Enhancement in Security and Copyright Protection Technique Using Digital Watermarking and AES

T.Sudheer Kumar [*1] , Naga Venkateshwara Rao.Kollipara [#2]

[*#]*ECE Department, St.Martins Engineering College, Dhulapally(v),Kompally,Secunderabad-500100,Telangana State ,India*

***Abstract*—As we know that, digital data are in various formats like text, audio, video, image, graphics, and message or in animated format. During transmission of digital data through channel, digital data requires of security as well as copyright protection. In this paper, 2-D digital still image is used for experimental purpose. There are variety of techniques and algorithms which can provide security and copyright protection services. The combination of DWT and DCT digital watermarking technique is used to provide copyright protection service and security services can be provided by AES technique using 256 bits key. The Combination of digital image watermarking and AES technique provides authenticity, copyright protection, and security to digital image against different attacks like Cropping, Gaussian noise, Salt and pepper noise, JPEG compression, Median filtering and Rotation attack**

***Keywords*— Gaussian noise, Salt and pepper noise, Median filtering, digital watermarking, AES technique, JPEG compression**

I. INTRODUCTION

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. One approach to copyrighting is to mark works by adding information about their relationship to the owner by a digital watermark. Digital watermarking provides a means of placing information within digital works. Digital watermarking is the process of embedding information into digital multimedia content such that the information can later be extracted for multiple purposes including copy prevention and control. The mark can be embedded in any legal versions and therefore be present in any copies made[1]. This helps the owner of the information to identify who has an illegal copy. Watermarking can be used to recognize owners, license information, or other information related to the cover carrying the watermark. Watermarks may also provide some control mechanisms such as determining if the work has been tampered with or copied illegally.

Another issue of concern in delivery of content in digital form is their security related issues which are becoming a greater concern. One key issue is confidentiality, which is typically achieved by encryption. The terminology steganography has a different flavour from encryption, its purpose is to embed a piece of critical information in a non-critical host message (e.g., Webpages, advertisements, etc.) to distract opponents' attention. Simple translation for Steganography is data hiding. There are various methods available in literature for hiding data, like cryptography, steganography and watermarking. Cryptography means secret writing and can be defined as the science of using mathematics to encrypt and decrypt data back. Third party can know that some message transfer is taking place, but cannot decrypt it without key. While cryptography is about protecting the content of the message, the steganography conceal even the existence of message from third party. Only sender and the intended receiver know how and where the message is kept[3]. Stenographic methods are not robust against attacks and modification of data that might occur during transmission or format conversion. An ideal stenographic system would embed a large amount of information perfectly securely, with no visible degradation to the host image. Watermarking is the branch of the steganography that has an additional requirement of robust against possible attacks. An ideal watermarking system, however would embedded an amount of information that could not be removed or altered without making the cover object entirely unusable.

Watermarking is closely related to Steganography, but there are differences between them: In watermarking the message is related to the cover. In Steganography typically relates to covert point-to-point communication between two parties. Therefore, steganography has limited robustness. Watermarking is frequently used whenever the cover is available to parties who know the existence of the hidden data and may have an interest in removing it[2]. Therefore, watermarking has the additional notion of resilience against attempts to remove the hidden data.

Principle Of Image Watermarking

The process of embedding information into another signal can be termed as watermarking. 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. The image after embedding the watermark is called watermarked image. Embedding and extractions are the two important steps of watermarking[9].

