International Journal of Electrical, Electronics and Computer Engineering **3**(2): 45-51(2014)

ISSN No. (Online): 2277-2626

To perform digital image watermarking by inverse 5/3 Integer Wavelet Transform

Neha Sahu*, Irshad Ahamad** and Vasim Khan**

**PG Scholar, Department of Electronics and Communication Engineering, Vikrant institute of technology, Indore, (MP) India*

***Associate Professor, Department of Electronics and Communication Engineering, Vikrant institute of technology, Indore, (MP) India*

(Corresponding author: Neha Sahu)

(Received 05 July, 2014 Accepted 09 August, 2014)

ABSTRACT: This paper aims to implement the watermarking technique to perform digital image watermarking. In this scheme first step is decomposition original image by using 5/3 Integer Wavelet Transform, watermark sequence generated by using histogram values of LL1 band. This watermark sequence embedded into LL1 band by using 2-D interleaving technique, and applied to inverse 5/3 Integer Wavelet Transform to get watermarked image. Then we apply the different attacks on watermarked image to evaluate its performance. In this scheme extraction of watermark sequence in two independent methods there by detecting tampering in the image. In this paper the proposed algorithm is efficiently implemented in MATLAB.

Index Term: Digital Image Watermarking, 5/3 integer wavelet transform, attacks on digital watermark.

I. INTRODUCTION

The inception of the internet has resulted in many new opportunities for the creation and delivery of content in digital form; applications include real-time video electronic advertising, digital repositories and libraries and audio delivery, and Web publishing. An important issue that arises in these applications is the protection of the rights of all participants. As digital media is getting more popular, its security related issues are becoming a greater concern. Growth of digital media could lead to replicate unlimited number of perfect copies that can be illegally produced, which is a great threat to the rights of content owners. The authors of a work are self-effacing to make such information available on the internet as it may be copied and retransmitted without the permission of the author. Now it is an issue, how to protect the copyright and intellectual property rights of those who legally own or possess digital works. Authors also may want samples of their works to be available [1]. Growth of Internet has resulted in increased use of Copyright marking, as it facilitates images, audio, video, etc to available in digital form. Though this provides an additional way to distribute material to end-users, it has also made far easier for copies of copyrighted material to be made and distributed. Using the internet a copy stored on a computer can be shared easily with anybody regardless of distance often via a peer-to-peer network which does not require the material to be stored on a server and therefore makes it harder for the copyright owner to locate and prosecute offending parties. Copyright marking is seen as a partial solution to these problems**.** The process of embedding information into another signal can be termed as watermarking [2].

Watermark is information, which is imperceptibly added to the cover-signal in order to convey the hidden data. The image in which secret information (watermark) is embedded is called host image [3]. The image after embedding the watermark is called watermarked image. Embedding and extractions are the two important steps of watermarking

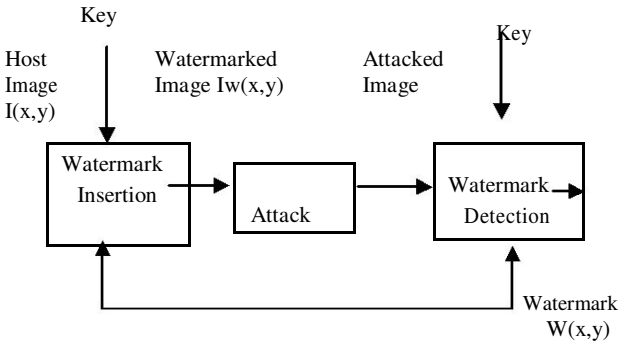

Fig. 1. Block diagram of image watermarking.

Fig. 1 shows the block diagram of image watermarking. The host image *I(x,y)* and watermark message *M(x, y)* is applied to the watermark embedding block. We are embedding some random sequence into the host image. The embedded image (water marked image) is $I_M(x, y)$. While transmitting the watermarked image there may be some intentional and unintentional attacks on the watermarked image. So *W(x, y)* is the attacked image [4].

We are applying attacked image and watermark message to the detection block, which gives the information regarding watermark is present or not in the image.

