A Novel Method For Video Watermarking Using 2LWT in YCbCr Color Space

[1]Munish Kumar, [2]Dr. Sandeep Kumar, [3]Dr. Yashpal Singh, [4]Subodh Gupta
[1]Dept. of ECE, DCRUST, Murthal University, Haryana, India
[2]Dept. of ECE, Sreyas Institute of Engineering & Technology, Hyderabad, India
[3]Dept. of ECE, OPJS, University Rajasthan, India
[4]Dept. of R & D, Dreamtree Infotech Pvt. Ltd, Gwalior, India

Abstract
Video Watermarking is a prominent technique used to provide the authentication to the multimedia data such as audio, video and text. It is also used to resolve the copyright protection and ownership problem. This paper presents secure transmission for video watermarking using two-level lifting wavelet transform (LWT). For copyright protection and image quality, we used 2-LWT for video watermarking. In our method, LWT is applied to decompose the video frames and produce the low and high-frequency coefficients to take benefits of "power compaction" goods. The experimental outcomes give good results up to 85.49% as compared to previous results. Several results show that the presented method is able to withstand various attacks. In this study, we determined the performance of this algorithm on the basis of Peak Signal Noise Ratio (PSNR) and Normalized Correlation (NC) value of various watermarked images.

Keywords
LWT, YCbCr, PSNR, NC, Video Watermarking.

I. Introduction

Now a day, internet is on fingertip of every mobile/ Desktop/ Laptop user, due to huge demand of internet, digital transfer of data such as images, video etc. improve tremendously [1,2]. Hence, it is important to avoid the unwanted redistribution data or unauthorized access by the illegal users. Digital watermarking is an effective way to solve this issue. Digital watermarking provides copyright protection of data and another application such as fingerprinting, broadcast monitoring and authentication applications [3]. Digital watermarking is the process of concealing secret information in a digital medium. The information should be embedded in a way that allows it to be extracted or detected [4]. There are different watermarking techniques which can be used. The main classification of watermarking is spatial domain and frequency domain. Again spatial and frequency domain techniques have a different classification. Spatial domain watermarking has least significant bit (LSB) [5] method where LSB value of cover image or frames of a video is replaced with watermark value and visible watermarking can be done using LSB method. Frequency domain watermarking makes use of techniques like Discrete Cosine Transform (DCT) [6], Discrete Wavelet Transform (DWT) [7].

II. Related Work

Ponni et al. [4] proposed a new secure and robust video watermarking based on the chaotic map with DWT and SVD. The use of proposed method achieves the imperceptibility and robustness of video watermark and extracted watermark. The confidentiality of embedding location is assured by chaotic key technique. The SVD method is used to provide stability and achieve robustness, DWT for localization. The time complexity of embedding and extraction is reduced by watermark embedded in the keyframe. The result of proposed method gives the perceptual quality of the video as well as watermark also proves well in security and capacity.

Jianfei Li et al. [8] discuss a new design idea of embedding watermark which is to embed the watermarking information into the last DC coefficient of the last macroblock in every slice in the luminance component. The result of the method shows that it reduced the complexity of the video watermarking system, the video's quality and bit rate of the video stream remains stable, and it can extract watermarking information without distortion. The watermark is embedded in the DC coefficients, because just a bit of watermarking information is embedded in a slice of a frame, so it can solve the blocking effect which may be caused by embedding watermark in the DC coefficients.

Sudhanshu et al. [9] combination of two transformed i.e. DWT-DCT for watermarking purposed. This combination of two frequency domain watermarking provides authenticity and copyright protection to the image. The objective of this research is to maintain the robustness of watermark and secure transmission of cheque image from home branch bank to a clearinghouse of branch using cheque truncation system. In this experiment, advanced encryption standard is used for providing security service to watermarked image using a 256-bit key. It is observed that PSNR value for watermarked image remains same against various attacks except for cropping attack. The discrete wavelet transform is a kernel technique for Jpeg 2000 and discrete cosine transform is used for compression. Due to this property, it prevents the Jpeg compression attacks. It helps to maintain the imperceptibility of the original image and the watermark robustness. By using this combination of two different techniques the watermark robustness is achieved 99% against all attacks except cropping attack. However, the robustness of watermark is 87% against rotation attack.

