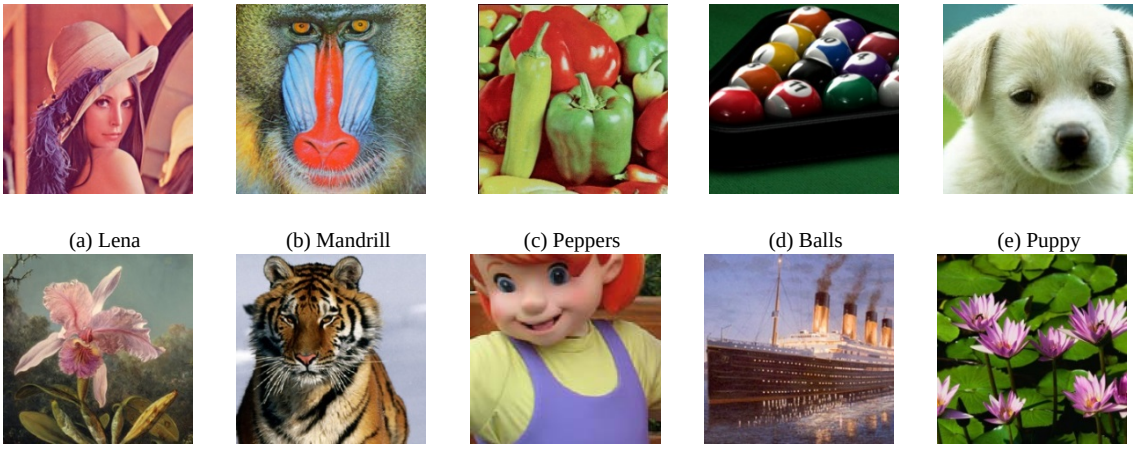
Mohd Rizal Mohd Isa and Salem Aljareh proposed a DCT based watermarking scheme in [11] to protect the biometric images especially for face recognition. Addition of watermarking scheme does not highly affect the recognition rate and better recognition rate is observed by authors under various attacks on biometric images. Jagdish C. Patra, Jiliang E. Phua and Deepu Rajan in [12] presented a novel Chinese Remainder Theorem (CRT) based watermarking scheme that works in the Discrete Cosine Transform (DCT) domain. Host image is divided into 8x8 blocks and DCT is applied to them. To embed watermark bits appropriate co-prime values are selected in

CRT algorithm. Dongyang Teng, Renghui Shi, Xiaoqun Zhao proposed the DCT image watermarking technique based on the mix of time-domain in [13]. Host image is divided into blocks and mixed with orthogonal matrices in time domain. A host image mixed in the time domain is subjected to DCT and watermark is embedded in frequency domain. Combination of pre-transformation in time-domain with DCT, disperse the noise and make the recovered watermarking image clearer. B.L. Gunjal and R. R. Manthalkar in [14] presented strongly robust digital image watermarking scheme based on 'Discrete Wavelet Transform', by embedding scrambled watermark in middle frequency sub band. The security levels are increased by generating PN sequence depending on periodicity of watermark image. The image scrambling is applied by Arnold Transform. The decomposition is done with Haar which is simple, symmetric and orthogonal wavelet and the direct weighting factor is used in watermark embedding and extraction process. Gerardo Pineda Betancourth in [15] presented a fragile watermarking scheme for image authentication. It has the ability to localize the tampered regions. In their proposed scheme, only few number of wavelet coefficients are watermarked but all are implicitly protected. This reduces embedding distortion. Other key features of this method are that it is key dependent, content based and nondeterministic neighborhood-dependent method. Hence it can resist attacks like transplantation attacks and vector quantization attacks.