II. WATERMARK EMBEDDING

Watermark embedding is used to insert the watermark into the host image. This is the first block of the image watermarking process

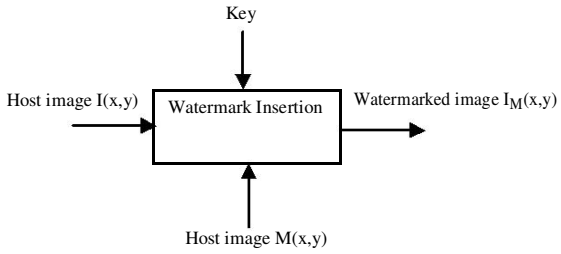

Fig. 2. Watermark Embedding.

Here I(x, y) is the original image or host image in which watermark is embedded. *M(x, y)* is the watermark message which will be embedded into the host image. The key has a one-to-one correspondence with Watermark signal which means, a unique watermark key exists for every watermark signal. The key is concealed and known to only authorized parties and it ensures that only authorized parties can detect the watermark. Further, note that the communication channel can be noisy and hostile, that is prone to security attacks and hence the digital watermarking techniques should be flexible to both noise and security attacks. Watermark is an identifying feature, like a company logo, which can be used to provide protection of some host data. A watermark may be either visible i.e. perceptible or invisible i.e. Imperceptible both of which offer specific advantages when it comes to protecting data[5]. Watermarks may be used to prove ownership of data, and also as an attempt to enforce copyright restrictions. Thus using watermark embedding process watermark is embedded into the host image.

III. WATERMARK EXTRACTION

Watermark extraction is used to extract the watermark present in the watermarked image.

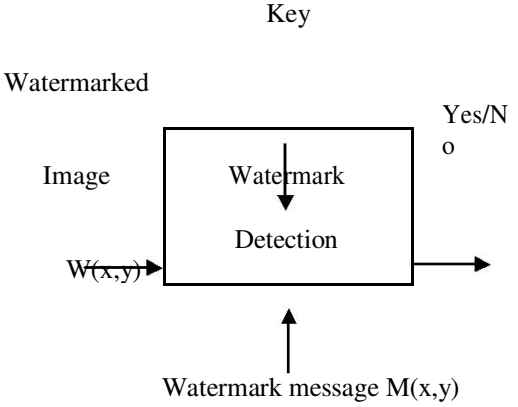

Fig. 3. Watermark Extraction.

IV. INTRODUCTION TO 5/3 LIFTING BASED INTEGER WAVELET TRANSFORM

In many applications (e.g. image compression and processing) the input data consists of integer samples. In addition the storage and encoding of integer numbers is easier, compared to floating point numbers. Unfortunately all of the above transforms assume that the input samples are floating point values. They return floating point values as wavelet coefficients, even if the input values actually were integer. Rounding the floating point values to integer values does not help because perfect reconstruction feature will be lost.

Fortunately the lifting scheme can be easily modified to a transform that maps integers to integers and it is reversible, and thus allows a perfect reconstruction. This will be done by adding rounding operations, at the expense of introducing a non-linearity in the transform.

In the recent past, lifting-based II^{nd} generation wavelet transforms have been proposed by Sweldens. The lifting technique requires three phases for its implementation, namely: split phase, predict phase and update phase. The 5/3 filter bank is an important class of biorthogonal filter where all filters have finite impulse response and linear phase. The 5/3 filter bank also belongs to a special class of integer-to-integer filter banks that maps integers to integers, allowing exact recovery of input signal by preventing rounding off errors. This property makes the 5/3 filter bank an ideal choice for lossless compression in the JPEG2000 standard [6]. The structure of 5/3 filter bank is relatively simple as a result; Prediction and update steps for this filter bank are straight forward. Due to its property of integer-to-integer transformation, it has recently being used for image watermarking applications [7].