Sneha et al. [10] proposed an effective algorithm for providing copyright protection using a new embedding strategy for Discrete Wavelet Transform (DWT) based video watermarking. The key generation is done using low-frequency component, use of watermark image and LL part of the video frame. The blind watermarking technique is also used that require the only key to extract the embedded watermark. The algorithm found blind watermarking with watermark detection and extraction is to be robust to most common attacks. The Normalized Correlation Coefficient (NC) and Structural Similarity (SSIM) index are approaching towards the value 1 which indicates that reconstructed watermark is matching to that of the original one.

Kaur et al. [11] performed invisible video watermarking for security purposes. We embed a watermark on RBG components of individual images, then embedding procedure further depends upon the quality of watermark. Whether it is blind or non-blind, we performed invisibly watermarking using DCT and LSB techniques, and LSB technique proves better results than DCT, the proposed DWT technique, and mojette transform will also be used for comparison.

A. Mahmoud et al. [12] proposed a watermarking technique for scanned colored PDF Files. In this technique, a watermark inserted into scanned colored PDF files. The main aim was to protect PDF documents authentication and copyright ownership. As a robust watermark for copyright, a logo was used and was embedded in the green channel of the file. The extraction of watermark was successfully done. The System survived against different attacks. Any manipulations in the PDF file caused the second fragile watermark to change and indicate forgery. The algorithm was successfully tested on different colored PDF files.

Rini T Paul et al. [13] proposed that robust watermarking are watermark embedding, attack, and watermark detection. In watermark embedding, a watermark signal (image) is constructed and then embedded into a Video to produce the watermarked signal. Once embedding is done, the watermarked video can be subjected to various attacks. The common attacks of video watermarking are frame dropping, frame averaging, statistical analysis, lossy compression, cropping. Techniques used for embedding are DCT, DWT, and PCA.

Md. Asikuzzaman et al. [14] proposed a basic blind digital video watermarking algorithm, the watermark was embedded into one level of dual-tree complex wavelet transform from the chrominance channel to provide superior quality watermarked video. This algorithm is robust to various geometrical attacks such as upscaling, rotation, and cropping.

Raoet et al. [15] a robust video watermarking technique is proposed. Here, frames are extracted from the video. Video frames are converted from RGB to YCbCr and SVD is applied over both video and watermark. The watermark bits are embedded diagonally in one of the three SVD matrices and video is reformed after converting video frames from YCbCr to RGB again. This method is inadequate for general use and there is need to improve the robustness of this method.

III. Proposed Work

A. Methodologies

1. Lifting Wavelet Transform

Signal transform is used to transform the signal to the different domain, perform several operations on the transformed signal and inverse the transform and bake to the original domain i.e. transform should be invertible. Wavelet transform can be performed using filter bank i.e. Low pass filter and high-pass filter. Lifting scheme splits the samples into odd and even samples. In 1998, Sweldens et al. designed the Lifting Wavelet Transform, second generation wavelet transform to extend the utility of wavelet methods. Lifting method is simple and efficient scheme as there is no complex mathematical calculation. Digital signal is generally a sequence of integer numbers, whereas wavelet transforms outputs in floating point numbers. For the efficient inverse transformation integer to integer, conversion is important. LWT can be modified to operate on integers and thus during inverse transform rounding error can be avoided [16].

LWT consist of main three steps:

(i). Split

Here it splits the signal into odd signal subsets (the wavelet coefficients filtered through the high-pass filter) and even signal subsets (filtered through lowpass filtered).

(ii). Predict

Here only even signal subsets are used to divide the signal into odd and even signal subsets by transforming odd signal subsets into wavelet coefficient.

(iii). Update

Here even signal subsets will be processed using wavelet coefficient, computed in predict phase for calculating the scaling function.