In [16], Ezz El-Din Hemdan1, Nawal El-Fishaw, Gamal Attiya1, and Fathi Abd El-Samii proposed hybrid watermarking technique which is based on DWT and SVD. Before embedding, two watermarks primary and secondary are fused using wavelet fusion algorithm. This fused watermark is embedded into singular values of one level wavelet decomposed cover image using appropriate scaling factor. This technique improved both the capacity of the embedded information and robustness without affecting the perceptual quality of the original image. In [17], Nagaraj V. Dharwadkar, B. B. Amberker & Avijeet Gorai proposed a non-blind watermarking scheme for color images. In their proposed scheme, watermark is embedded in blue channel of cover image. Blue channel of cover image is subjected to wavelet decomposition and then singular values of each sub band are obtained. Singular values of watermark are embedded in these singular values of blue channel. Embedding watermark in all four sub bands makes it very difficult to remove. M.A. Dorairangaswamy proposed a blind watermarking scheme in [18]. This research work presents a robust and blind watermarking scheme for copyright protection against piracy of digital images. This scheme makes use of a binary image as watermark data for protecting the copyrights of the digital image. Here, for every pixel of the host image, a binary watermark image pixel is embedded on the basis of the gain factor and the generated random matrix. The embedded binary watermark is extracted from the watermarked image using watermark image size and the correlation coefficient. K.-C. Liu, C.H. Chou proposed a robust and transparent watermarking scheme for color images in [19]. Watermark is embedded in perceptually significant sub bands of luminance and chrominance components of color image in wavelet domain. The higher perceptual redundancy in each color component of the color image indicates that the great strength of the watermark can be embedded into the color image for higher robustness without resulting in visible distortion. Robust watermarking scheme is proposed by Yasunori Ishikawa, Kazutake Uehira and Kazuhisa Yanaka in [20]. In their proposed technique of optical watermarking in which size of pixel blocks is varied by a trade-off in the efficiency of embedded watermarking. 4x4, 8x8, and 16x16 pixels were used in one block to embed one bit of watermark. A detection accuracy of 100% was obtained by using a block with 16x16 pixels.

## III. PROPOSED SCHEME

Proposed scheme has been experimented on the dataset of 10 color host images of size 256x256 and 5 color images of size 128x128 as watermarks. Figure 1 and Figure 2 show the host images and watermark images used in the scheme.



(a) Lena (b) Mandrill (c) Peppers (d) Balls (e) Puppy

(f) Flower (g) Tiger (h) Cartoon (i) Titanic (j) Waterlili

Figure 1. Cover images used for experimentation


(a)Austral (b) Bear (c) CCD (d) Logo (e)Nmims

Figure 2. Watermark images used for experimentation

Steps in embedding of watermark are as follows:

**Step 1.** Compress the watermark with compression ratio 2.67 by applying column DCT wavelet transform to it.

**Step 2.** Compress the host image with compression ratio 1.1 by applying column DCT wavelet transform to it.

**Step 3.** These compression ratios are selected based on appropriate level of perceptibility of compressed image without visual loss of information from image.

**Step 4.** Normalize the transformed watermark.

**Step 5.** Strength of normalized watermark is increased by using suitable weight to make it robust against various attacks.

**Step 6.** Replace mid-frequency coefficients of host image by transform coefficients of weighted normalized watermark obtained in Step 4. These mid-frequency coefficients are selected from compressed host.

**Step 7.** Replace remaining high frequency coefficients of compressed host by its original transform coefficients to reduce the error.

**Step 8.** Take inverse column DCT wavelet transform of host image obtained in step 6 to get watermarked image.

**Step 9.** Imperceptibility of proposed scheme is measured by calculating Mean Absolute Error (MAE) between host image and watermarked image.