The 5/3 Daybechies biorthogonal wavelet has received a wide range of interest in various applications due to its filter tap coefficients are particularly useful in real-time implementation. Furthermore, the lifting implementation of this wavelet contains filters with coefficients that can be written as powers of two leading to a multiplication free realization of the filter-bank. Several linear or nonlinear decomposition structure that are published in the literature report better performance than the 5/3 wavelet using signal adapted filters including. Among these works shows the method to achieve the lifting style implementation of any DWT filter bank, whereas extends the idea of linear filters in the lifting style to nonlinear filters. The prediction filter was made adaptive according to the local signal properties, the 5/3 wavelet has an efficient set of filter coefficients which Enables fast, simple, and integer-shifts-only implementations, and due to these properties it was also adapted by the JPEG-2000 image coding standard in its lossless mode.

V. WATERMARKING TECHNIQUE USING IWT

In this scheme the image is processed using 2-level 5/3 integer wavelet transform (IWT) to get integer wavelet coefficients.

For embedding watermark, LL1 sub-band (shown in Fig. 4) is used because the perceptual distortion at low frequencies is less and hence strong watermark can be embed [8]. To have self-authentication capability, some image property must be used for generating watermark sequence. Further, the watermarking process should be such that this image property does not change after watermarking. To achieve this, histogram of wavelet coefficients of the LL1 band is used to generate the watermark sequence. Let *Ixy*, Original and *I'xy*, be the watermarked pixel intensity, respectively. *Cxy* and *C'xy* are the wavelet coefficient before and after embedding, i.e. in the LL1 sub-band.

VI. WATERMARK EMBEDDING

Input host image is color image from this blue plane is separated. This blue plane is decomposed by using 2-level 5/3 lifting based Integer Wavelet Transform results into four sub bands those are LL1, LH1, HL1 and HH1 shown in Fig. 4.

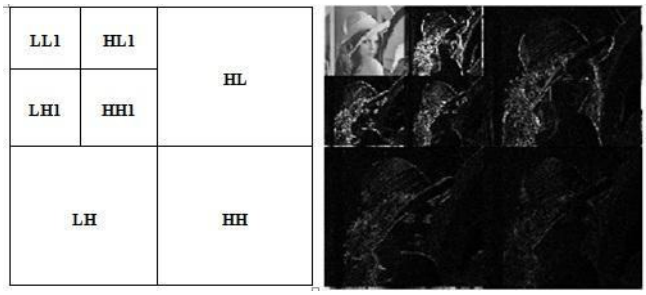

Fig. 4. Original image decomposed by 2-level Integer Wavelet Transform.

VII. GENERATION OF WATERMARK SEQUENCE

Intensity histogram of the wavelet coefficient in LL1 band is calculated and segmented into „*k'* non-overlapping bins of Θ interval. The i^{th} bin Θi *contains* pixel intensity in the range of $[(i-1)*\Theta : i*\Theta]$. The number of pixels (*ni).* In Θi bin is evaluated and concatenated to give a string *N* expressed as

$$N = [n_1 n_2 n_3 \ldots n_k] \quad \ldots(1)$$

This „*N'* is used to generate a pre-watermark sequence (W_p) in which each decimal count n_i is represented by *b* bits binary equivalent expressed as

$$W_p = [W_{p1} W_{p2} W_{p3} \ldots W_{p\theta}\ ,\ W_{pi} \varepsilon (1,0)] \quad \ldots(2)$$

Where $\Theta = k*b$. To reduce false detection during extraction of the watermark, this pre-watermark sequence is spread using two orthogonal codeword of length „*L*" as

$$\begin{pmatrix} \hat{W}_{ni} \text{ --- -> } v_1 & \Xi\ [v_1 v_2 v_3 \ldots v_L] \text{ if } W_{pi} = 0 \\ \hat{W}_{pi} \text{ --- -> } v_2 & \Xi\ [v_1 v_2 v_3 \ldots v_L] \text{ if } W_{pi} = 1 \end{pmatrix} \quad \ldots(3)$$

Finally, the spread watermark sequence (W) to be used for embedding is

$$W = [\hat{w}_1\ \hat{w}_2\ \hat{w}_3 \ldots\ldots\ \hat{w}_o]$$

Where

$$\begin{pmatrix} \hat{wi} = \hat{v1}\ ,\ \ Wpi = 0 \\ \hat{wi} = \hat{v2}\ ,\ \ Wpi = 1 \end{pmatrix} \quad \ldots(4)$$

