Secure Extraction of Image Data based on Optimized Transform Method

Reena Gunjan
Dept. of E &TC,
Cummins College of Engg. for Women, Pune, India
email: reenagunjan@gmail.com

Priyam Pandia
Software Developer
SAP (India Limited)
Bangalore, India
email: priyampandia@gmail.com

Rajeev Mohnot,
Vice President,
Meryll Lynch, Bank of America,
New Jersey, USA
email: mohnotr@gmail.com

***Abstract*— A novel method is proposed which deals with secure extraction of data by utilizing transform based image watermarking techniques. The image is embedded with a watermark using a combination of Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT) and Discrete Wavelet Transform (DWT) in this scheme. The conventional transforms are applied in an optimized mode in these schemes in different spatial regions of the image to embed a watermark. The scheme is subjected to Signal processing attacks and Geometric attack to test against the robustness of the image. The watermarking of image is made secure by testing against unauthorized detection techniques employed by attackers. This is realized by a correlation based detector applied to the scheme. Experimental results show that the watermarked image is robust and secure against Signal Processing attacks, Geometric attacks and unauthorized Detection attacks.**

***Index Terms*—Digital Watermarking, Blind watermark detection, Correlation detector, Secure Watermark**

I. INTRODUCTION

The rapid advances in the field of computing by making use of Internet have grown many folds over recent years. The information is communicated through Internet in the form of digital images, audio and video. It is now very easy to access digital data over the Internet and copy, modify and distribute it at one's own convenience. This depicts advancement in technology but at the same time poses a threat to the security of multi-media content. The attackers or hackers can intercept data and corrupt it. At the same time there are issues related to the copyright ownership of the data. Digital Watermarking [1] has been in vogue for many years to maintain the integrity of the data. In this technique, a watermark is embedded in the digital images or artwork. A watermark [2] can be visible or invisible. It can be a text, image, symbol or logo of an organization. The technique involves in placing it in such a position that it is difficult to remove it. To prove the ownership rights, this watermark has to be extracted from the image. The schemes are so designed so as to extract the watermark securely.

There are many techniques used for watermarking of digital contents. These are based on the spatial and transform domain methods. In spatial domain method, the watermark is embedded by altering the pixel values of the image. In the transform domain method, the watermark is embedded by taking the transform of the image and then altering the transform coefficients. The proposed scheme makes use of a combination of transforms. Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Discrete Fourier Transform (DFT) are used to perform watermarking on images [3,4].

The main motivation for this approach was using the hybrid approach which meant the usage of multiple transforms. Several image watermarking algorithms, with the application of two or more transforms, had been proposed to meet the requirements of robustness and security. The algorithms used in the literature were based on sequential hybrid watermarking. This type of watermarking made use of a multiple transforms. The schemes that were implemented till now dealt with one transform on the original image and then another transform was applied to some of the coefficients of the previous transform. Yet another transform was applied to the coefficients of the previous transforms in some schemes. The watermark information was now embedded in these modified coefficients. The application of transforms one after the other increased the computation time. If one of watermarking method among the chain of the methods failed then the whole watermarking information was lost. Multiple watermark bits were embedded into the coefficients on the same pixel index increasing amount of noise and thus reduced the clarity and imperceptibility of the watermarked image.

This paper brings a novel approach of dividing the image into regions which are spatially disjointed. Each area is selected sequentially and watermarked using different transforms. Same watermark is simultaneously embedded in a single image in random order at different places. The shortcomings of one transform based watermarking scheme are overcome by the other. Hence, if any method fails against an attack the watermark can be efficiently extracted by the other implemented methods.

An algorithm proposed by Kasmani et al. [5] was based on joint DWT and DCT transform. The three level DWT transform of original image was computed. The watermark used for embedding was a binary image. Each sub-band of

978-1-5090-6644-5/17 $31.00 © 2017 IEEE
DOI 10.1109/CSCloud.2017.30

IEEE computer society

DWT was transformed by DCT and its middle frequency coefficients were segregated. The bits of the watermark were embedded in these coefficients. In the extraction process, the sharpening and Laplacian filters were applied to the watermarked image. The approach used in embedding was used to localize the DCT coefficients. The watermarked bits were extracted by finding out the correlation between middle frequency components and binary watermark sequence.