Steps in extraction of watermark are as given below:

**Step 1.** Take the column DCT wavelet transform of watermarked image.

**Step 2.** Extract the mid-frequency coefficients of transformed watermarked image.

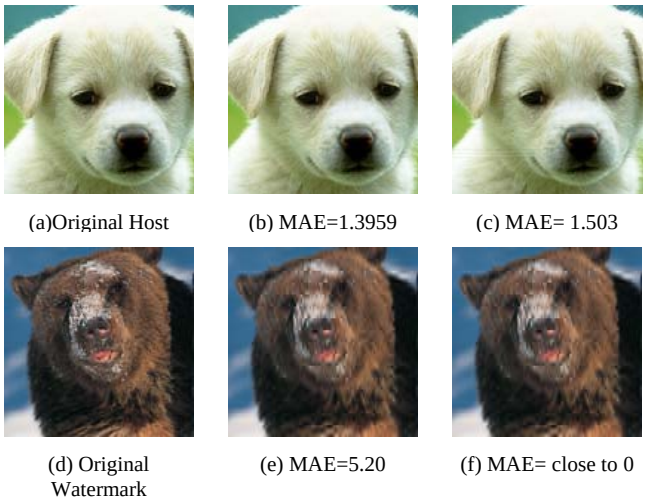
**Step 3.** Reduce the strength of these coefficients by same weight.

**Step 4.** Denormalize the coefficients obtained from Step 3.

**Step 5.** Take inverse column DCT wavelet transform to recover watermark.

**Step 6.** Robustness of extracted watermark is measured by calculating Mean Absolute Error (MAE) between compressed watermark and recovered watermark.

Result images for embedding and extraction of watermark are shown in Figure 3.



(a)Original Host (b) MAE=1.3959 (c) MAE= 1.503

(d) Original Watermark (e) MAE=5.20 (f) MAE= close to 0

Figure 3. Cover images used for experimentation (a)Original Host 'Puppy' (b)Compressed host (c)watermarked Image (d)Original watermark 'bear' (e)Compressed watermark 'bear' (f)Extracted watermark 'bear'

Table I below shows average of MAE values between host and watermarked images and MAE between embedded and extracted watermark over ten host images for each of five watermarks. Strong robustness can be observed from Table I since MAE between embedded and extracted watermark is close to zero for all watermarks.

TABLE I. AVERAGE MEAN ABSOLUTE ERROR (MAE) BETWEEN TEN HOST AND WATERMARKED IMAGES AND AVERAGE MAE BETWEEN EMBEDDED AND EXTRACTED WATERMARK FOR FIVE WATERMARKS USED IN SIMULATION WORK

| Watermark | Average MAE between compressed host and watermarked image | Average MAE between embedded compressed watermark and extracted watermark |
|---|---|---|
| Nmims | 2.719 | Close to 0 |
| Austral | 2.731 | Close to 0 |
| Ccd | 2.710 | Close to 0 |
| Logo | 2.705 | Close to 0 |
| Bear | 2.687 | Close to 0 |

## IV. PERFORMANCE OF PROPOSED SCHEME UNDER VARIOUS ATTACKS:

### *A. Lossy compression of watermarked image using DCT wavelet:*

Watermarked image is subjected to compression with compression ratio 1.95 under column DCT wavelet transform. From this compressed watermarked image, watermark is extracted using extraction procedure. Proposed scheme shows excellent performance for compression attack. Some result images are given below in Figure 4.


(a) (b) MAE=2.407 (c) MAE=2.053 (d) (e) MAE= 2.407 (f) MAE=1.782

Figure 4. Result images for compression attack with compression ratio 1.95 (a) 'Puppy' watermarked with 'austral' (b)watermarked 'Puppy' after compression (c)extracted watermark 'austral' (d) 'Puppy' watermarked with 'nmims' (e) watermarked 'Puppy' after compression (f) extracted watermark 'nmims'

### *B. Compression of watermarked image using other orthogonal transforms like DCT, DST and Walsh:*

Watermarked images are subjected to compression with compression ratio 1.14. But here instead of using same column transform as that of used in watermark embedding (i.e. DCT wavelet) orthogonal transforms like DCT, DST and Walsh are applied column wise to watermarked images. Figure 5 shows result images for 'puppy' when subjected to compression using column DCT transform. Figure 6 and Figure 7 show result images for 'puppy' when subjected to compression using column DST transform and column Walsh transform respectively.