In order to have blind self-authentication capability, histogram values of LL1 band before and after watermarking should be unchanged [1]. Thus, the watermark embedded should be such that, no coefficient changes its bin. Depending on the value „0" or „1" to be embedded, the wavelet intensity coefficients (*Cxy*) are re-quantized as an integral multiple of two integer values Ψ1 or Ψ2, respectively. The re-quantization of a pixel *Cxy* falling in a bin Θi is restricted within its bin range, thereby preserving the histogram of the watermarked image. To make the watermark more robust to impulsive noise, the embedding done uses 2-D interleaving. Watermark embedding at location *x, y* in the sub-band LL1 is carried out by first identifying the bin to which it corresponds.

Embedding a „0" or „1" is achieved by altering the coefficient *Cxy* to *C'xy* shown in Fig. 4.

The Blind water marking scheme is implemented in the following procedure. The property that we use here to generate the water marking is the histogram of the image. The histogram of the image is calculated after it is decomposed by „2" levels using 5/3 IWT using lifting scheme. The image is divided into (k) number of bins (eg.

5) which are of (θ) interval (that means: total number of pixel values range from „0" to „255" I.e., 256/5=51 bits in one interval) .So, we get „5" different values of histogram. We convert the decimal value of the histogram values into 16- bit binary value which is said to be a pre-watermarking sequence. These bits are assigned with different code sequences for „1"and „0".That is we generate a different 7-bit sequence for „0" and another 7-bit for „1".The resultant sequence is watermarking sequence.

VIII. EMBEDDING PROCESS

Embedding process is done by re-quantize the coefficient value of the LL1 band in order to embed „0"or „1".In order to embed „1" or „0" the re-quantized value is defined by the below equation.

For „0"

$$[C'xy\ \alpha] = \min(\text{abs}(Cxy - \Psi 1\mu)) \quad \mu = 1, 2, \ldots 9$$

$$C'xy = \Psi 1\alpha$$

Where „α" is the value of μ for which the absolute value of difference between *Cxy* and product „Ψ1α" is minimum with the condition that later remains in the same bin „Θi' as *Cxy*. Similarly, to embed a „1" following processing is carried out:

For „1"

$[C'xy\beta] = \min(\text{abs}(Cxy - \Psi 2\mu))\ \mu = 1,2,\ldots 9$

$C'xy = \Psi 2\beta$

Where „β" is the value of „μ" for which absolute value of difference between Cxy and product „Ψ1 β" is minimum.

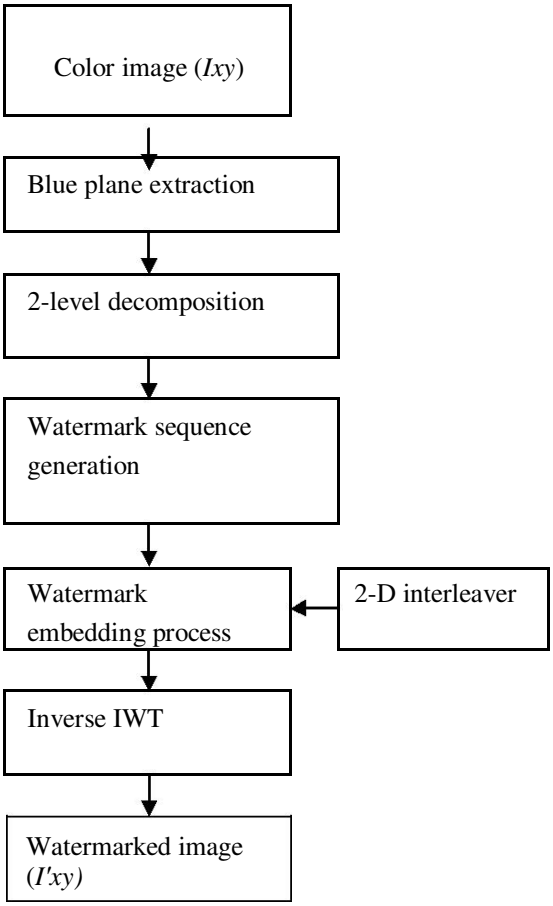

Fig. 5. Block diagram for watermark Embedder.