An algorithm proposed by Lama et al. [6] used the DWT and DCT transforms jointly. The interpolation of high frequency coefficients in DWT were interpolated in the DCT domain using the zero pad method. The inverse DWT is compiuted to generate the upscaled image. Another scheme proposed by Feng et al. [7] used a blind watermarking algorithm with a combination of DWT and DCT. The watermark was permuted using Arnold's transform and was embedded into a spread spectrum pattern. The DCT was applied to LL sub band of image and watermark was embedded. Wang et al. [8] enhanced the already existing hybrid methods of DCT and DWT by applying Singular Value Decomposition (SVD) to the coefficients of DCT before embedding the watermark.

A cryptography approach is proposed [9] to ensure cloud data privacy and security so that the cloud service operators are restrained from the access to the sensitive data. In this approach, the file is divided and the data is stored in the distributed cloud servers. Another approach is implemented to shorten the computation time by finding if data packets needed a split.
Another approach [10] employs the combined DWT and DCT to embed the information of patient outside region of interest (ROI) in medical image. The important regions are found out using saliency and blocks are identified based on minimum overlap with region of interest.

A scheme was proposed [11] based on dual watermarking. It consisted of a gray image watermarking algorithm and a two watermark image. The DCT is used in combination with DWT method for the dual embedding. The scheme reduced the loading effect of original watermark and enhanced the strength of self-recovery system.

The hybrid methods had been introduced in the papers to increase the domain of the resisted attacks. But these methods had their own constraints. The complexity of these methods was very high. An assessment of image quality was done by multiple watermarking approaches [12] showing the robustness of watermark. The hybrid methods were introduced to satisfy the imperceptibility and robustness requirements. Multiple watermarks were simultaneously embedded in a single image in random order. The advantage of this concurrent watermarking method was that it made the watermark invariant to the Signal processing attacks.

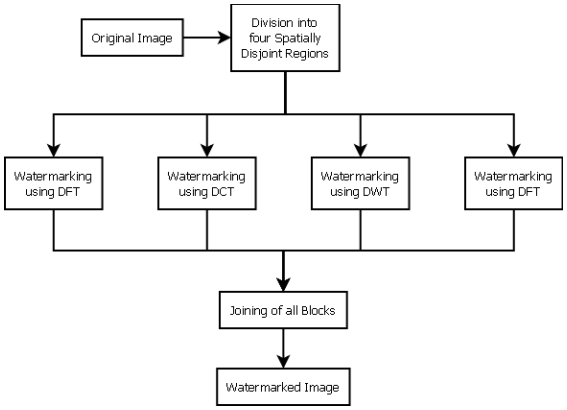

Fig. 1. Spatially Disjoint Region Embedding

A novel image watermarking scheme is introduced with an aim to satisfy the imperceptibility and robustness requirements. The division of the image is done into regions which are spatially disjointed. Watermarking is done by applying DWT, DCT and DFT.

The rest of the paper is organized as follows. Section 2 introduces the Spatially Disjoint scheme. The quality of the watermarking schemes used is assessed and are followed by performance analysis and results in Section 3. Section 4 elaborates upon the comparison with other schemes. The conclusion is brought forward in Section 5.

II. SPATIALLY DISJOINT SCHEME

An image watermarking method is described here for interleaving the same or different watermarks using various watermarking schemes. The interleaving of watermarks is done by dividing the image into several equal sized spaces. The image is divided into four equal areas as depicted in Figure 1. For each area a different watermarking procedure is applied treating that particular area as a reduced sized image. All the four areas are watermarked independently with same watermark or using the same watermark as a seed to generate the watermark. After the watermarking procedures, the four areas are joined at their original spatial location to get the final watermarked image. If the image incurs tampering, then the watermark can be retrieved by dividing the watermarked image into the same number of areas of same size as it was done in the embedding process. The appropriate transforms are applied to each area for retrieval of the original watermark to prove the copyright ownership of the image.

A. Embedding Algorithm

The original image I is a gray scale image with N X N pixels. The image is divided into 4 sub-images. Let W be the grayscale watermark used. The embedding algorithm is discussed as below.

The block diagram in Figure 1 explains the embedding procedure.