(a) (b) MAE=0.975 (c) MAE=18.69 (d) (e) MAE= 0.975 (f) MAE=19.45

Figure 5. Result images for compression of watermarked image using column DCT transform (a) 'Puppy' watermarked with 'austral' (b)watermarked 'Puppy' after compression (c)extracted watermark 'austral' from compressed 'puppy' (d) 'Puppy' watermarked with 'nmims' (e) watermarked 'Puppy' after compression (f) extracted watermark 'nmims' from compressed 'puppy'


(a) (b) MAE=1.076 (c) MAE=19.29 (d) (e) MAE= 0.975 (f) MAE=20.07

Figure 6. Result images for compression of watermarked image using column DST transform (a) 'Puppy' watermarked with 'austral' (b)watermarked 'Puppy' after compression (c)extracted watermark 'austral' from compressed 'puppy' (d) 'Puppy' watermarked with 'nmims' (e) watermarked 'Puppy' after compression (f) extracted watermark 'nmims' from compressed 'puppy'


(a) (b) MAE=1.57 (c) MAE=33.35 (d) (e) MAE= 1.57 (f) MAE=34.90

Figure 7. Result images for compression of watermarked image using column Walsh transform (a) 'Puppy' watermarked with 'austral' (b)watermarked 'Puppy' after compression (c)extracted watermark 'austral' from compressed 'puppy' (d) 'Puppy' watermarked with 'nmims' (e) watermarked 'Puppy' after compression (f) extracted watermark 'nmims' from compressed 'puppy'

### *C. JPEG compression attack:*

Watermarked images are subjected to JPEG compression attack with quality factor 100. Results of JPEG compression attack are shown in Figure 8.


(a) (b) MAE=0.005 (c) MAE=45.99 (d) (e) MAE= 0.005 (f) MAE=41.95

Figure 8. Result images for JPEG compression (Quality factor 100) of watermarked image (a) 'Puppy' watermarked with 'austral' (b)watermarked 'Puppy' after JPEG compression (c)extracted watermark 'austral' from JPEG compressed 'puppy' (d) 'Puppy' watermarked with 'nmims' (e) watermarked 'Puppy' after JPEG compression (f) extracted watermark 'nmims' from JPEG compressed 'puppy'

Table II shows average of MAE values between host and watermarked images labelled as MAE1. It also shows average MAE values between embedded and extracted watermark for compression of watermarked images achieved using different transforms. Values in Table II indicate that, proposed scheme is strongly robust for lossy compression performed using the same transform used for embedding watermark. At the same time it shows good resistance to lossy compression obtained using orthogonal transforms like DCT, DST and Walsh transforms. Among these transforms, compression using DCT is better than DST and Walsh. JPEG compression shows acceptable level of robustness.

TABLE II. AVERAGE MEAN ABSOLUTE ERROR BETWEEN HOST AND WATERMARKED IMAGE (MAE1) AND AVERAGE MAE BETWEEN EMBEDDED AND EXTRACTED WATERMARK (MAE2) FOR FIVE WATERMARKS USED IN SIMULATION WORK UNDER COMPRESSION ATTACKTABLE TYPE STYLES

| Watermark | Compression attack using | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | *DCT wavelet* | | *DCT* | | *DST* | | *Walsh* | | *JPEG* | |
| | ***MAE1*** | ***MAE2*** | ***MAE1*** | ***MAE2*** | ***MAE1*** | ***MAE2*** | ***MAE1*** | ***MAE2*** | ***MAE1*** | ***MAE2*** |
| nmims | 3.794 | 1.782 | 1.378 | 29.144 | 1.425 | 29.281 | 2.279 | 53.501 | 0.059 | 69.833 |
| austral | 3.794 | 2.053 | 1.378 | 27.948 | 1.425 | 28.085 | 2.280 | 51.534 | 0.059 | 64.666 |
| ccd | 3.794 | 2.568 | 1.377 | 35.059 | 1.424 | 35.216 | 2.278 | 64.433 | 0.060 | 78.673 |
| logo | 3.793 | 0.576 | 1.378 | 35.077 | 1.425 | 35.236 | 2.279 | 64.457 | 0.059 | 79.772 |
| bear | 3.793 | 0.650 | 1.376 | 18.088 | 1.423 | 18.178 | 2.276 | 33.065 | 0.057 | 41.756 |

### *D. Cropping watermarked image:*

Watermarked image is cropped at four corners. 16x16 and 32x32 size squares are cropped. Also 32x32 size square is cropped at the center of an image. Results of cropping attack are shown in following Figure 9 to Figure 11.