Finally applying inverse 2-level IWT, the watermarked image with modified pixel intensity is generated.

IX. HISTOGRAM METHOD

A second watermark sequence W″p is calculated using the LL1 sub band bin intensity histogram by applying Equations. (1.1)–(1.4). Finally, Authentication-Cum-Robustness (χ) function is computed as

$$X = W'p \odot W''p .$$

Where „⊙" denotes the correlation value between W′p and W″p. A threshold $\square_0(0.46)$ can be set for deciding about the presence of watermark and if it is equal to

„1" then the image is self authenticated as well. For robustness measure of the proposed watermarking scheme.

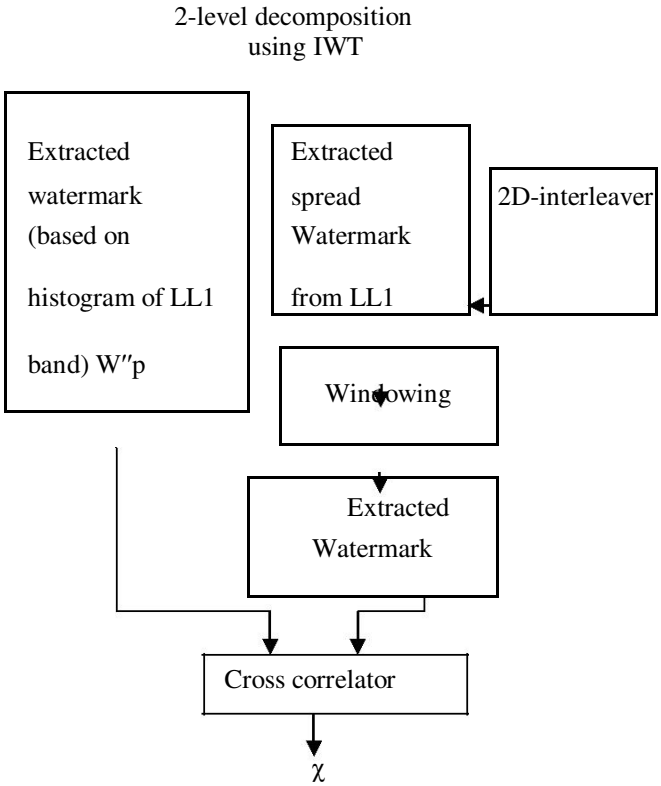

Fig. 6. Block diagram for watermark Detector.

X. SIMULATION RESULTS WITHOUT ATTACK

Watermark sequence of length 560 is embedded in the original color image and the difference image and watermarked image is obtained. Fig.4.5 shows the original image, decomposed image, watermarked image and difference image

Table 1. Performance metrics without any attack.

χ	PSNR (dB)	MSE	SIM	BCR
0.708	**85.27**	**3.5415**	**1.000**	**0.9321**

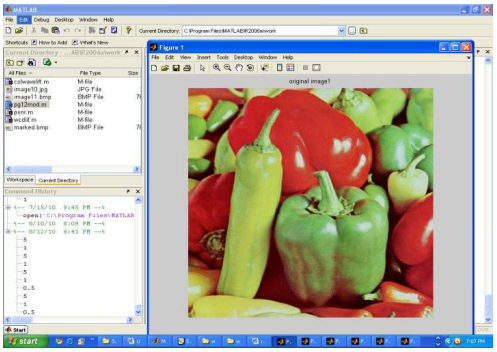

Fig. 7 (a): Original Image.

Fig. 7 (a) is an input to the embedding technique which is a original color image

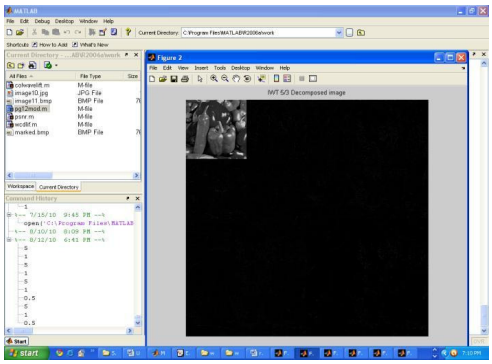

Fig. 7 (b): Decomposed Image.