Step 1. Divide the image I into four sub images of equal size, I_1, I_2, I_3 and I_4.
Step 2. Consider each sub image as an independent sub-image and divide it into 8 X 8 blocks.
Step 3. Watermark each sub images with DCT, DFT and DWT chosen randomly using the same watermark.
Step 4. I_2'= DCT(I_2) {For the blocks of sub image I_1, perform the 2D DCT Transform and embed the watermark W}
Step 5. I_1'= DFT(I_1) and I_4'= DFT(I_4) {For the blocks of sub image I_1 and I_4, perform the 2D DFT Transform and embed the watermark W)
Step 6. I_3'= DWT(I_3) {For the blocks of sub image I_1, perform the 2D DWT Transform and embed the watermark W}
Step 7. Z_2 = IDCT(I_2'), Z_1 = IDFT(I_1'), Z_4 = IDFT(I_4'), Z_3 = IDCT(I_3') {Apply the inverse DFT, DCT, DWT, DFT on the blocks of parts I_1, I_2, I_3 and I_4 respectively.}
Step 8. Z = Z_1, Z_2, Z_3, Z_4 {Join all the four watermarked sub-images at their original spatial location to obtain the complete watermarked image Z}.

B. Extraction Algorithm

Step 1. Z = Watermarked Image
Step 2. Input image = Z.
Step 3. Divide Z into Z_1, Z_2, Z_3, Z_4
Step 4. Consider each area as an independent sub-image and divide it into blocks.
Step 5. Z' = DCT(Z_2)
Step 6. Z' = DFT(Z_1)
Step 7. Z' = DFT(Z_4)
Step 8. Z' = DWT(Z_3)
(Apply DCT, DFT or DWT on the blocks depending upon the type of transform which had been applied for embedding earlier.)
Step 9. Extract the watermark from the embedded coefficients of the blocks.

III. PERFORMANCE ANALYSIS

The experiments were carried out with the images of Lena and Baboon of size 512 times 512. The cover image was divided into blocks as shown in Figure 2(a) and the watermarks embedded are shown in Figure 2(b). Two blocks were watermarked using DFT, third block was watermarked using DCT and the fourth block was watermarked using DWT.

This scheme was tested on gray scale images of Lena and peppers. As a measure of the quality of a watermarked image, the peak signal to noise ratio (PSNR) was typically used. The PSNR value of the watermarked image having hidden watermarks came out to be 38.95 dB for Peppers image and 40.06 dB for Lena image. These values were quite high and provided good quality of the watermarked image even in the presence of four watermarks.

Fig. 2(a). Blocks of Image

Fig. 2(b). Watermarks Embedded

A. Signal Processing Attacks

The Table I shows the performance of the watermarking algorithm against various Signal processing attacks. Results consist of SM values detected during the experiments of extraction of watermark from Lena and Peppers images. The high SM values prove that at least one of the watermarks is extractable from any of the areas even after application of attacks. Also the attacks where DFT watermark is not invariant, the DCT based watermark can be detected with high SM values. It depicts the usefulness of the proposed watermarking scheme. It is concluded from the results that DCT and DWT performs well for frequency based attacks. The results of JPEG compression for Lena and Peppers images are also shown. The image was compressed to a quality factor of 20, 40 and 70 percent. Even after this compression the SM between the original and the detected watermark is very high due to invariance of DFT watermark against JPEG compression.

B. Geometric Attacks

The Table II shows the performance of the watermarking algorithm against Geometric attacks. The SM values are calculated for the extracted and original watermark from Lena and Peppers images.

TABLE I. SIMILARITY MEASURE VALUES FOR SIGNAL PROCESSING ATTACKS

Attack Categories	Watermarked Image Peppers			Watermarked Image Lena		
	DFT	***DCT***	***DWT***	***DFT***	***DCT***	***DWT***
Average Filter(2X2)	1.00	0.76	0.62	1.00	0.69	0.68
Median filter 5X5	0.99	0.45	0.65	0.99	0.58	0.61
Gaussian filter 5X5	0.97	0.98	0.98	0.94	0.98	0.98
Disk filter 0.8	0.93	0.93	0.96	0.91	0.92	0.93
Gaussian noise 0.6	0.97	0.54	0.73	0.97	0.22	0.73
Salt & Pepper noise	0.98	0.43	0.72	0/97	0.25	0.75
Poisson noise	1.00	0.48	0.94	1.00	0.45	0.95
Blurring 0.6	1.00	0.95	0.80	1.00	0.91	0.81
Sharpening 0.6	1.00	0.93	0.83	1.00	0.90	0.80
Motion 2bits 90	0.95	0/91	0.91	0.95	0.89	0.91
JPEG comp 20%	1.00	0.3	0.40	1.00	0.32	0.47
JPEG comp 40%	1.00	0.50	0.63	1.00	0.4	0.62
JPEG comp 70%	1.00	0.70	0.75	1.00	0.69	0.78

