Advanced Image Watermarking for Image Authentication and Hiding Secret Data using LWT and SVD Technique

Gurneet Kaur Bhatia, Dr. Akash Awasthi

Abstract— **The protection and illegal redistribution of digital media has become an important issue in the digital era. This is due to the popularity and accessibility of the Internet now a day by people. This results in recording, editing and replication of multimedia contents. Digital watermarking can be used to preserve digital info in opposition to unauthorized modification and circulation. Digital watermarking technique is the process of embedding noise-tolerant signal such as audio or image data in the carrier signal. This technique provides a robust solution to the problem of intellectual property rights for online contents. This paper reviews different aspects and techniques of digital watermarking for protecting digital contents. To minimize the difference between original and watermarked singular values, an optimized-quality formula is proposed. First, the peak signal-to-noise ratio (PSNR) is defined as a performance index in a matrix form. Then, an optimized-quality functional that relates the performance index to the quantization technique is obtained.**

The proposed method achieves high values of peak signal to noise ratio (PSNR) of watermarked image and high values of normalized correlation (NCC) of the extracted watermark.

Index Terms— **Image Watermarking; 3D L_DWT (Three Dimension Lifting Discrete Wavelet Transformation); SVD (Singular Value Decomposition) Image Extraction; PSNR; MSE; NCC**

I. INTRODUCTION

With the pervasive distribution of digital data over the World Wide Web, the safety of intellectual religion rights has come to be progressively important.

This information, as encompass images, audio, image, yet textual content are stored yet transmitted within a digital format [1, 3].

Information is saved within digital format can keep without difficulty copied besides someone impairment regarding exorcism and correctly distributed. Digital watermark is after delivered in accordance with remedy that problem. Digital watermarking is a branch of statistics screen as is old in conformity with hide proprietary statistics of digital media as photographs, digital music, or digital picture [6, 9].

The easement together with who digital content be able keep exchanged over the Internet has built copyright break issues. Copyrighted fabric perform remain effortlessly exchanged above peer-to-peer networks, then this has triggered major concerns in imitation of those content companies whosoever origin these digital content material [3, 7].

For making a digital watermarking Technique according to lie environment friendly such have to stand unrecognized, yet Herculean according to standard photograph amendment like compression, filtering, rotation, scaling cropping, or collusion attacks amongst dense mean digital sign technology operations [2,11].

Digital Image watermarking methods do be classified of twain authoritative two classes:

Spatial Domain Watermarking and Frequency Domain Watermarking. Compared in imitation of spatial area methods, frequency-domain watermarking strategies standardized rod high-quality with observance after accomplishing the unobserved and robustness requirements regarding digital image watermarking algorithms. Generally used frequency-domain transforms include the Discrete Wavelet Transform (DWT), the Discrete Cosine Transform (DCT) [4,12] then Discrete Fourier Transform (DFT) [8].

There are twain primary essential residences over Digital Watermarking, i.e. Robustness then Imperceptibility of watermarked photo this houses must smoke of consideration. In this paper, perdue powerful digital watermarking is proposed the use of L-DWT (Discrete Wavelet Transform) within YCbCr Color space [5]. The overall performance concerning the proposed algorithm is compared along some previous works yet outcomes located are extra powerful towards a number attacks (Blur, Average, Gaussian, Crop).

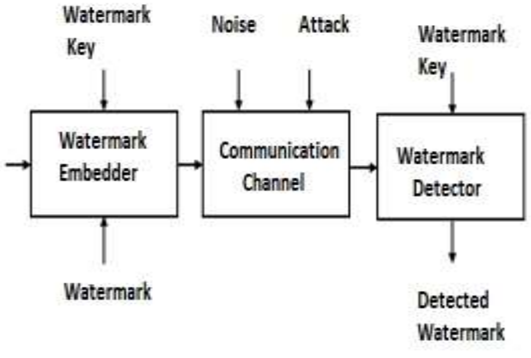


Figure1: Watermarking System

II. 3L_ LIFTING WAVELET TRANSFORM (LWT)

Lifted Wavelet Transformation (LWT) of image produces the multi-resolution representation of image. A multi-resolution representation provides a simple hierarchical framework for interpreting the image information. At different resolutions, the details of an image generally characterize different physical structures of the image. At a low level resolution,

Gurneet Kaur Bhatia, M.Tech Scholar, Department of Computer Science & Engineering, Naraina Vidya Peeth Engineering And Management Institute, Kanpur (U.P.), India.