In Lifting wavelet decomposition image is decomposed into approximation coefficient subset (cA) and detail coefficient subsets, horizontal (cH), vertical (cV) and diagonal (cD).

2. YCbCr

For color image watermarking, several color space representations have been reported in the literature. Most commonly RGB, YIQ, YCbCr, YUV, HSI, HSV etc. color spaces are used for watermarking. Most of the early work used RGB representation and watermark embedding in Blue channel but blue channel embedding suffers against compression types of attacks such as JPEG because, in JPEG Compression, Blue channel is heavily quantized. Therefore, embedded watermark is lost up to great extent. A study about the selection of appropriate color space and choice of suitable channel for watermark embedding is presented in [17]. It says that the Y-channel in YCbCr system is the ideal space for data hiding whenever tolerance against JPEG compression and noise addition are the most important concerns. On the other hand, Cr-channel in the same color space is the best choice when the proposed algorithm should resist against scaling and rotation attacks while Cb-channel is a better option for resistance against cropping. To achieve maximum robustness against the majority of attacks YCbCr color space is used for watermarking. JFIF-YCbCr conversion as defined in CCIR 601 (256 levels) standard is chosen for proposed scheme [18] to achieve maximum compatibility and robustness against JPEG type of compression. The conversion rule for RGB to JFIF-YCbCr is given below [19]

B. Proposed Algorithm

1. Embedding Algorithm

Input: Cover Video and Watermark Image

Output: Watermarked Video

- Read cover video 'P'and watermark image 'WI' with NXN size.
- The cover video and watermark image are converted into YCbCr color space from RGB color space and one of the channels is chosen for embedding.
- Perform 1-LWT on the Y channel of P and WI to split into four groups.
- Perform 2-LWT on the LL, LH, HL, HH band of P and WI

to split into four groups.

- Modify the wavelet value of S_i by embedding the wavelet value of watermark image such that

$S_e = S_i + alpha*S_j$

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.

- Perform the two-level inverse LWT (ILWT) on the LWT transformed image, to obtain the watermarked video on four coefficients.

Input: Watermarked Video

Output: Attacked Video

- Apply Rotation Attack, Resizing Attack and Gamma Correction Attack on watermarked video for security and robustness.

Extraction Algorithm

Input: Watermarked Video

Output: Extracted Watermark Image

- Apply two levels LWT transform to decompose the watermarked frames W into four overlapping sub-bands.
- Modify the wavelet value of Si by extracting the wavelet value of watermarked frames such that

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

- Perform the two-level inverse LWT (ILWT) on the LWT transformed image, to obtain the extracted watermark image on four coefficients.