TABLE II. SIMILARITY MEASURE VALUES FOR GEOMETRIC ATTACKS

Attack Categories	Watermarked Image Peppers			Watermarked Image Lena		
	DFT	***DCT***	***DWT***	***DFT***	***DCT***	***DWT***
Rotation 30°	1.0000	0.3176	0.6931	1.0000	0.3198	0.6581
Scaling 1.5	0.9946	0.5183	0.6187	0.9889	0.5134	0.6011
Inverting Pixels Side by Side	1.0000	0.5351	0.6233	1.0000	0.4583	0.4567
Inverting Pixels Diagonally	1.0000	0.5474	0.5921	1.0000	0.5287	0.5493

It is seen that the DCT and DWT based watermarks are not robust against RST (Rotation, Scaling and Translation) attacks.

This problem is counteracted by DFT based watermark. Similarity Measure values for Signal processing attacks. The watermark can be detected completely even after rotating the image through 30° or scaling up to 1.5 times as shown in the Table 2.

C. Blind Detection Attacks

For Blind Watermark Detection attack, it is assumed that the counterfeiter knows about the type of transform, DCT, DWT or DFT performed on each block. The coefficients used for watermarking from each block are stored in block in a two dimensional array called extracted information. The correlation of extracted information with the percentage of watermark known is performed. If the correlation coefficient is greater than the threshold, then the watermark is detected otherwise it is not detected. The three transforms have been used in random manner so that the attacker is misguided as to which transform has been used on the block. From the Table 4, it is observed that the watermark has been detected for block 1 and 4 in which watermark was embedded using DFT. Watermark has not been detected for block 2 and 3 where watermark was embedded using swap based DCT and DWT respectively. Figure 4 demonstrates the results graphically.

In Detection Algorithm, it is assumed that the attacker knows about the type of transform, DCT, DWT or DFT performed on each block. The detection for spatially disjoint region watermarking is depicted in Figure 3.

Here, it is assumed that the attacker knows about the type of transform, DCT, DWT or DFT performed on each block. The detection for spatially disjoint region watermarking is depicted in Figure 4.

Detection Algorithm

Step 1. Take the watermarked image Z as input image.

Step 2. Divide the image Z into four spatial areas of equal size.

Step 3. Consider each area as an independent sub-image and divide it into blocks

Step 4. Apply DCT, DFT or DWT depending upon the type of transform which had been applied for embedding earlier.

Step 5. Select the coefficient in which watermark was embedded for DCT, DFT and DWT from each block.

Step 6. Store the coefficient from each block in a two dimensional array called extracted information.

Step 7. Input the watermark of known percentage.

Step 8. Perform the correlation of extracted information with the percentage of watermark known.

Let the correlation coefficient be r.

Step 9. If $r >$ Threshold T, then the watermark is detected.

Step 10. If $r \leq$ Threshold T, then the watermark is not detected.

The detection algorithm is applied to the scheme by using the thirty three more images in addition to Lena and Peppers to test the scheme against detection attack. Three watermarks of different statistical property were used. These were MNIT logo, Secret and Curve. Here, the percentage P at which the watermark is detected is worked out and correlation coefficient has been calculated. The values are displayed in the Table IV. The plot in Figure 4 illustrates the detection statistics for the images and the percentage of watermark known. The numerals in the graph correspond to images as shown in Table V.

It is observed that the watermark in the image of Fishing Boat has been detected when DCT transform is used in the