(a) (b) MAE=1.542 (c) MAE=3.656 (d) (e) MAE= 1.542 (f) MAE=2.638

Figure 9. Result images for cropping 16x16 squares at four corners of watermarked image (a) 'Puppy' watermarked with 'austral' (b)watermarked 'Puppy' after cropping 16x16 square at four corners (c)extracted watermark 'austral' from cropped 'puppy' (d) 'Puppy' watermarked with 'nmims' (e) watermarked 'Puppy' after cropping 16x16 square at four corners (f) extracted watermark 'nmims'


(a) (b) MAE=11.77 (c) MAE=12.60 (d) (e) MAE= 11.77 (f) MAE=10.35

Figure 10. Result images for cropping 32x32 squares at four corners of watermarked image (a) 'Puppy' watermarked with 'austral' (b)watermarked 'Puppy' after cropping 32x32 square at four corners (c)extracted watermark 'austral' from cropped 'puppy' (d) 'Puppy' watermarked with 'nmims' (e) watermarked 'Puppy' after cropping 32x32 square at four corners (f) extracted watermark 'nmims'


(a) (b) MAE=1.583 (c) MAE=0.582 (d) (e) MAE= 1.583 (f) MAE=0.821

Figure 11. Result images for cropping 32x32 squares at centre of watermarked image (a) 'Puppy' watermarked with 'austral' (b)watermarked 'Puppy' after cropping 32x32 square at centre (c)extracted watermark 'austral' from cropped 'puppy' (d) 'Puppy' watermarked with 'nmims' (e) watermarked 'Puppy' after cropping 32x32 square at centre (f) extracted watermark 'nmims'

Table III shows performance of proposed scheme against cropping attack. Cropping 32x32 size square at center of watermarked image performs best among all types of cropping attacks. Cropping at corners of watermarked image also shows strong robustness.

TABLE III. AVERAGE MEAN ABSOLUTE ERROR (MAE) BETWEEN HOST AND WATERMARKED IMAGE AND AVERAGE MAE BETWEEN EMBEDDED AND EXTRACTED WATERMARK FOR FIVE WATERMARKS USED IN SIMULATION WORK UNDER CROPPING ATTACK

| Watermark | Type of attack | | | | | |
|---|---|---|---|---|---|---|
| | *Cropping 16x16 squares at four corners* | | *Cropping 32x32 squares at four corners* | | *Cropping 32x32 squares at center* | |
| | ***Average MAE between host and watermarked image*** | ***Average MAE between embedded and extracted watermark*** | ***Average MAE between host and watermarked image*** | ***Average MAE between embedded and extracted watermark*** | ***Average MAE between host and watermarked image*** | ***Average MAE between embedded and extracted watermark*** |
| nmims | 2.188 | 2.638 | 6.691 | 10.350 | 1.752 | 0.821 |
| austral | 2.188 | 3.656 | 6.691 | 12.608 | 1.752 | 0.582 |
| Ccd | 2.188 | 1.146 | 6.690 | 9.716 | 1.752 | 0.183 |
| Logo | 2.188 | 0.912 | 6.690 | 3.615 | 1.752 | 0.165 |
| Bear | 2.188 | 2.359 | 6.691 | 6.655 | 1.752 | 0.060 |

### *E. Binary distributed run length noise:*

Noise with random run and discrete magnitude of -1 and 1 is generated with equal probabilities. This noise is then added to the watermarked image. From the attacked watermarked image watermark is extracted by following the extraction procedure. Figure 12 shows the noise added images and watermarks extracted from them. Proposed scheme shows excellent robustness against this attack.