Akash Awasthi, Associate Professor, Department of Computer Science & Engineering, Naraina Vidya Peeth Engineering And Management Institute, Kanpur (U.P.), India.

these details correspond to the larger structures which provide the image content. Wavelet transformation consist of two main steps namely LWT and ILWT (Inverse LWT). LWT segments a digital signal into high frequency quadrant and low frequency quadrants. The low frequency quadrant is split again into two more parts of high and low frequencies and this process is repeated till the signal has been entirely decomposed. In watermarking, generally 1-5 level of decompositions is used. The reconstruct of the original signal from the decomposed image is performed by ILWT. Several types of wavelets exist for decomposition. Generally, application of LWT divides an image into four sub bands (Figure 1a), which arise from separable applications of vertical and horizontal coefficients. The LH, HL and HH sub bands represents detailed features of the images, while LL sub band represents the approximation of the image. To obtain the next coarse level, the LL sub-band is further be decomposed (Figure 1b), thus resulting in the 2-level wavelet decomposition. The level of decomposition performed is application dependent. The present work considers decomposition up to two levels[10].

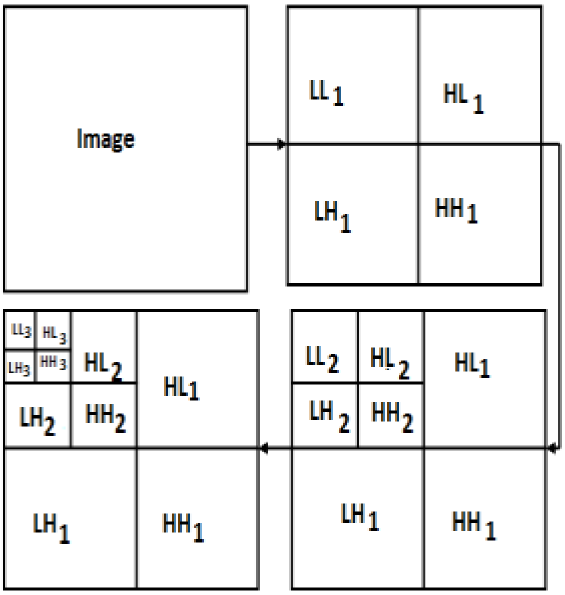


Figure 2: Wavelet Decompositions

III. PROPOSED METHOD

In the proposed method, we appeal the idea over Singular Value Decomposition in conformity with attach a watermark between the cover photo and according to remove this watermark beside the watermarked image. The watermark is advance cut up between couple shares. However, only the forward section acts as like a watermark while the 2nd piece acts as much the black key. Thus, the ignoble portion is the authorization to reconstruct the watermark. The visually crypted watermarks may be transmitted concerning the net then the lawful resolution piece is maintain through the copyright proprietor of watermarked image so the stolen key. In that sense, such is dead easy then quickly in imitation of function the photograph authenticate by way of just superimposing the solution quantity above the decrypted watermark picture

Flowchart of Proposed Architecture

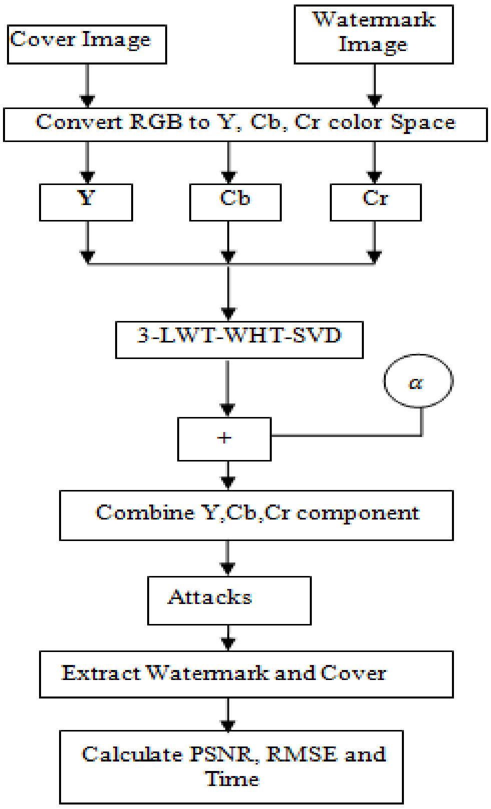

Cover Image
Watermark Image
Convert RGB to Y, Cb, Cr color Space
Y
Cb
Cr
3-LWT-WHT-SVD
α
+
Combine Y,Cb,Cr component
Attacks
Extract Watermark and Cover
Calculate PSNR, RMSE and Time