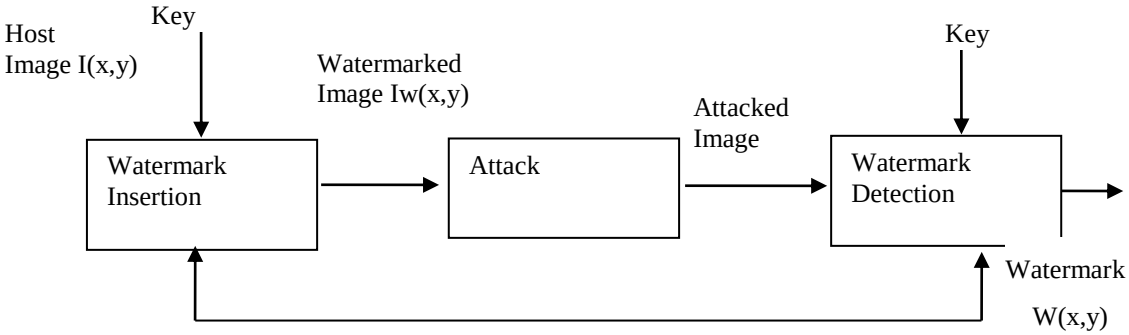

Figure 1: Block diagram of image watermarking.

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 (watermarked 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. EVALUATION OF WATERMARKING TECHNIQUE

The performance of watermarking technique can be evaluated depending upon the different factors. Performance matrix Measurements contains Peak Signal to Noise Ratio (PSNR), Correlation coefficient, Similarity Index Matrix (SIM), Correlation Coefficient (CC) and Bit Correction Rate (BCR). These performance matrices are evaluated to study the robustness of watermarking scheme.

If 'I' is the original image and I_W is the water marked (attacked) image of size M x N. Then performance matrices can be given below

Mean Square Error (MSE) is defined as

$$MSE = 1/M*N \left(\sum(I_W-I)^{2)}\right) \quad (1)$$

PSNR is defined as

$$PSNR = 10 \log 10 \left(I^2peak / MSE\right)db \quad (2)$$

Here Ipeak is 255

Similarity Index Matrix (SIM) is given as,

$$SIM = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} I(i,j) * I_w(i,j)}{\sum_{i=1}^{M}\sum_{j=1}^{N} I_w(i,j)^2} \quad (3)$$

Bit Correction Rate (BCR) can be given as,

$$BCR = \frac{\text{Total no.of correctly detected watermark bits}}{\text{Total no.of embedded watermark bits}} \quad (4)$$

These measurements are calculated to verify the robustness of the watermarking technique

III. . 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.2) is used because the perceptual distortion at low frequencies is less and hence strong watermark can be embed. To have self-authentication capability, some image property must be used for generating watermark sequence[5]. 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.

A. *Watermark Embedding*

Input host image is colour 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..2.