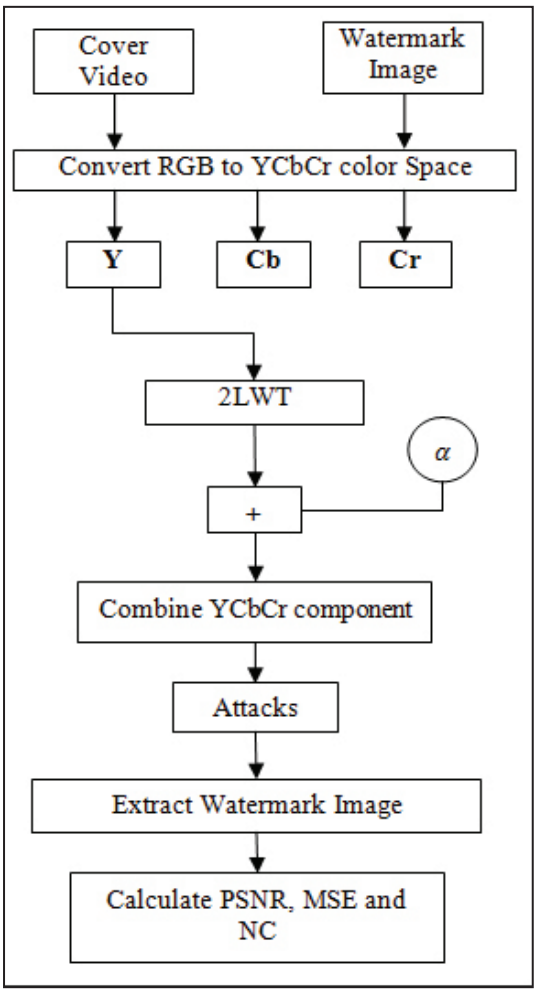


Fig. 1: Block Diagram of Proposed Architecture

Fig. 2: Calculate PSNR and MSE value of watermarked video and cover video.

$$MSE(x) = \frac{1}{N}||x - x\hat{}||^2 = \frac{1}{N}\sum_{i=1}^{N}(x - x\hat{})^2$$

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

$$PSNR(x) = \frac{10\ X\log((255))}{MSE(x)} \quad (10)$$

Where m is the maximum value of the cover video

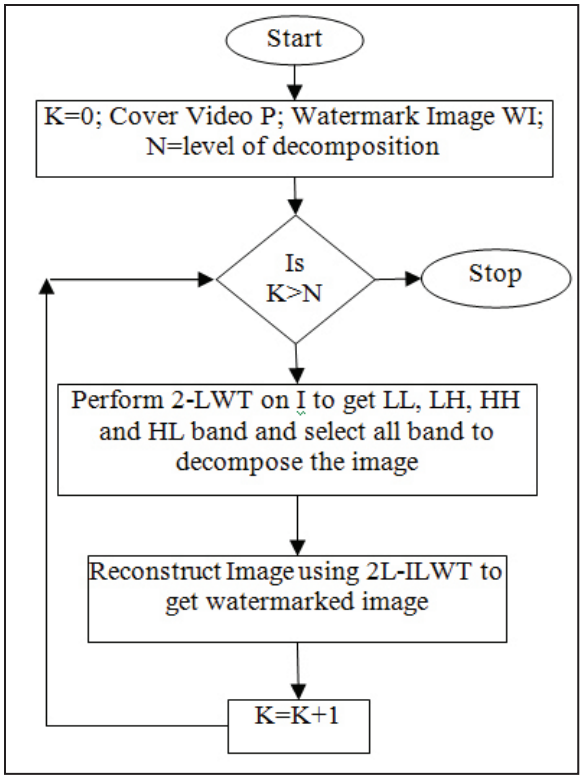


Fig. 3: Flow Chart of Embedding System

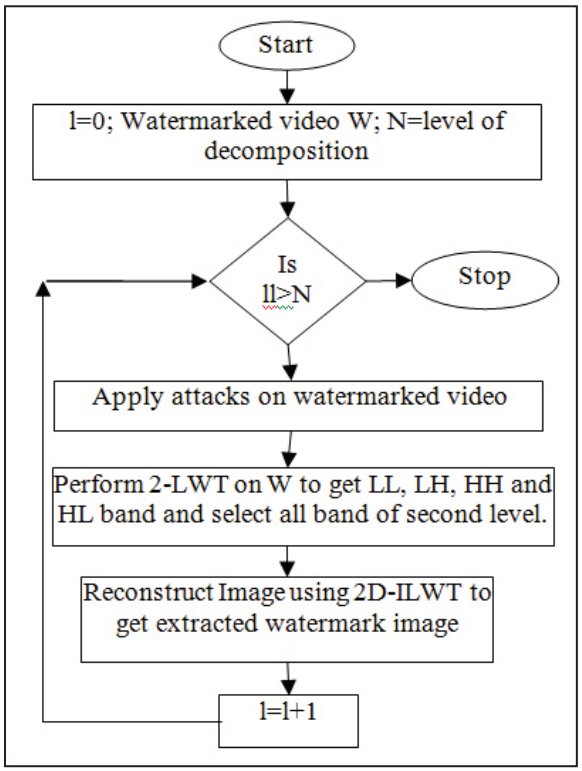


Fig. 3: Flow Chart of Extraction System

ISSN : 0976-8491 (Online) | ISSN : 2229-4333 (Print)