Decomposed image is obtained after applying the original image to 2 level decomposition using IWT

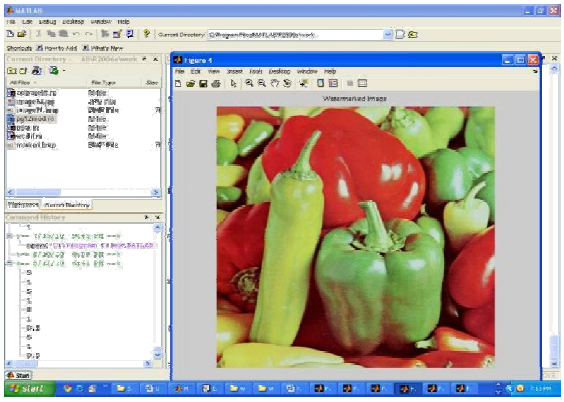

Fig. 7 (c): Watermarked images.

Watermark sequence of 560 bits (using histogram of LL1 band) are embedded into LL1 band of image, finally applying inverse 2-level IWT, watermarked image with modified pixel intensity is generated. Observing figures 7(c) and 7(d), there is no degradation in the perceptual quality.

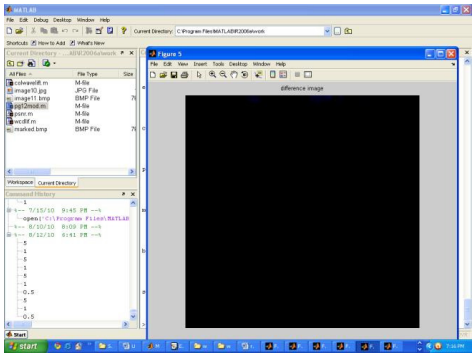

Fig. 7(d): Difference image.

The difference image is absolute difference of the pixel intensities of the watermarked image and the original image.
Figure 7: (a) Original, (b) Decomposed, (c) Watermarked, (d) Difference image

XI. SALT AND PEPPER NOISE

Image after adding salt and pepper noise of „0.04" noise density and recovered Histogram values are shown in Fig.8. Performance metrics of watermarked Image corrupted with salt and pepper noise of different noise densities is shown in Table 2.

Table 2 Performance metrics for salt and pepper noise Attack.

Noise density	χ	PSNR (dB)	MSE	BCR	SIM
0.01	0.679	49.39	220.55	0.921	0.994
0.02	0.693	43.35	442.05	0.925	0.988
0.03	0.547	39.94	654.70	0.889	0.983
0.04	0.635	37.46	670.72	0.107	0.978

As noise density increases PSNR value decreases and MSE increases. The correlation coefficient and similarity rate of the attacked image with respect to the original image is decreasing as the noise density is increasing.

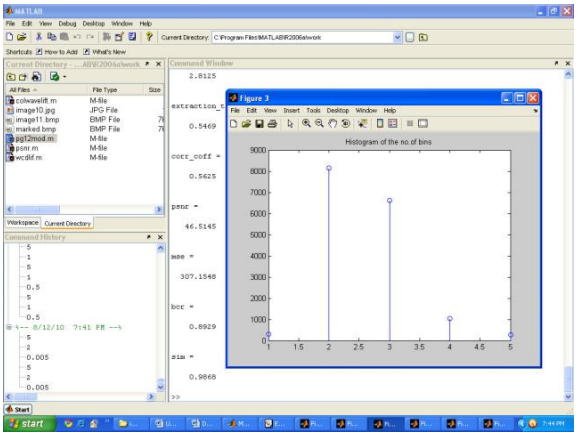

Fig.8(a): Histogram before embedding watermark.

Figure 8 (a) shows the graphical representation of histogram values of LL1 band of an image before embedding watermark.