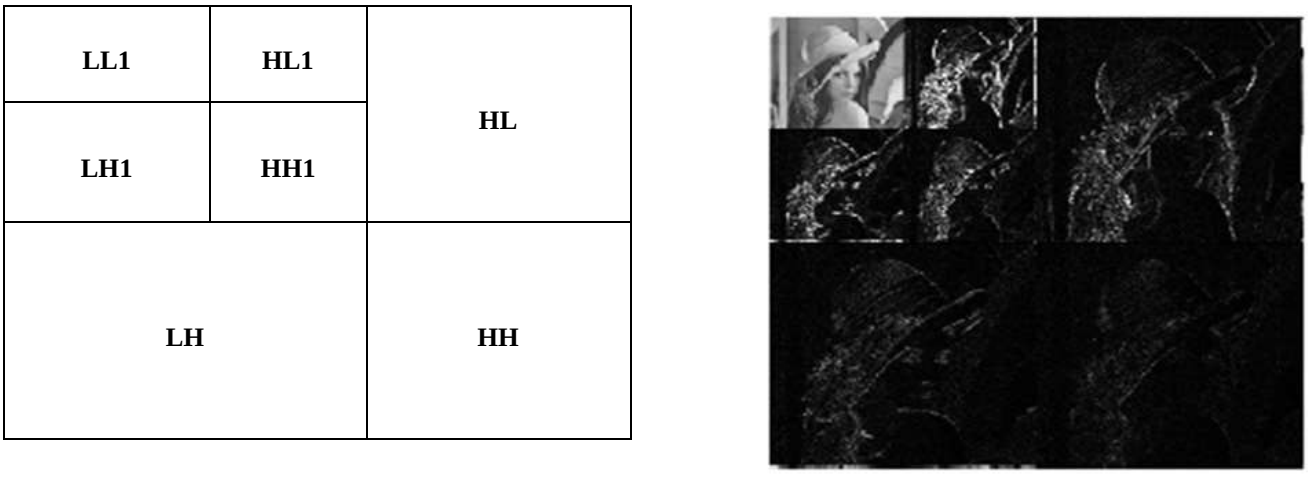

Fig: 2: Original image decomposed by 2-level Integer Wavelet Transform

Intensity histogram of the wavelet coefficient in LL1 band is calculated and segmented into 'k' non-overlapping bins of Θ interval. The ith binΘ I contains pixel intensity in the range of [(i− 1) ∗ Θ:i∗Θ]. The number of pixels (ni).In Θi bin is evaluated and concatenated to give a string N expressed as[8]

$$N= [n1,n2,n3\ldots nk] \quad (5)$$

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

$$Wp = [Wp1Wp2Wp3\ldots Wp\theta] ,Wpi\varepsilon[1,0] \quad (6)$$

Where Θ =k∗b. To reduce false detection during extraction of the watermark, this pre-watermark sequence is spread using two orthogonal code word of length 'L'as

$$Wpi \text{ --- -> } \hat{v}1 \ \Xi \ [v1v2v3\ldots vL] \ \text{ if } \ Wpi = 0$$

$$Wpi \text{ --- -> } \hat{v}2 \ \Xi \ [v1v2v3\ldots vL] \ \text{ if } \ Wpi = 1 \quad ..(7)$$

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

$$W = [\hat{w}1 \ \hat{w}2 \ \hat{w}3..... \ \hat{w}\theta]$$

$$\text{Where } \hat{w}i = \hat{v}1 ,Wpi = 0$$

$$\hat{w}i= \hat{v}2 , Wpi = 1 \quad (8)$$

In order to have blind self-authentication capability, histogram values of LL1 band before and after watermarking should be unchanged [15]. 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 Θiis 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...3

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[6].

B. .*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':

$$[C' \ xy \ \alpha \ ] = \min (abs (Cxy- \Psi 1\mu)) \ \mu=1, 2, \cdots 9 \quad .(9)$$

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

Where 'α'is the value of μfor 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[7]:

For '1':

$$[C' \ xy \ \beta \ ] = \min (abs (Cxy- \Psi 2\mu)) \ \mu=1,2,\cdots 9.. \quad .(10)$$