IV. Result Analysis

This section presents the experimental results and their analysis. The performance of the algorithm can be measured in terms of its imperceptibility and robustness against the possible attacks. The watermarked frame is subjected to a variety of attacks such as Gamma correction, Contrast adjustment, etc. In case of geometric attacks, the scheme is tested against Frame resizing, Frame rotation. To evaluate the performance of any watermarking system, Peak Signal to Noise Ratio (PSNR) is used as a general measure of the visual quality of the watermarking system.

PSNR: The Peak-Signal-To-Noise Ratio (PSNR) is used to measure the deviation of the watermarked and attacked frames from the original video frames and is defined as:

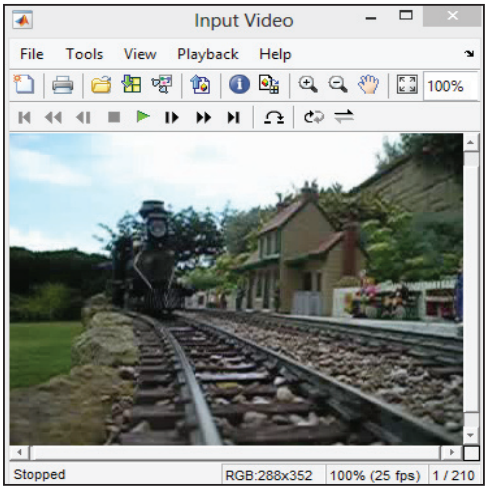


Fig. 5: Shows Cover Video

Fig. 6: Shows Watermark Image

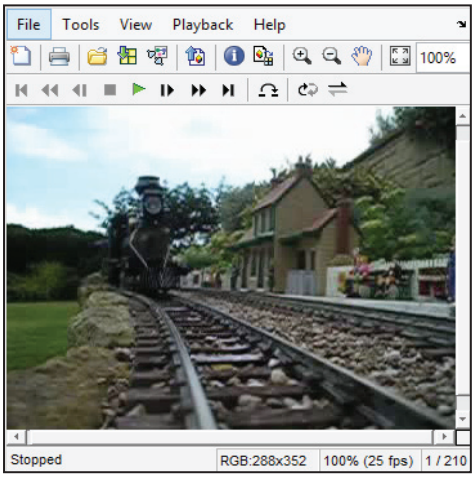


Fig. 7: Shows Watermarked Video

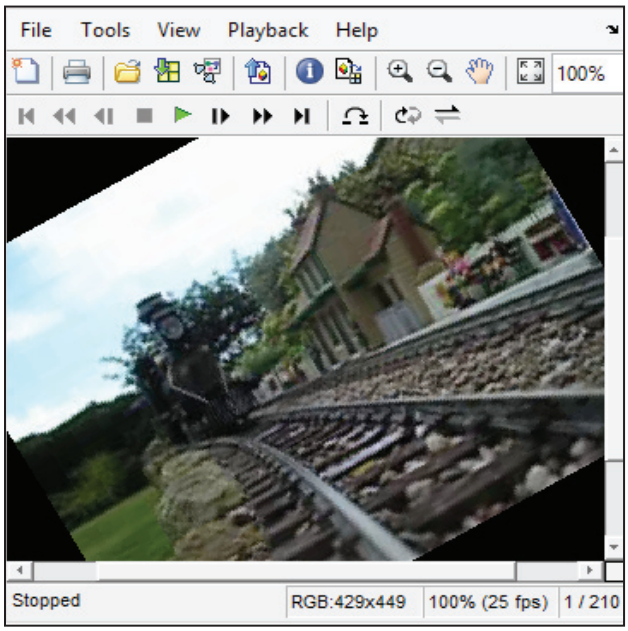


Fig. 8: Shows Rotation Attack Video

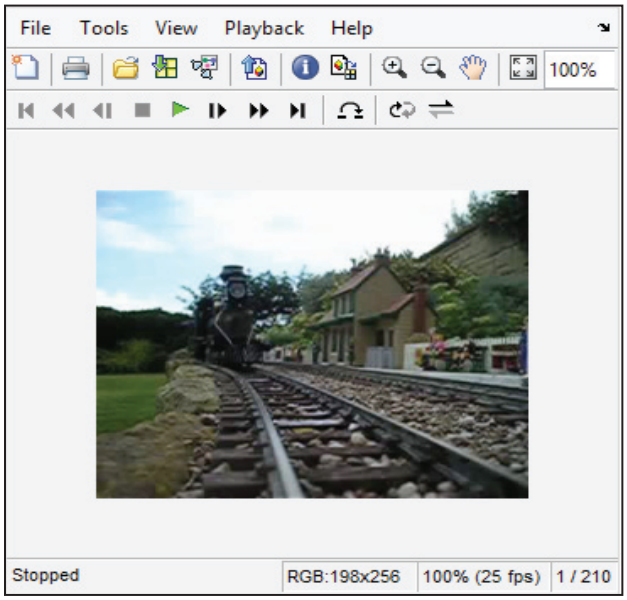


Fig. 9: Shows Resizing Attack Video

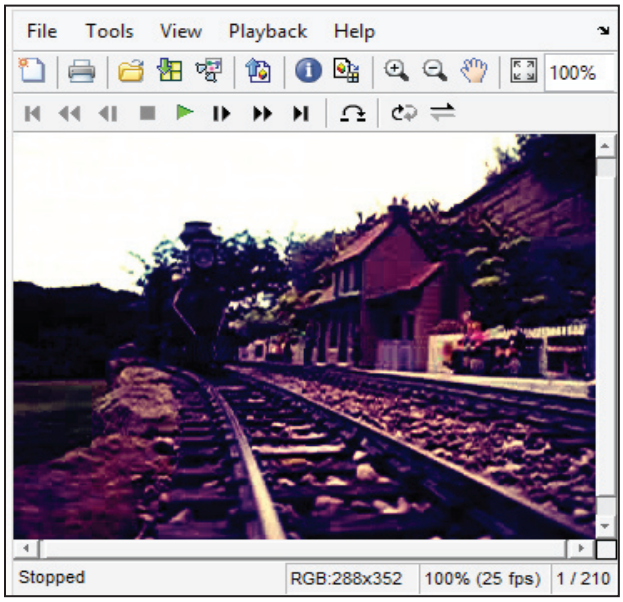


Fig. 10: Shows Gamma Correction Attack Video

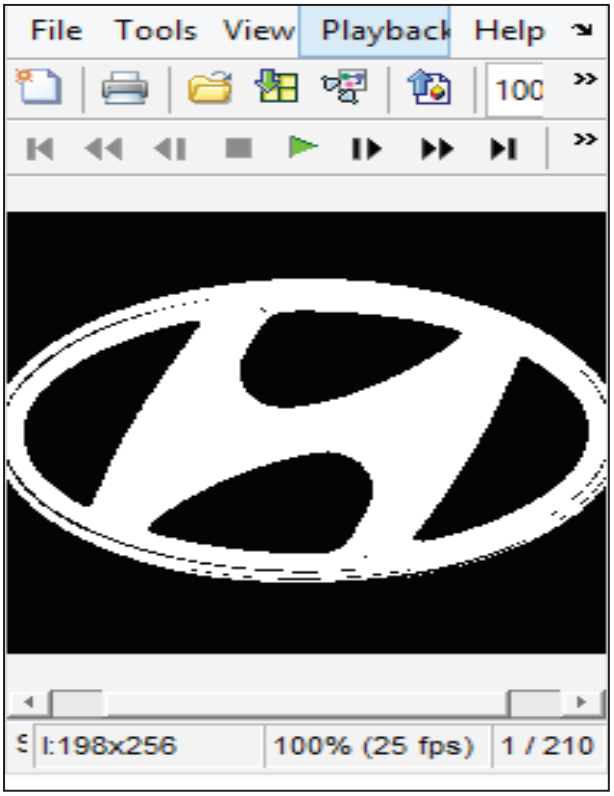


Fig. 11: Shows Extracted Watermark Image

Table 1: PSNR Comparison Between REF and Proposed for Embedding and Extracting.