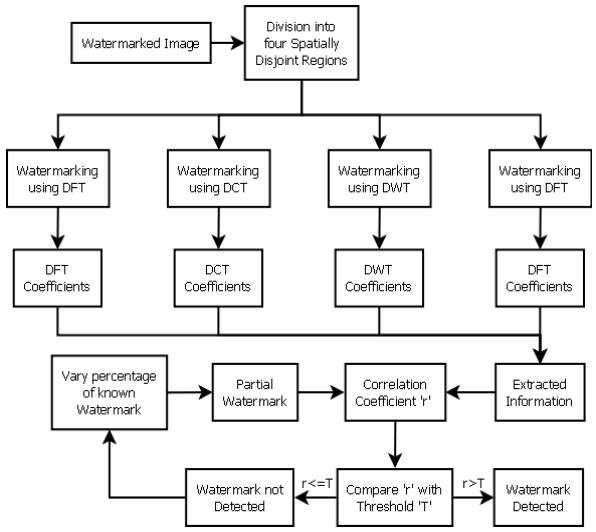

Fig. 3. Spatially Disjoint Region Detection

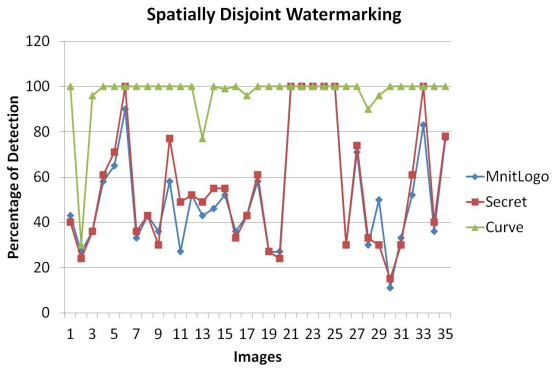

Fig. 4. Detection Statistics

TABLE III. RESULT COMPARISON FOR LENA IMAGE

Attack Category	Similarity Measure for Schemes				
	Proposed	*Kasmani's [5]*	*Feng's [7]*	*Wang's [8]*	*Zhu's [11]*
Gaussian Noise	0.9716	0.9563	0.9558	0.9502	NA
Gaussian Filter	0.9892	0.9853	NA	0.9335	NA
Rotation	1.0000	0.5342	NA	0.8819	0.99
JPEG Comp 40	1.0000	0.9461	0.9839	0.9439	0.95
Scaling	0.9889	1.0000	0.9798	NA	0.96
Median Filtering	0.9934	NA	0.9777	NA	0.79

third block. Whereas, on applying Spatially Disjoint method, the DWT is applied in this block and the watermark is not detected. Hence, DCT should not be used for third block. DWT is more suitable for this block. The watermark is detectable on applying the Blind Watermark Detection attack on blocks of images using DFT. However, the results for the watermark curve show that the detection attack can be resisted by choosing a very low frequency watermark such as curve. But such a simple watermark may not appeal to the authors.

IV. COMPARISON WITH OTHER SCHEMES

The watermarking has been done using hybrid methods to increase the sustenance against attacks. So far, the methods used in hybrid scheme dealt with dual transform watermarking scheme. Here one transform is applied on the cover image and then another one is applied in some of its coefficients [9,10]. Thereafter watermark is embedded in the modified coefficients. In these methods, if any one of the watermarking method fails then the watermarking information is lost. In the proposed scheme, the watermarking is done by using three transforms simultaneously in different blocks making the method robust against different type of attacks.

In this section, the experimental results of the proposed scheme for Lena image were evaluated and compared with the Kasmani's scheme [5], Feng's scheme [7], Wang's scheme [8] and Zhu's scheme [11] as shown in Table III. The comparison of the Similarity Measure values of the proposed scheme with these schemes for Gaussian Noise Attack, Scaling Attack, Rotation Attack, Gaussian Filtering Attack, Scaling and JPEG Compression was performed. For Gaussian noise attack, the SM value was computed to be 0.9716 and for Gaussian Filter attack, this value was 0.9892. The SM values for rotation and JPEG Compression attack was 1.0 showing that watermark was accurately extractable and the values were found to be

TABLE IV. TEST IMAGES

Image No.	Image	Image No.	Image
1	Barbara	19	Apple
2	Baboon	20	Fruits
3	Elaine	21	Bird
4	Lena	22	Star
5	Baby	23	Line Boxes
6	Box	24	Train
7	Glasses	25	Line Car
8	Scanner	26	Waves
9	Tilted Glass	27	Blue Hills
10	Cups	28	Trees
11	Flower	29	Lake
12	Opera House	30	Snow
13	Car	31	Katrina
14	Cow	32	Tintin
15	Fishing Boat	33	Doraemon
16	Peepers	34	Rapunzel
17	Vegetables	35	Ninja Hattori
18	Pumpkin		

better than compared schemes. It was observed that the SM values of the proposed scheme based on Spatially Disjoint techniques were better than Kasmani's scheme except for Scaling attack where the difference was 0.02 and was comparable. It is seen that the proposed method has better robustness and imperceptibility for both images. The comparisons show that the proposed scheme outperforms the compared scheme.