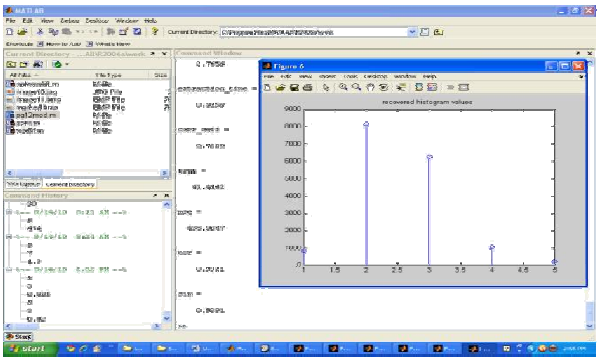

Fig. 8 (b): Recovered Histogram.

Fig. 8(b) shows the graphical representation of histogram values of LL1 band of watermarked image after embedding watermark. Observing figures 8(a) and 8(b), histogram values before embedding and after extraction from watermarked image are same. Hence self-authentication property is achieved.

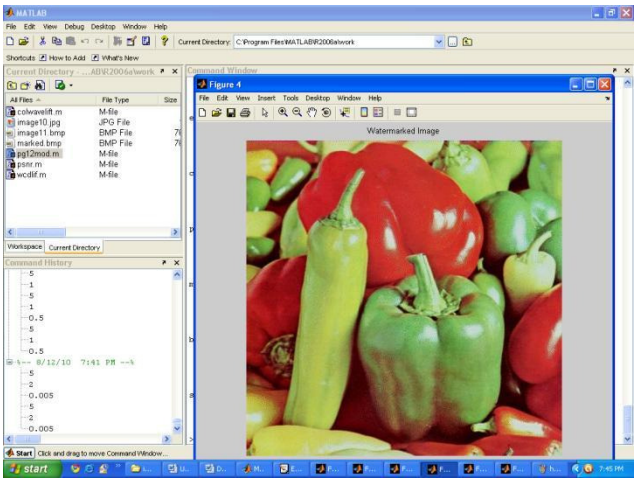

Fig: 8 (c). Watermarked image.

Watermark sequence of 560 bits (using histogram of LL1 band) are embedded into LL1 band of image, finally applying inverse 2-level IWT, watermarked image with modified pixel intensity is generated.

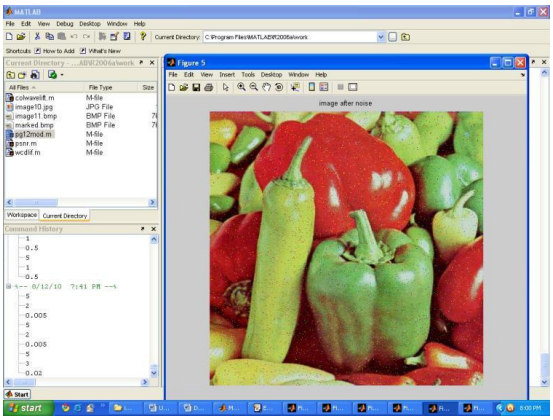

Fig. 8 (d). Salt and pepper of 0.04 noise density attacked image.

Fig. 8: (a) Histogram of original image, (b) Recovered Histogram (c) Watermarked image, (d) Salt and pepper noise attacked image.

XII. CONCLUSION

In this paper, a novel robust watermarking is implemented with self-authentication capability. It uses IWT, which requires less computation as compared to schemes based on conventional discrete wavelet transform. The key advantage of this scheme is its self-authentication capability along with robust watermarking while maintaining high perceptual quality. It is a blind self-authentication scheme, but requires the original embedded watermark sequence for evaluating the robustness measure from the results obtained it is evident that the implemented scheme can resist the common geometric attacks. A scheme for robust watermarking of images is being implemented based on second-generation wavelets (lifting based integer wavelet transform). The scheme along with its robustness has got the capability of blind self-authentication of the watermarked images. The watermarked images show no perpetual degrading and give peak signal to noise ratio (PSNR) in excess of 40 dB due to the use of integer-to-integer transform. Simulation results show the superior performance of the implemented scheme as compared to similar existing schemes under different attacks such as filtering, compression and rotation

REFERENCES

[1] Amit Bohra, Omar Farooq, Izharuddin, "Blind self-authentication of images using Integer wavelet transform", *International Journal AEU of electronics and communication,* May 2008.