Figure 3: Block Diagram of Proposed Architecture

Flowchart of Embedding Architecture

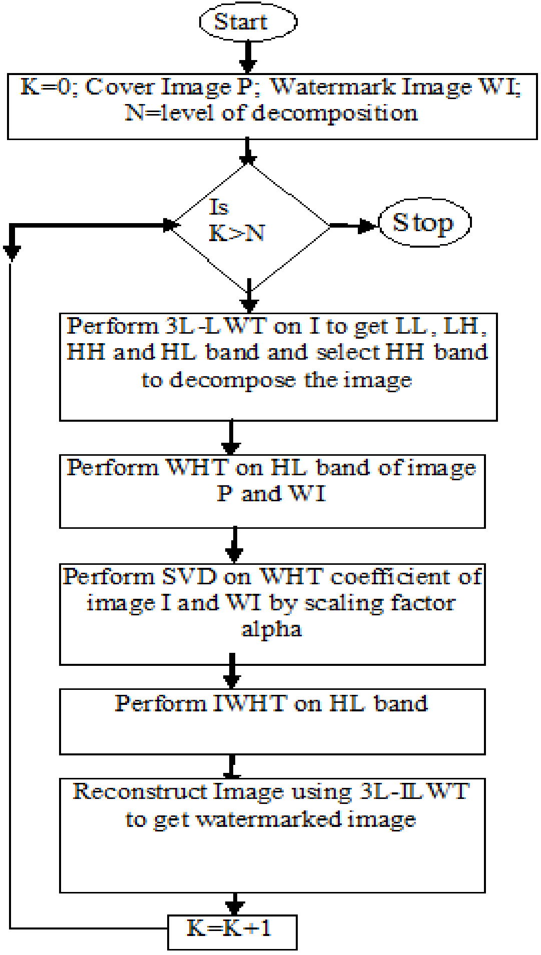

Start
K=0; Cover Image P; Watermark Image WI; N=level of decomposition
Is K>N
Stop
Perform 3L-LWT on I to get LL, LH, HH and HL band and select HH band to decompose the image
Perform WHT on HL band of image P and WI
Perform SVD on WHT coefficient of image I and WI by scaling factor alpha
Perform IWHT on HL band
Reconstruct Image using 3L-ILWT to get watermarked image
K=K+1

Figure 4: Block Diagram of Embedding Architecture

Flowchart of Extraction Architecture

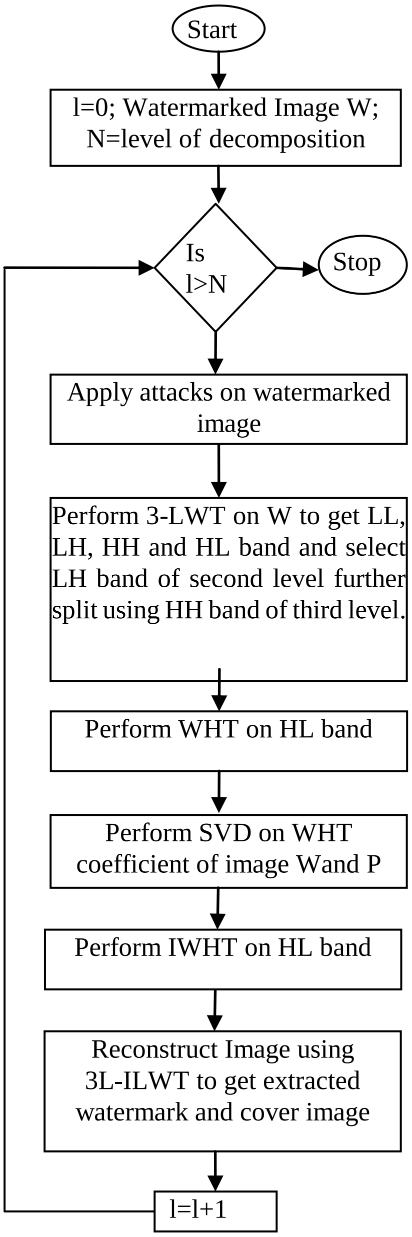

Start
l=0; Watermarked Image W; N=level of decomposition
Is l>N
Stop
Apply attacks on watermarked image
Perform 3-LWT on W to get LL, LH, HH and HL band and select LH band of second level further split using HH band of third level.
Perform WHT on HL band
Perform SVD on WHT coefficient of image Wand P
Perform IWHT on HL band
Reconstruct Image using 3L-ILWT to get extracted watermark and cover image
l=l+1

Figure 5: Block Diagram of Extraction Architecture

METHOD IMPLEMENTATION

Implementation of the method is as follows-

Embedding Algorithm

Input: Cover Image and Watermark Image
Output: Watermarked Image

The patient information or the watermark image is embedded into the medical image as follows-

Step 1: Read cover image 'P' and watermark image 'WI' with NXN size

Step 2: The cover image and watermark image is converted into YCbCr color space from RGB color space and one of the channels is chosen for embedding.

Step 3: Perform 1-LWT on the Y channel of P and WI to split into four groups.

Step 4: Perform 2-LWT on the HH band of P and WI to split into four groups

Step 5: Perform 3-LWT on the HH band of P and WI to split into four groups.