V. CONCLUSIONS

In this paper, Similarity Measure values obtained were approximately equal to one. Thus, the watermark was said to have been successfully extracted, making the scheme using multiple transforms in different regions very robust. Experimental results demonstrate that Similarity Measure (SM) of DFT based watermarking is the highest for all the kinds of attacks due to invariance of DFT watermark against attacks. DWT based watermarking has proved to be better than DCT for Gaussian Noise, Salt and Pepper Noise, Poisson Noise, Rotation and Scaling attacks.

The DCT and DWT based watermarking display high SM values for Gaussian Filter, Disk Filter, Blurring, Sharpening and Motion attacks. DFT based watermarking is invariant to Geometric attacks. The DCT and DWT based methods are resilient to Frequency based attacks but fail against geometric attacks. Hence if any method fails against an attack, the watermark can be efficiently extracted by the other implemented methods. The shortcomings of one transform based watermarking scheme are compensated by the other transforms.

TABLE V. DETECTION ON SPATIALLY DISJOINT REGIONS WATERMARKING (ND = NOT DETECTED)

		Logo					Secret					Curve				
Images		**P**	**Correlation Coefficient**				**P**	**Correlation Coefficient**				**P**	**Correlation Coefficient**			
			DFT	*DCT*	*DWT*	*DFT*		*DFT*	*DCT*	*DWT*	*DFT*		*DFT*	*DCT*	*DWT*	*DFT*
Face	Barbara	43	ND	0.302 5r2	ND	ND	40	ND	0.304 2r2	ND	ND	100	ND	ND	ND	ND
	Baboon	27	0.31	ND	ND	ND	24	0.30	ND	ND	ND	30	0.30	ND	ND	ND
	Elaine	36	ND	ND	ND	0.30	36	ND	ND	ND	0.30	96	ND	ND	ND	0.31
	Lena	58	ND	ND	ND	0.30	61	ND	ND	ND	0.32	100	ND	ND	ND	ND
	Baby	65	0.30	ND	ND	ND	71	ND	ND	ND	0.30	100	ND	ND	ND	ND
Sharp Objects	Box	90	0.30	ND	ND	ND	100	ND	ND	ND	ND	100	ND	ND	ND	ND
	Books	33	ND	ND	ND	0.31	36	ND	ND	ND	0.36	100	ND	ND	ND	ND
	Scanner	43	ND	ND	ND	0.31	43	ND	ND	ND	0.30	100	ND	ND	ND	ND
	Tilted Glass	36	ND	ND	ND	0.31	30	ND	ND	ND	0.30	100	ND	ND	ND	ND
	Fan	58	0.31	ND	ND	ND	77	ND	ND	ND	0.30	100	ND	ND	ND	ND
Natural Objects	Flower	27	0.32	ND	ND	ND	49	ND	ND	ND	0.31	100	ND	ND	ND	ND
	Opera House	52	ND	ND	ND	0.30	52	ND	ND	ND	0.30	100	ND	ND	ND	ND
	Car	43	0.30	ND	ND	ND	49	0.31	ND	ND	ND	77	0.30	ND	ND	ND
	Cow	46	0.34	ND	ND	ND	55	0.30	ND	ND	ND	100	ND	ND	ND	ND
	Fishing Boat	36	ND	ND	ND	ND	30	ND	ND	ND	ND	99	ND	ND	ND	0.32
Fruits and Vege-tables	Peppers	36	0.30	ND	ND	ND	33	0.31	ND	ND	ND	100	ND	ND	ND	ND
	Vegetables	43	0.34	0.322 5r2	ND	0.30	43	ND	0.347 5r2	ND	ND	96	ND	0.306 1r2	ND	ND
	Pumpkin	58	ND	ND	ND	0.33	61	ND	ND	ND	0.33	100	ND	ND	ND	ND
	Apple	27	0.32	ND	ND	0.30	27	0.33	ND	ND	0.31	100	ND	ND	ND	ND
	Fruits	27	ND	ND	ND	0.31	24	ND	ND	ND	0.33	100	ND	ND	ND	ND
Line Objects	Bird	100	ND	ND	ND	ND	100	ND	ND	ND	ND	100	ND	ND	ND	ND
	Star	100	ND	ND	ND	ND	100	ND	ND	ND	ND	100	ND	ND	ND	ND
	Line Boxes	100	ND	ND	ND	ND	100	ND	ND	ND	ND	100	ND	ND	ND	ND
	Jug	100	ND	ND	ND	ND	100	ND	ND	ND	ND	100	ND	ND	ND	ND
	Train	100	ND	ND	ND	ND	100	ND	ND	ND	ND	100	ND	ND	ND	ND
Natural Scenes	Waves	30	ND	ND	ND	0.34	30	ND	ND	ND	0.34	100	ND	ND	ND	ND
	Blue Hills	71	0.31	ND	ND	0.32	74	ND	ND	ND	0.31	100	ND	ND	ND	ND
	Trees	30	0.30	ND	ND	ND	33	0.32	ND	ND	ND	90	0.30	ND	ND	ND
	Lake	30	ND	ND	ND	0.32	30	ND	ND	ND	0.32	96	ND	ND	ND	0.31
	Snow	11	ND	ND	ND	0.30	15	ND	ND	ND	0.30	100	ND	ND	ND	ND