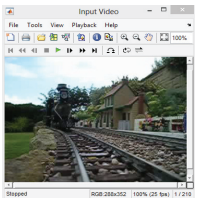
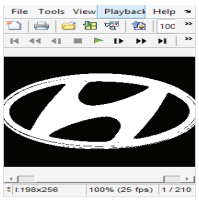
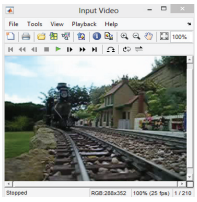
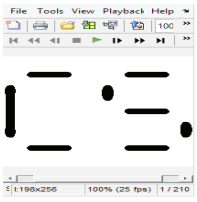
Cover Video	Extracted Watermark Image	Ref Embedding PSNR	Proposed Embedding PSNR	Ref Extracted PSNR	Proposed Extracted PSNR
		76.8005	121.42	12.5580	21.6033
		71.4884	109.19	0.4682	18.6998

Table 2: NC and PSNR Comparison Between REF and Proposed for Watermarking.

Attack	Ref NC	Proposed NC	Ref PSNR	Proposed PSNR
Rotation	-1.4858	0.4281	14.3519	76.97
Resizing	-2.7587	0.9198	26.6591	85.89
Gamma Correction	-1.4691	0.8727	18.4797	80.77

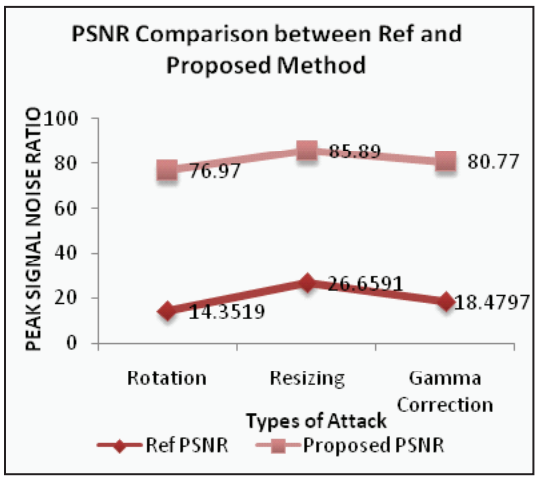


Fig. 12: Shows PSNR Comparison

V. Conclusion

This paper presents secure transmission for digital watermarking using two-level Lifting Wavelet Transform (LWT) and the algorithm is required for the security of the content. From the observation, we can say that proposed estimation exhibits its proficiency against attacks. The trial results, evaluate the eventual outcome of the existing technique and proposed technique considering the parameters of PSNR and Normalized Correlation. From the results, we can say that the proposed technique works better than the previous techniques. The PSNR is 85.89after the attacks. NC is close to 0.9198 which shows the robustness to the attacks. The performance analysis validates that the presented watermarking method has good imperceptibility too. The comparison outcomes with DWT based algorithm. It shows that the superiority of our method.

References

[1] Ikpyo Hong, Intaek Kim, and Seung-Soo Han "A Blind watermarking technique using Wavelet transform," In IEEE International Symposium on Industrial Electronics, pp.1946-1950, 2001.

[2] G. Ramkumar and M. Manikandan, "Uncompressed Digital VideoWatermarking Using Stationary Wavelet Transform," In IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), pp.1252-1258, 2014.

[3] C. Rawat, C. D., and Sneha M. Shivamkutty. "Digital watermarking of video using hybrid techniques." In IEEE International Conference on Advances in Communication and Computing Technologies (ICACACT), pp. 1-5, 2014.