Step 6: Apply WHT on HL band of cover and watermark image.

for x,m = 0,1,2,........,M-1, and y,n = 0,1,2,... ...... N-1.For MxM square images the above transform pair is reduced to

$$H(m,n) = \frac{1}{M}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} HL(x,y)\,(-1)^{\sum_{i=0}^{n-1}[b_i(x)b_i(m)+b_i(y)b_i(n)]} \quad (5)$$

$b_z(k)$is thekth bit in the binary representation of z, $HL(x,y)$ is the HL band of cover and watermark image in rows and columns.For (m,n) = 0,1,2,. . . . . .N-1,n is order of sequence.

Step 7: Perform SVD on the WHT coefficient of the P and WI image.

$$[U_j, S_j, V_j] = svd(X(k)) \qquad (2)$$

Step 8: Modify the singular value of S_i by embedding the singular value of watermark image such that

$$S_e = S_i + alpha * S_j \qquad (3)$$

Where WI is modified matrix of $S_i$and alpha denotes the scaling factor, is used to have power over the signal $S_j$power of watermark.

Step 9: Embed singular matrices with orthogonal matrices for final watermark image as W with below formula:

$$W = U_i * S_e * V_i{}' \qquad (4)$$

Step 10: Apply 2D-IWHT to reconstruct the matrix.

$$HL(x,y) = \frac{1}{M}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} H(m,n)\,(-1)^{\sum_{i=0}^{n-1}[b_i(x)b_i(m)+b_i(y)b_i(n)]} \qquad (5)$$

Step 11: Perform the two level inverses LWT (ILWT) on the LWT transformed image, to obtain the watermarked image on four coefficients.

Input: Watermarked Image
Output: Attacked Image

Step 12: Apply Motion Blur (MB) and Average attack (AA) on watermarked image for security and robustness.

Extraction Algorithm

Input: Watermarked Image
Output: Extracted Watermark Image

The watermarked image as follows-

Step 1: Apply two levels LWT transform to decompose the watermarked image W into four overlapping sub-bands.

Step 2: Apply WHT to HL sub band using equation (1).

Step 3: Apply SVD to $X_m$sub band i.e.,

$$[U_m, S_m, V_m] = svd(X_m) \qquad (6)$$

Step 4: Modify the singular value of S_i by extracting the singular value of watermarked image such that

$$S_j = (S_m - S_i)/alpha \qquad (7)$$

Step 5: Extract singular matrices with orthogonal matrices for final extracted watermark image and cover image as W with below formula:

$$W = U_m * S_j * V_m{}' \qquad (8)$$

Step 6: Apply 2D-IWHT to reconstruct the matrix in equation (5).

Step 7: Perform the three level inverse LWT (3-ILWT) on the LWT transformed image, to obtain the extracted watermark and cover image on four coefficients.

Step 8: Calculate PSNR and RMSE value of watermarked and cover image.

$$RMSE\,(x) = \sqrt{\frac{1}{N}||x - x^{\wedge}||^2 = \frac{1}{N}\sum_{i=1}^{N}(x - x^{\wedge})^2} \qquad (9)$$

Where x is cover image, x^ is watermarked image, N is the size of the cover image

$$PSNR\,(x) = \frac{10\ X\log((255))}{RMSE(x)} \qquad (10)$$

Where m is the maximum value of the cover image

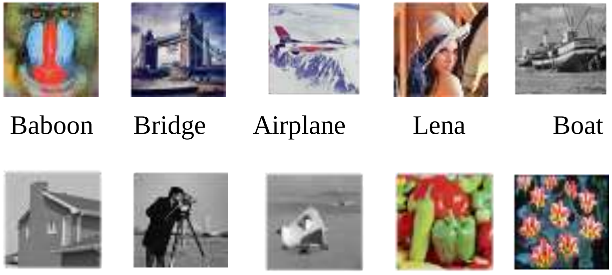
IV. RESULTS

The proposed algorithm has been simulated by using MATLAB software. For proposed watermarking process, different medical images of different sizes have been taken as the cover images and different binary images have been taken as watermark images or different patient information. We have used the following attacks, while watermarking the images

1) Blur Attack
2) Average Attack

Original image or input images have a RGB combination. Image processing begins with an image acquisition process. The two elements are required to acquire digital images.

The following figure 3 has been taken to test the system.



Baboon Bridge Airplane Lena Boat

House Cameraman Lifting Body Peppers Tulips

Figure 5 Experimental Dataset

Here in Figure 6, we have taken cover image as baboon image and watermark image as Tulips image with Blur attack using ref techniques.