$$C' \ xy = \Psi 2 \ \beta$$

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

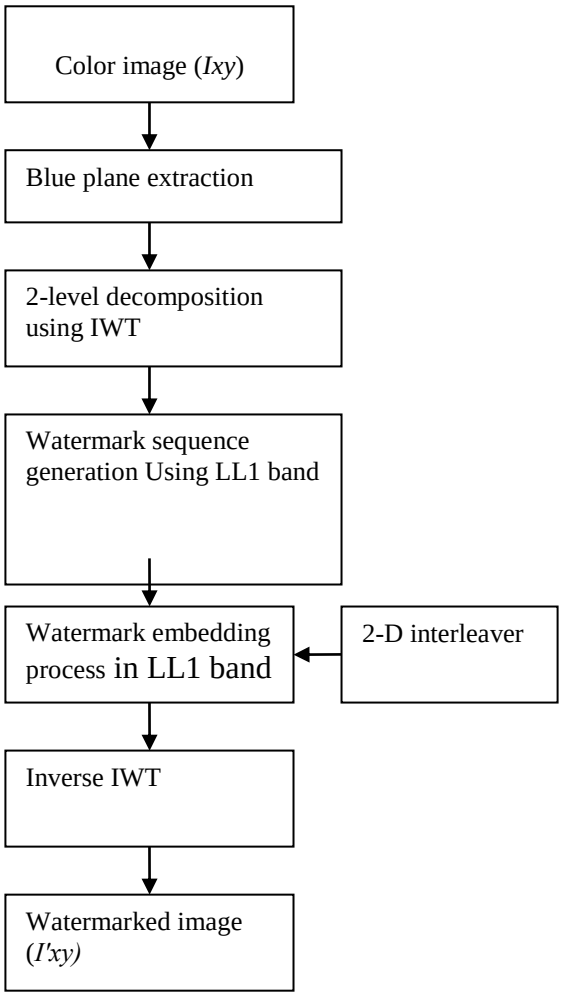

Fig.3: Block diagram for watermark Embedder

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

IV. EXPERIMENTAL RESULTS

To prove the robustness of algorithm for common signal processing attacks, by applying attacks like rotation, scaling, noise addition, cropping, median filtering, and compression on the watermarked image. This attacked image is applied to the extraction algorithm and performance metrics are evaluated to study the robustness of watermarking scheme. Performance matrix measurements contain Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), Similarity Index Measurement (SIM), Correlation Coefficient χ (CC) and Bit Correction Rate (BCR). In this Papert the proposed algorithm is efficiently implemented in MATLAB

A. *Simulation Results Without Attack*

Watermark sequence of length 560 is embedded in the original colour image and the difference image and watermarked image is obtained. Fig.4 show 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:4. Original Image

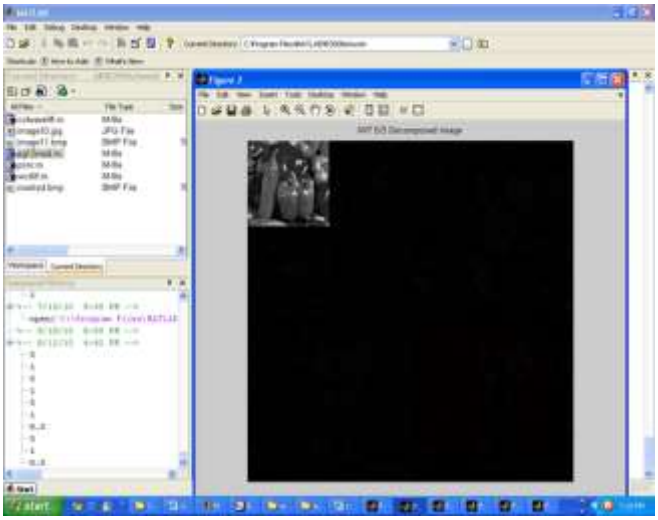

Fig: 5. Decomposed Image

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

Fig: 6: 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. Observing figures 5.2(c) and 5.2(d), there is no degradation in the perceptual quality.

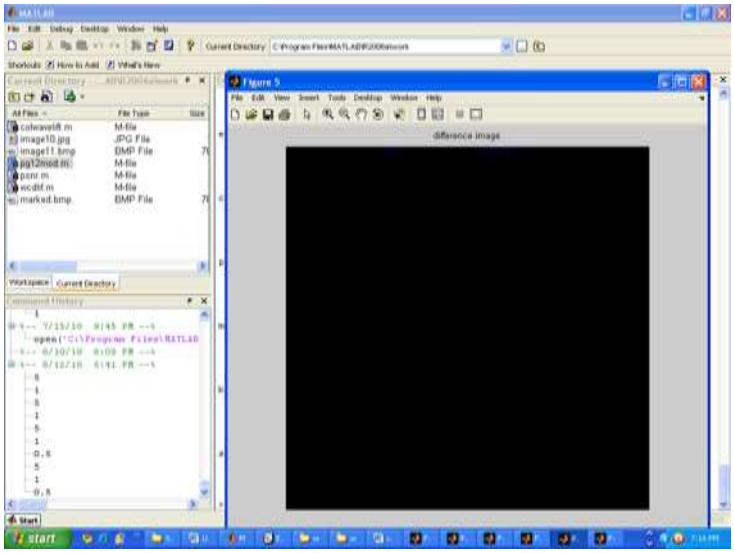

Fig::7 .Difference image

The difference image is absolute difference of the pixel intensities of the watermarked image and the original image.