[4] Ponnisathya, S., S. Ramakrishnan, S. Dhinakaran, P. Sabari Ashwanth, and P. Dhamodharan. "CHAOTIC map based video watermarking using DWT and SVD." In IEEE International Conference on Inventive Communication and Computational Technologies (ICICCT), pp. 45-49, 2017.

[5] T. Jayamalar, V. Radha, "Survey on digital video watermarking techniques and attacks on watermarks", International Journal of Engineering Science and Technology, Vol. 2, No. 12, pp. 6963-6967, 2010.

[6] Kothari, Ashish M., and Ved V. Dwivedi. "Performance Analysis of Digital Video Watermarking using Discrete Cosine Transform." International Journal of electrical and Computer engineering systems, Vol. 2, No. 1, pp. 11-15, 2011.

[7] Yassin, Nisreen I., Nancy M. Salem, and Mohamed I. El Adawy. "Block based video watermarking scheme using wavelet transform and principle component analysis." International Journal of Computer Science (IJCSI) Vol. 9, No. 1, pp. 296-301, 2012.

[8] Li, Jianfei, Yongbin Wang, and Shusen Dong. "Video watermarking algorithm based DC coefficient." In 2nd IEEE International Conference on Image, Vision and Computing (ICIVC), pp. 454-458, 2017.

[9] Gonge, Sudhanshu Suhas, and Ashok A. Ghatol. "An enhancement in security and copyright protection technique used for digital still image." In IEEE International Conference on Nascent Technologies in Engineering (ICNTE), pp. 1-9, 2017.

[10] Kadu, Sneha, Ch Naveen, V. R. Satpute, and A. G. Keskar. "Discrete wavelet transform based video watermarking technique." In IEEE International Conference on Microelectronics, Computing and Communications (MicroCom), pp. 1-6, 2016.

[11] Kaur, Harpreet, and Veerdeep Kaur. "Invisible video multiple watermarking using optimized techniques." In IEEE Online International Conference on Green Engineering and Technologies (IC-GET), pp. 1-9, 2016.

[12] Mahmoud, Abdulqader, Hamza Al Maharmeh, and Hussain Al-Ahmad. "A new watermarking algorithm for scanned colored PDF files using DWT and hash function." In IEEE International Conference on Information and Communication Technology Research (ICTRC), pp. 140-143, 2015.

[13] Rini T Paul "Robust Video Watermarking Techniques Computational Science – New Dimensions & Perspectives", North Coastal Consortium for Special Education (NCCSE), pp. 90-95, 2015

[14] H. Sadreazami, M. O. Ahmad, and M. N. S. Swamy, "A study of multiplicative watermark detection in the contourlet domain using alpha-stable distributions," IEEE Transactions on Image Processing, Vol. 23, No. 10, pp. 4348- 4360, 2014.

[15] Rao, Y. Raghavender, E. Nagabhooshanam, and Nikhil Prathapani. "Robust video watermarking algorithms based on svd transform." In IEEE International Conference on Information Communication and Embedded Systems (ICICES), pp. 1-5, 2014.

[16] Sejpal, Shveti, and Nikesh Shah. "Comparative Performance Analysis of Secured LWT-SVD Based Color Image Watermarking Technique in YUV, YIQ and YCbCr Color Spaces." International Journal of Computer Applications, Vol. 147, No. 7, 2016.

[17] EhsanVahedi, Reza Aghaeizade Zoroofi, and Mohsen Shiva, "On Optimal Color Coordinate Selection for Wavelet-based Color Image Watermarking", International Conference on Intelligent and Advanced Systems, pp. 635 - 640, 2007.

[18] JPEG File Interchange Format (JFIF) Version 1.02 from http://www.jpeg.org/public/jfif.pdf accessed on 10/10/2012.

[19] Verma, A. K., Mayank Singhal, and C. Patvardhan. "Robust temporal video watermarking using YCbCr color space in Wavelet domain." In IEEE 3rd International conference on Advance Computing Conference (IACC), pp. 1195-1200, 2013.