[2] Zou D, Shi YQ, ZN, Su W. "A semi-fragile lossless digital watermarking scheme based on integer wavelet transforms". *IEEE Trans Circuits System Video Technology* 2006; **16**(10): 1294–300.

[3] Yuan Y, HD, Liu D. "An integer wavelet based multiple logo watermarking scheme. *In: 1st International multi symposiums on computer and computational sciences"*, vol. **2**, 2006.

[4] Xiaoyun W, Junquan H, G Z, Jiwu H. "A secure semi-fragile watermarking for image authentication based on integer wavelet transform with parameters". In: *Proceedings of the conference Australasian information security workshop*, vol. **44**, 2005. p. 75–80.

[5] Vizireanu DN, Preda,RO. A new digital watermarking scheme for image copywriting protection using wavelet packets. *In: 7th international conference on telecommunications in modern satellite, cable and broadcasting services*, vol. **2**, 2005. p.518-21.

[6] Ng TM, Garg HK. "Maximum-likelihood detection in dwt domain image watermarking using Laplacian modeling". *IEEE Signal Process Lett* 2005; **12**(4): 285–8.

[7] Bao P, Xiaohu M. "Image adaptive watermarking using wavelet domain singular value decomposition". *IEEE Trans Circuits Syst Video Technol* 2005; **15**(1):96–102.

[8] Liu HM, Liu JF, JWHDRH, Shi YQ. "A robust dwt-based blind data hiding algorithm". *Proc IEEE Circuits Syst* 2002; **2**: 672–5.

[9] Chun-Shien Lu, Hong-Yuan Mark Liao, "Multipurpose Watermarking for Image Authentication and Protection", *IEEE Transactions on Image Processing*, Vol. **10**, No. 10, 1579-1592, October 2001.

[10] WG1 I. J. Jpeg 2000 part i. Final committee draft Version 1.0.

[11] Lu CS, HYL. Sze CJ. Combined watermarking for image authentication and protection. *In: proceedings of IEEE international conference on multimedia and expo*, vol**. 3**, 2000.p-1415-8.

[12] Fridrich, J. and Goljan, M., "Comparing robustness of watermarking techniques"in Security and Watermarking, vol. 567. *San Jose CA: Soc. for Imaging Science. and Tecnology and Intl. Soc. for Optical Eng*., pp. 214-225. 1999.

[13] F. Bartolini, M. Barni, V. Cappellini, and A. Piva, "Mask Building for Perceptually Hiding Frequency Embedded Watermarks," *Proc. Int. Conf. on Image Processing,* Oct. 1998, vol. **I**, pp. 450-454.

[14] Kundur D, Hatzinakos D. "Towards a telltale watermark techniques for tamper proofing. *Proc IEEE Int Conf Image Process*" 1998; **2**:409–13.

[15] J. Delaigle, C. De Vleeschouwer, and B. Macq, "Psychovisual Approach to Digital Picture Watermarking," *Journal of Electronic Imaging*, vol. **7**, no. 3, pp. 628-640, July 1998.

[16] P. Bas, J. Chassery, and F. Davoine, "Using the Fractal Code to Watermark Images," *Proc. IEEE Int. Conf. on Image Processing,* vol. **I,** 1998, pp.469-73.

[17] Sweldens W. "The lifting scheme: a construction of second generation wavelets". *SIAM J Math Anal* 1998; **29**(2):511–46.

[18] Cox, J. Kilian, F. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," *IEEE Transactions on Image Processing,* vol. **6**, no. 12, pp. 1673-1687, Dec. 1997.

[19] X. Xia, C. Boncelet, and G. Arce, "A Multiresolution Watermark for Digital Images," *Proc. IEEE Int. Conf. on Image Processing,* Oct. 1997, vol. **I**, 548-51.

[20] Lu CS, Liao, HY. "Oblivious cocktail watermarking by sparse code shrinkage: a regional and global-based scheme". *In: Proceedings of international conference on image processing proceedings*, vol. **3**, 1987. p. 13–6.