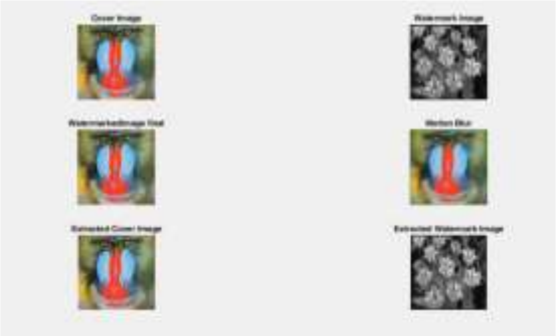


Figure 6: Ref Watermarking Procedure with Blur attack

Here in Figure 7, we have taken cover image as baboon image and watermark image as Tulips image with Average attack using ref techniques.

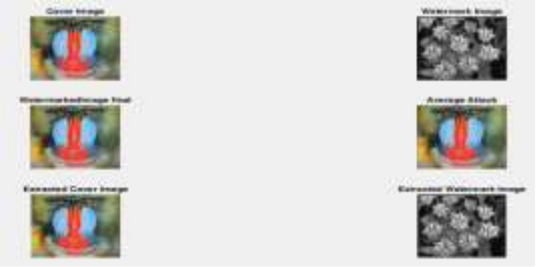


Figure 7: Ref Watermarking Procedure with Average attack

Here in Figure 8, we have taken cover image as airplane image and watermark image as peppers image with Blur attack using ref techniques.

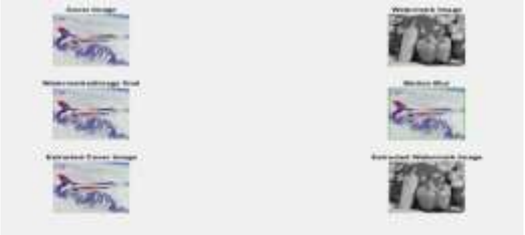


Figure 8: Ref Watermarking Procedure with Blur attack

Here in Figure 9, we have taken cover image as airplane image and watermark image as peppers image with Average attack using ref techniques.

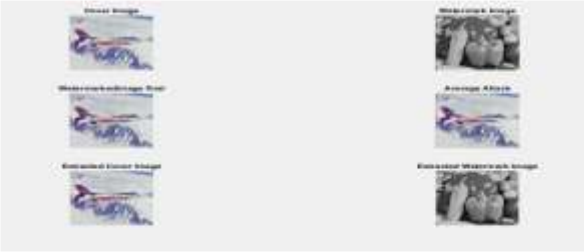


Figure 9: Ref Watermarking Procedure with Average attack

Here in Figure 10, we have taken cover image as bridge image and watermark image as liftingbody image with Blur attack using ref techniques.

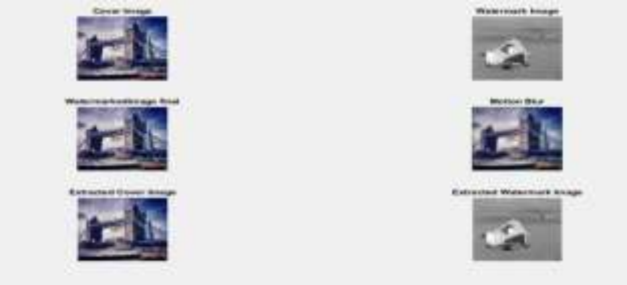


Figure 10: Ref Watermarking Procedure with Blur attack

Here in Figure 11, we have taken cover image as bridge image and watermark image as liftingbody image with Average attack using ref techniques.

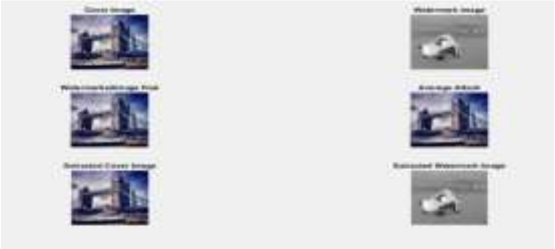


Figure 11: Ref Watermarking Procedure with Average attack

Here in Figure 12, we have taken cover image as lena image and watermark image as boat image with Blur attack using ref techniques.

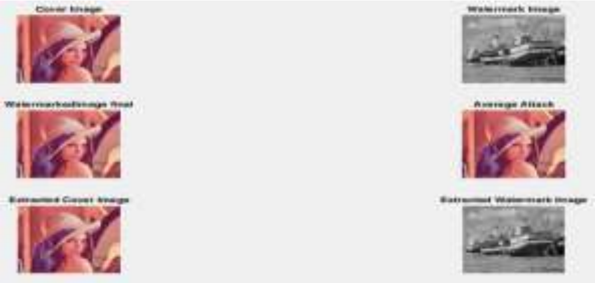


Figure 12: Ref Watermarking Procedure with Blur attack

Here in Figure 13, we have taken cover image as as lena image and watermark image as boat image with Average attack using ref techniques.