(a) (b) MAE=1 (c) MAE=close to 0 (d) (e) MAE= 1 (f) MAE=close to 0

Figure 12. Result images for binary distributed run length noise added to watermarked image (a) 'Puppy' watermarked with 'austral' (b)watermarked 'Puppy' after adding noise (c)extracted watermark 'austral' from noise added 'puppy' (d) 'Puppy' watermarked with 'nmims' (e) watermarked 'Puppy' after adding noise (f) extracted watermark 'nmims' from noise added 'puppy'

### *F. Gaussian distributed run length noise:*

In Gaussian distributed type of noise, once again noise of variable run length with discrete magnitude in the range of -2 to 2 is generated and added to the image. Extraction procedure is followed to recover watermark from attacked watermarked image. Figure 13 shows the noise added images and watermarks extracted from them. Proposed scheme shows excellent robustness against this attack.


(a) (b) MAE=0.746 (c) MAE=3.22 (d) (e) MAE= 0.746 (f) MAE=3.359

Figure 13. Result images for Gaussian distributed run length noise added to watermarked image (a) 'Puppy' watermarked with 'austral' (b)watermarked 'Puppy' after adding noise (c)extracted watermark 'austral' from noise added 'puppy' (d) 'Puppy' watermarked with 'nmims' (e) watermarked 'Puppy' after adding noise (f) extracted watermark 'nmims' from noise added 'puppy'

Table IV shows performance of proposed scheme against two different types of noises namely binary distributed run length noise and Gaussian distributed run length noise. For both type of noises, high level of robustness is achieved.

TABLE IV. AVERAGE MEAN ABSOLUTE ERROR BETWEEN HOST AND WATERMARKED IMAGE (MAE1) AND AVERAGE MAE BETWEEN EMBEDDED AND EXTRACTED WATERMARK (MAE2) FOR FIVE WATERMARKS USED IN SIMULATION WORK UNDER BINARY DISTRIBUTED RUN LENGTH NOISE AND GAUSSIAN DISTRIBUTED RUN LENGTH NOISE ATTACK

| Watermark | Type of noise added to watermarked image | | | |
|---|---|---|---|---|
| | *Binary distributed Run length* | | *Gaussian distributed Run length* | |
| | ***MAE1*** | ***MAE2*** | ***MAE1*** | ***MAE2*** |
| Nmims | 1 | Close to 0 | 0.746 | 3.359 |
| Austral | 1 | Close to 0 | 0.746 | 3.224 |
| Ccd | 1 | Close to 0 | 0.746 | 4.042 |
| Logo | 1 | Close to 0 | 0.746 | 4.043 |
| Bear | 1 | Close to 0 | 0.746 | 2.086 |

*G. Image resizing:*

Watermarked image is resized to four times of its original size and back to original size (Type 1) using bicubic interpolation. Another attempt made in resizing is that watermarked image is resized to double of its original size and then reduced back to its original size (Type 2). Sample image results for Type 1 and Type 2 resizing attack are shown in Figure 14 and Figure 15 respectively.


(a) (b) MAE=1.125 (c) MAE=20.4 (d) (e) MAE= 1.125 (f) MAE=21.51

Figure 14. Result images for Type 1 image resizing attack on watermarked image (a) 'Puppy' watermarked with 'austral' (b)watermarked 'Puppy' after resizing (c)extracted watermark 'austral' from resized 'puppy' (d) 'Puppy' watermarked with 'nmims' (e) watermarked 'Puppy' after resizing (f) extracted watermark 'nmims' from resized 'puppy'


(a) (b) MAE=1.096 (c) MAE=19.84 (d) (e) MAE= 1.096 (f) MAE=20.92

Figure 15. Result images for Type 2 image resizing attack on watermarked image (a) 'Puppy' watermarked with 'austral' (b)watermarked 'Puppy' after resizing (c)extracted watermark 'austral' from resized 'puppy' (d) 'Puppy' watermarked with 'nmims' (e) watermarked 'Puppy' after resizing (f) extracted watermark 'nmims' from resized 'puppy'

Table V shows average MAE values between host and watermarked images and between embedded and extracted image for two types of resizing attacks obtained using bicubic interpolation. High imperceptibility and acceptable level of robustness is achieved in both cases.