However there are some limitations. It is inferred that the blocks watermarked using DCT and DWT transforms are resilient against the Blind Watermark Detection attack. But, the watermark is detectable on applying the Blind Watermark Detection attack on blocks of images using DFT transform. Thus, watermarking using DFT is robust for Signal Processing and Geometric Attacks but fails for Detection attack. The scheme can be significantly improved by taking into account the statistical properties of the image. The transformations can be applied depending upon the high and low frequency regions of the image. The size of the areas can be further reduced which may increase the processing time but at the same time make the algorithm more robust. This initiates the future avenues of research to devise a scheme to make the watermark resistant to Signal processing as well as Detection attacks.

REFERENCES

[1] J. Liu, X. He, "A Review Study on Digital Watermarking*"* First International Conference on Information and Communication Technologies, ICICT 2005, pp. 337-341, Aug. 2005.

[2] T. Liu, Z. Qiu, "The survey of digital watermarking-based image authentication techniques", 6th International Conference on Signal Processing, vol. 2, pp. 1556- 1559, Aug. 2002.

[3] R.C. Gonzales, R.E. Woods, "Digital Image Processing", 3rd Edition, Pearson Education, 2009.

[4] I J Cox, M L Miller, J A Bloom, Digital Watermarking, 2nd Edition, Morgan Kaufmann Publishers.

[5] Kasmani S A, Nilchi A N. July 2008, "A New Robust Watermarking Technique based on Joint DWT-DCT Transformation", International Conference on Convergence and Hybrid Information Technology, pp. 539-544, July 2008.

[6] R. K. Lama, S. Shin, M. Kang, G. Kwon, "Interpolation Using Wavelet Transform and Discrete Cosine Transform for High Resolution Display", IEEE International Conference on Consumer Electronics (ICCE), pp. 184-186, Jan 2016.

[7] L.P. Feng, L.B. Zheng, P. Cao, "A DWT-DCT Based Blind Watermarking Algorithm for Copyright Protection", 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), vol. 7, pp. 455-458, July 2010.

[8] B. Wang, J. Ding, Q. Wen, X. Liao, C. Liu, "An Image Watermarking Algorithm based on DWT, DCT and SVD", Proceedings of IC-NIDC, pp. 1034-1038, 2009.

[9] Y. Li, K. Gai, L. Qiu, M. Qiu, H. Zhao, "Intelligent cryptography approach for secure distributed big data storage in cloud computing", Information Science, Elsevier, Volume 387, Pages 103–115, May 2017.

[10] M. Jamali, S. Samavi, N. Karimi, S.M.R. Soroushmehr, K. Ward, K. Najarian "Robust Watermarking in Non-ROI of Medical Images", 2016 38th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), pp. 1200 - 1203, Aug. 2016.

[11] Y. Zhu, L. Lin, "Digital Image Watermarking Algorithms Based on Dual Transform Domain and Self-Recovery", International Journal on Smart Sensing and Intelligent Systems, vol. 8, no. 1, March 2015.

[12] Gunjan R, Maheshwari S, Laxmi V, Gaur M S. July 2011, "Robust Watermarking Through Spatially Disjoint Transformations", Proc. International Conference on Advances in Computing and Communications (ACC-2011), Springer Verlag, CCIS-192, pp. 478-487, 2011.