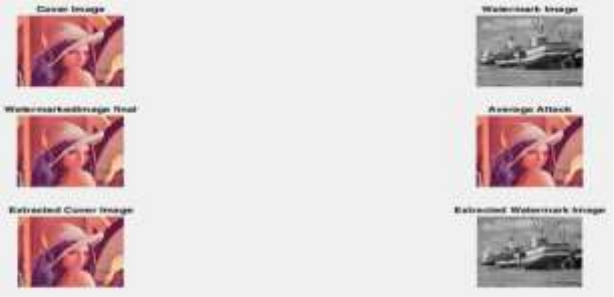


Figure 13: Ref Watermarking Procedure with Average attack

Here in Figure 14, we have taken cover image as baboon image and watermark image as Tulips image with Blur attack using proposed techniques.

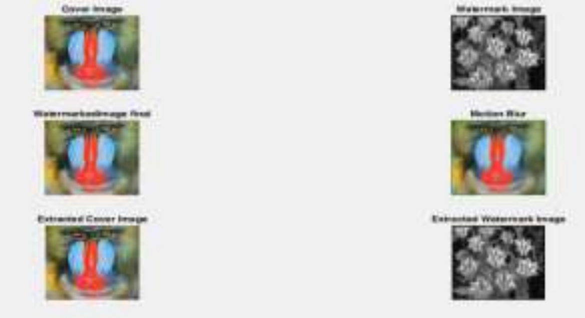


Figure 14: Proposed Watermarking Procedure with Blur attack

Here in Figure 15, we have taken cover image as baboon image and watermark image as Tulips image with Average attack using proposed techniques.

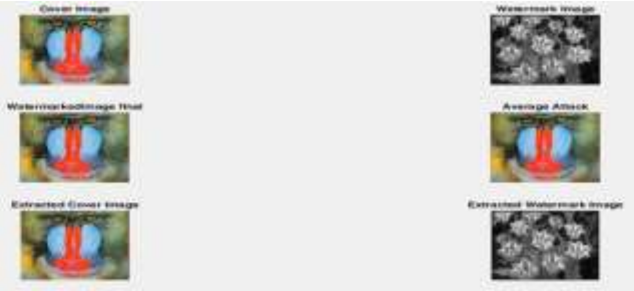


Figure 15: Proposed Watermarking Procedure with Average attack

Here in Figure 16, we have taken cover image as airplane image and watermark image as peppers image with Blur attack using proposed techniques.

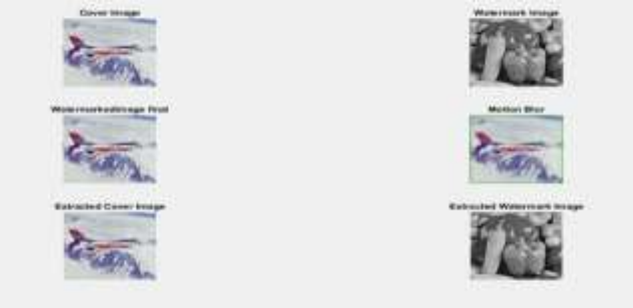


Figure 16: Proposed Watermarking Procedure with Blur attack

Here in Figure 17, we have taken cover image as airplane image and watermark image as peppers image with Average attack using Proposed techniques.

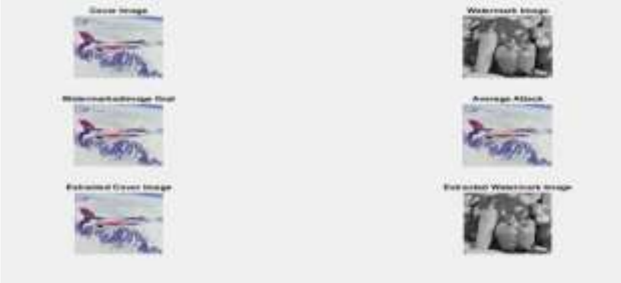


Figure 17: Proposed Watermarking Procedure with Average attack

Here in Figure 18, we have taken cover image as bridge image and watermark image as liftingbody image with Blur attack using proposed techniques.

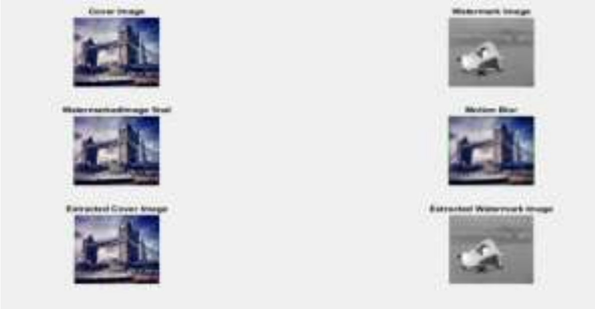


Figure 18: Proposed Watermarking Procedure with Blur attack

Here in Figure 19, we have taken cover image as bridge image and watermark image as liftingbody image with Average attack using Proposed techniques.