TABLE V. AVERAGE MEAN ABSOLUTE ERROR BETWEEN HOST AND WATERMARKED IMAGE (MAE1) AND AVERAGE MAE BETWEEN EMBEDDED AND EXTRACTED WATERMARK (MAE2) FOR FIVE WATERMARKS USED IN SIMULATION WORK UNDER RESIZING ATTACK

| **Watermark** | **Type of resizing done** | | | |
|---|---|---|---|---|
| | ***Original-4times-original*** | | ***Original-double-original*** | |
| | ***MAE1*** | ***MAE2*** | ***MAE1*** | ***MAE2*** |
| Nmims | 1.721 | 33.822 | 1.766 | 34.738 |
| Austral | 1.721 | 32.117 | 1.766 | 32.986 |
| Ccd | 1.882 | 40.193 | 1.931 | 41.247 |
| Logo | 1.720 | 40.238 | 1.766 | 41.328 |
| Bear | 1.719 | 20.188 | 1.764 | 20.726 |

## V. CONCLUSION:

Embedding compressed watermark in host image, improves the perceptual quality of watermarked image. Compression ratio for watermark compression is selected such that it will not cause significant loss of information from watermark.

Simply normalizing the transform of watermark does not guarantee the robustness. However, increasing strength of normalized watermark with suitable weight factor makes it sustainable against various attacks performed in simulation work.

Applying column transform instead of full transform during watermarking, significantly reduces computational overhead. Hence the proposed scheme is proved computationally much efficient than other wavelet based techniques proposed in [21-24].

Also Mean Absolute Error between original and extracted watermark without performing any attack on watermarked image is close to zero in proposed scheme. In previously presented watermarking techniques in [21-24], this error is high due to multilevel wavelet decomposition as at each level of decomposition, some error is introduced in image itself. Higher imperceptibility is also a considerable characteristic of proposed watermarking scheme than the techniques in [21-24].

Proposed scheme gives excellent performance for noise attacks and cropping attacks.

## REFERENCES


[1] H.B.Kekre, Archana Athwale, Dipali Sadavarti, "Algorithm to Generate Wavelet Transform from an Orthogonal Transform", International Journal of Image Processing, Vol.4, Issue 4, pp. 444-455, 2010.

[2] Kaushik Deb, Md. Sajib Al-Seraj, Md. Moshiul Hoque and Md. Iqbal Hasan Sarkar "Combined DWT-DCT Based Digital Image Watermarking Technique for Copyright Protection", In IEEE proc. of 7th International Conference on Electrical and Computer Engineering, 2012, pp. 458-461.

[3] Gil-Je Lee, Eun-Jun Yoon, Kee-Young Yoo, "A Novel Multiple Digital Watermarking Scheme for the Copyright Protection of Image", In Proc. of Fourth International Conference on Innovative Computing, Information and Control, 2009, pp. 756-759.

[4] Wei Wang, Aidong Men, Bo Yang and Xiaobo Chen, "A novel robust zero watermarking scheme based on DWT and SVD", In proc. of IEEE 4th International Congress on Image and Signal Processing, 2011, pp. 1012-1015.

[5] Haohao Song, Zihua Qiu, Jian Gu, "A Novel Semi-fragile Image Watermarking Scheme Based on Wavelet", In Proc. of IEEE, ICALIP, 2010, pp. 1504-1510.

[6] Ouazzane Hana, Mahersia Hela, Hamrouni Kamel, "A Robust Multiple Watermarking Scheme Based on the DWT", In IEEE Proc. of 10th International Multiconference on Systems, Signals and Devices, 2013, pp. 1-6.