B. *Attacks On Watermarked Images*

NOISE ADDITION

The watermarked images are added with a scaled Gaussian noise of zero mean and different variances and salt and pepper noise with different densities. After attacking the image with these noise additions we can apply the attacked image to the extraction algorithm

GAUSSIAN NOISE

Histogram values before embedding watermark, watermarked image, Image after adding noise of '0.005' variance and recovered Histogram values are shown in Fig

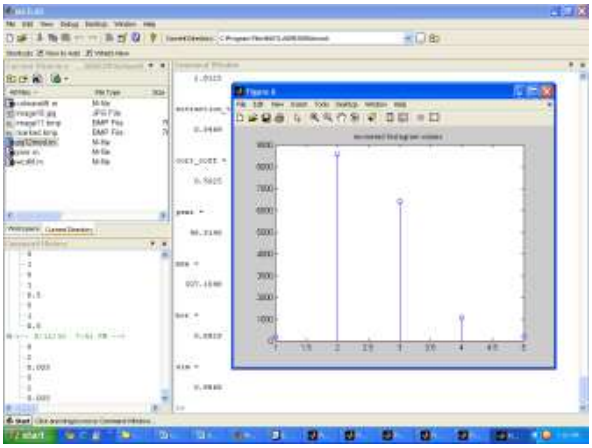

Fig::8

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

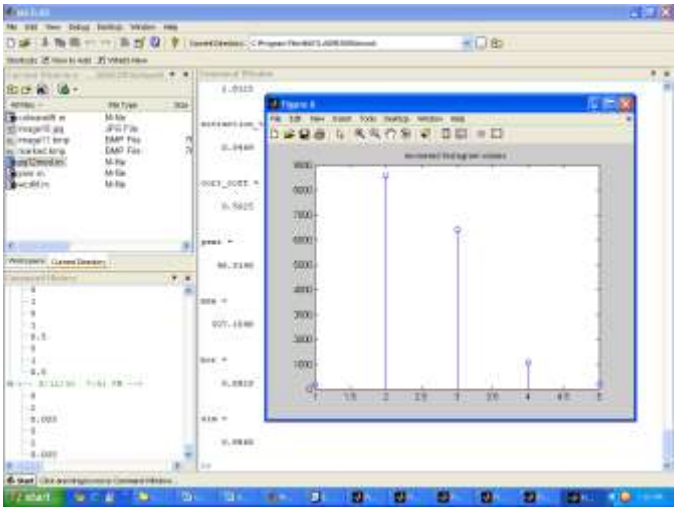

Fig::9

Figure: 9 shows the graphical representation of histogram values of LL1 band of watermarked image after embedding watermark.

Observing figures 8 and 9, histogram values before embedding and after extraction from watermarked image are same. Hence self-authentication property is achieved.

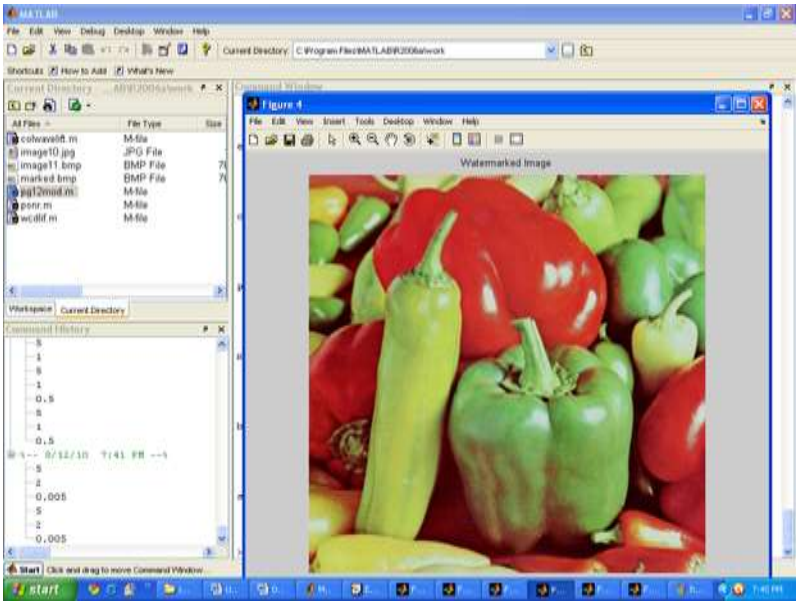

Fig: 10.Watermarked image

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.11: Gaussian noise attacked image