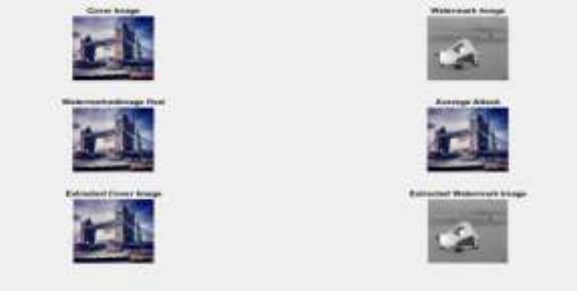


Figure 19: Proposed Watermarking Procedure with Average attack

Here in Figure 20, we have taken cover image as lena image and watermark image as boat image with Blur attack using Proposed techniques.

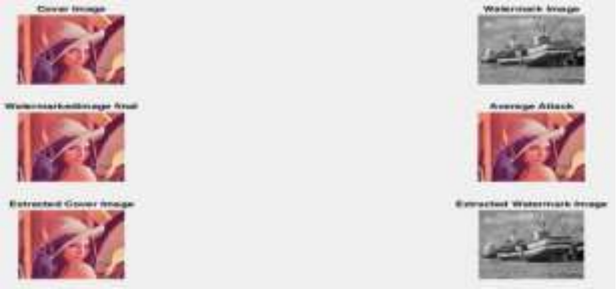


Figure 20: Proposed Watermarking Procedure with Blur attack

Here in Figure 21, we have taken cover image as Lena image and watermark image as boat image with Average attack using proposed techniques.

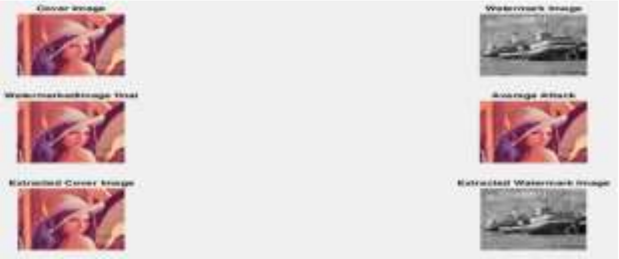


Figure 21: Proposed Watermarking Procedure with Average attack

Similarly, we can test with different images; the following table illustrates the performance.

Table 1: PERFORMANCE OF BLUR ATTACKS

Tick Label	Cover Image	Watermark Image	Blur Attack	
			Reference PSNR	**Proposed PSNR**
A	Baboon	Tulips	52.1241	55.2482
B	Airplane	Pepper	52.1186	59.8033
C	Bridge	Lifting Body	52.2080	58.5613
D	Lena	Boat	52.0408	59.0492
E	Cameraman	House	52.2412	59.1452
F	Pepper	Bridge	52.0572	59.0865

Table 2: PERFORMANCE OF AVERAGE ATTACKS

Tick Label	Cover Image	Watermark Image	Average Attack	
			Reference PSNR	**Proposed PSNR**
A	Baboon	Tulips	52.1241	55.2482
B	Airplane	Pepper	52.1186	59.8033
C	Bridge	Lifting Body	52.2080	58.5613
D	Lena	Boat	52.0408	59.0492
E	Cameraman	House	52.2412	59.1452
F	Pepper	Bridge	52.0572	59.0865

TABLE 3: TIME COMPARISON BETWEEN REF AND PROPOSED FOR EMBEDDING

Tick Label	Cover Image	Watermark Image	Reference Embedding Time	Proposed Embedding Time
A	Baboon	Tulips	0.5300	0.4529
B	Airplane	Pepper	0.5129	0.4761
C	Bridge	Lifting Body	0.5264	0.4510
D	Lena	Boat	0.5655	0.4553
E	Cameraman	House	0.5355	0.4632
F	Pepper	Bridge	0.5106	0.4231

Here in Figure 5.18, we have compared the PSNR for ref and proposed techniques.

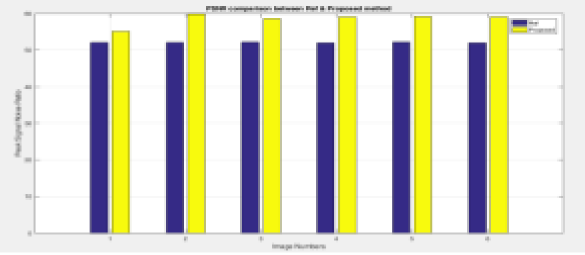


Figure 22 PSNR comparisons between Ref and Proposed method

Here in Figure 22 we have compared the embed time for ref and proposed techniques.