[7] Muhammad Imran, Abdul Ghafoor, Muhammad Rizwan Khokher, "A Robust Non-blind Color Image Watermarking Scheme", In IEEE Proc. of 12th International Conference on Control, Automation, Robotics & Vision, 2012, pp. 1392-1396.

[8] Dr. M. A. Dorairangaswamy, B.Padhmavathi, "An Effective Blind Watermarking Scheme for Protecting Rightful Ownership of Digital Images", In IEEE Proc. of TENCON, 2009, pp. 1-6.

[9] Taha. Jassim and Raed Abd-Alhameed and Hussain Al-Ahmad, "New Robust and Fragile Watermarking Scheme for Colour Images Captured by Mobile Phone Cameras", In IEEE Proc. of 15th International Conference on Computer Modelling and Simulation, 2013, pp. 465-469.

[10] Chun-Yu Lin and Chung-Yen Su proposed an improved wavelet tree based watermarking scheme, "An Improved Wavelet-tree Watermarking Scheme", IEEE International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS 2012), pp. 275-279.

[11] Mohd Rizal Mohd Isa and Salem Aljareh, "Biometric Image Protection Based on Discrete Cosine Transform Watermarking Technique", In IEEE Proc. of International Conference on Engineering and Technology (ICET), 2012 , pp.1-5.

[12] Jagdish C. Patra, Jiliang E. Phua and Deepu Rajan in, "DCT domain watermarking scheme using Chinese remainder theorem (CRT) for image authentication", In IEEE Proc. of ICME, 2010, pp. 111-116.

[13] Dongyang Teng, Renghui Shi, Xiaoqun Zhao proposed the DCT image watermarking technique based on the mix of time-domain, "DCT Image Watermarking Technique Based on the Mix of Time-domain", In IEEE Proc. of International Conference on Information Theory and Information Security (ICITIS), 2010, pp. 826-830.

[14] B.L. Gunjal and R.R.Manthalkar, "Discrete Wavelet Transform based Strongly Robust Watermarking Scheme for Information Hiding in Digital Images", In IEEE Proc. of 3rd International Conference on Emerging Trends in Engineering and Technology (ICETET), 2010, pp. 124-129.

[15] Gerardo Pineda Betancourth, "Fragile Watermarking Scheme for Image Authentication", In IEEE Proc. of 5th International Conference on Human System Interactions, 2012, pp. 168-174.

[16] Ezz El-Din Hemdan1, Nawal El-Fishaw/, Gamal Attiya1, Fathi Abd El-Samii,"Hybrid Digital Image Watermarking Technique for Data Hiding", 2013, pp. 220-228.

[17] Nagaraj V. Dharwadkar, B. B. Amberker & Avijeet Gorai, "Non-blind Watermarking scheme for color images in RGB space using DWT-SVD", In Proc. of IEEE Proc. of International Conference on Communications and Signal Processing (ICCSP), 2011, pp. 489-493.

[18] M.A. Dorairangaswamy, "Protecting Digital-Image Copyrights: A Robust and Blind Watermarking Scheme", In IEEE Proc. of First International Conference on Networked Digital Technologies, 2009, pp. 423-428.

[19] K.C. Liu, C.H. Chou, "Robust and transparent watermarking scheme for colour images", IET Image Processing, Vol. 3, Issue 4, 2009, pp. 228–242.

[20] Yasunori Ishikawa, Kazutake U ehira and Kazuhisa Yanaka, "Robust Optical Watermarking Technique by Optimizing the Size of Pixel Blocks of Orthogonal Transform", In IEEE Proc. of Industry Applications Society Annual Meeting (IAS), 2011, pp. 1-6.

[21] 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.

[22] 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.

[23] 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.

[24] 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.


## AUTHORS PROFILE

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 more than 150 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 09 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 15 papers in International Conferences/journal to her credit.