Image after adding the noise of 0.005 variance is shown in figure.11

. Performance metrics of watermarked Image corrupted with Gaussian noise of zero mean and varying the variance of the noise is shown in Table.2

Table 2. Performance metrics for Gaussian noise attack

Gaussian noise Variance	χ	PSNR (dB)	MSE	BCR	SIM
0.001	0.562	59.80	66.50	0.891	0.997

0.002	0.602	54.10	128.16	0.903	0.994
0.003	0.602	54.10	188.45	0.9036	0.992
0.004	0.518	48.40	247.04	0.882	0.984
0.005	0.518	46.48	308.12	0.88214	0.9872

In Similar manner Performance metrics for salt and pepper noise, Compression & rotation attack are given in the Table.3,4&5

Table 3. 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

Table 4: Performance metrics for compression attack

JPEG quality factor	χ	PSNR (dB)	MSE	BCR	SIM
90	1.00	80.11	6.41	1.00	0.999
70	0.591	77.29	8.87	0.90	0.999
50	0.601	60.11	60.27	0.914	0.996
30	0.63	58.27	74.89	0.910	0.997

Table 5: Performance metrics of rotation attack

Rotation (degrees)	X	PSNR (dB)	MSE	BCR	SIM
-0.25	0.99	42.98	461.31	1.00	0.992
-0.5	0.708	42.35	495.76	0.928	0.991
0.25	0.724	42.80	470.3	0.934	0.992
0.5	0.67	41.89	522.75	0.921	0.991
1	0.577	36.29	926.92	0.896	0.984

Results are presented with colour images and the statistical analysis of the proposed method and the previous method is shown. The proposed scheme has been tested for different colour images which show much higher robustness as compared to the Liu scheme . It shows that this technique can be used for both robust watermarking of the images with blind self-authentication.

V. CONCLUSION

In this Paper, 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]. 1. S.P. Mohanty ; N. Ranganathan ; R.K. Namballa ; A VLSI architecture for visible watermarking in a secure still digital camera (S/sup 2/DC) design (Corrected)*

[2]. Ehsan Nezhadarya ; Z. Jane Wang ; Rabab Kreidieh Ward ; Robust Image Watermarking Based on Multiscale Gradient Direction Quantization.

[3]. Jian Cao ; Jiwu Huang ; Controllable Secure Watermarking Technique for Tradeoff Between Robustness and Security.

[4]. Yasunori Ishikawa ; Kazutake Uehira ; Kazuhisa Yanaka ; Optimization of Size of Pixel Blocks for Orthogonal Transform in Optical Watermarking Technique.

[5]. Yu-Hsun Lin ; Ja-Ling Wu ; A Digital Blind Watermarking for Depth-Image-Based Rendering 3D Images.

[6]. Hua Yuan ; Xiao-ping Zhang ; A Secret Key Based Multiscale Fragile Watermark in the Wavelet Domain.

[7]. Ming Chen ; Zhenyong Chen ; Xiao Zeng ; Zhang Xiong ; Model Order Selection in Reversible Image Watermarking.

[8]. Zhe-Ming Lu ; Dian-Guo Xu ; Sheng-He Sun ; Multipurpose image watermarking algorithm based on multistage vector quantization.

[9]. Xinbo Gao ; Cheng Deng ; Xuelong Li ; Dacheng Tao ; Geometric Distortion Insensitive Image Watermarking in Affine Covariant Regions.