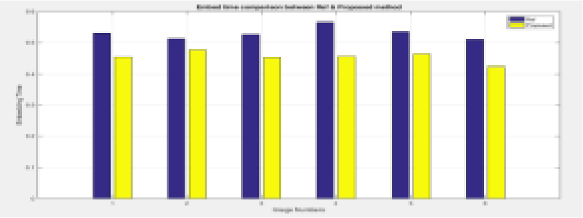


Figure 23 Time comparison between Ref and Proposed for embed

V. PERFORMANCE PARAMETER

The motive about calculating the performance regarding the photograph then afterwards that assessment among ref then proposed strategies wish exhibit who technique is better because Image watermarking. Such method is in the main appropriate according to extraordinarily right detection with various attacks. The (Peak sign to noise ratio) PSNR, (Signal in imitation of noise ratio) SNR is high; (mean squared error) MSE is low. This proposed method is a speedy approach because Image watermarking.

The attached table demonstrates the perfect execution regarding the photo as like indicated by means of the table periodic race is the beneficial race for outcry removable procedure.

The speech Peak Signal to Noise Ratio, fast abbreviated PSNR, is an engineering term for the ratio into the most possible monitoring on a sign then the rule of corrupting clamor that influences the trust about its representation. Because many alerts bear at all huge dynamic range, PSNR is commonly expressed of phrases of the logarithmic decibel scale.

$$PSNR\ in\ dB = 10log_{10}\left(\frac{255^2}{MSE}\right) \tag{5}$$

$$MSE = \frac{\Sigma_i \Sigma_j (\gamma(i,j) - \gamma(i,j)^2)}{M \times N} \tag{6}$$

VI. CONCLUSION

The pc simulation has proven the comparisons concerning PSNR or MSE outcomes regarding special pixel because ref as like nicely as much proposed methods. The pilot results (PSNR and MSE) have in contrast including yield because different images. Clearly, the proposed method offers a higher

PSNR yet less MSE effects than the median filter method do because of the illustrated images.

REFERENCES

[1] Al-amri, He, H. J., Zhang, J. S. and Tai, H. M., (2006), "A Wavelet-Based Fragile Watermarking Scheme for Secure Image Authentication", Springer-Verlag Berlin Heidelberg 2006.

[2] Bhatnagar, G. and Raman, B. (2008), "A new robust reference watermarking scheme based on DWT-SVD" , Elsevier B.V. All rights reserved.

[3] Boland F.M., Ruanaidh J.J.K., Dautzenberg C., "Watermarking digital images for copyright protection", Proc. IEE Int. Conf. on Image Processing and Its Applications, Edinburgh, U.K., pp. 326-330, July 1995.

[4] Bors, A. and Pitas, I. (1996),"Image watermarking using DCT domian constraints", In Proceedings of IEEE International Conference on Image Processing" , Vol. 2. IEEE Computer Society Press, Los Alamitos, CA, 231–234.

[5] Bossen F., Kutter M., Jordan F., "Digital signature of color images using amplihlde modulation", Proc. of SPlE storage and retrieval for image and video databases, Sanlose, USA, vol. 3022-5, pp. 518-526, Feb. 1997.

[6] Bounkong S., Toch B., Saad D., Lowe D., "ICA for watermarking digital images",The Journal of Machine Learning Research, vol. 4, Publisher: MIT Press, Dec. 2003.

[7] Caronni, "Assuring ownership rights for digital images", Proc. Reliable IT Systems,VIS '95, Germany, pp. 251-263, 1995.

[8] Chang-Tsun Li "Oblivious fragile watermarking scheme for image authentication", Acoustics, Speech, and Signal Processing, 1993. In ICASSP-93, IEEE International Conference on 27-30 April on pages IV – VI, 1993.

[9] Chen T.P.C., Chen T., "Progressive image watermarking", Proc. IEEE Int. Conf.on Multimedia and Expo, pp. 1025–1028, July 2000.

[10] Macq. B.M. & Quisquater. J.J. (1994), "digital Image multiresolution encryption", The journal of the intractive Multimedia Association Intellectual property project. L (1) 179-206

[11] Petitcolas, F. A. P., Anderson, R. J. and Kuhn, M. G., (1999), "Information Hiding—A Survey", Proceedings of the IEEE, VOL. 87, NO. 7, JULY 1999

[12] Ravi K Sheth,Dr. V V Nath,"Secured Digital Image Watermarking with Discrete Cosine Transform and Discrete Wavelet Transform method",IEEE International Conference on Advances in Computing,Communication,& Automation (ICACCA) (Spring),2016.

Gurneet Kaur Bhatia, M.Tech Scholar, Department of Computer Science & Engineering, Naraina Vidya Peeth Engineering And Management Institute, Kanpur (U.P.), India.
Akash Awasthi, Associate Professor, Department of Computer Science & Engineering, Naraina Vidya Peeth Engineering And Management Institute, Kanpur (U.P.), India.
.