An Improved Image Watermarking based on LPM and AQIM

Somanath Chikane
Department of Electronics and Telecommunication Engineering
PG Student, ICOER, Pune, India

Sukhwinder K. Bhatia
PhD Research Scholar
IKGPTU Jalandhar
JSPM, ICOER, Pune, India

Rajneesh Talwar
Principal, CGC Group of Colleges
Jhanjeri, Punjab

ABSTRACT
Watermarking refers to the hiding of a message in a host message in such a way that if this signal is altered; the hidden message still survives if the host survives. Watermarking used for covert communication, Authentication, broadcast monitoring, tamper proofing, etc. This paper proposes an improved image watermarking scheme based on log polar mapping (LPM) and angle quantization index modulation (AQIM).To keep the watermark robust to translation, rotation and scaling attacks, Log Polar mapping followed by Fast Fourier transform is performed on the original unwater marked image before embedding the watermark. Using AQIM, the watermark is embedded in the gradient vectors of large magnitudes by quantizing the angle. Gradient vectors are obtained in the form of Discrete Wavelet Transform (DWT) coefficients. To makes the watermark robust to amplitude scaling attacks, this method Embeds watermark in the vector angle. Imperceptibility is increased by embedding watermark in the gradient vectors with large magnitudes. Increase in the watermarking capacity, is achieved by employing multiple levels DWT.

Keywords
LPM, AQIM, DWT, DCT

1. INTRODUCTION
With the use of internet and other multimedia technology, fast and inexpensive transmission of digital data became possible. This result an unauthorized copying and distribution of data. This yields loss of credits of owners. To avoid this Use some encryption algorithm. But this is not proper solution. This encrypted data can be decrypted easily and can be freely distributed or manipulated. So solution to this is only Digital Watermarking. Digital watermarking is a technique for inserting ownership information to the digital data to prove the authenticity, tamper proofing, broadcast monitoring, covert communication etc. Digital watermark is of two types visible and invisible but invisible watermark is preferred since it does not cause perceptual degradation of host signal. Another requirement of watermark is that it should be robust against attacks. That is it should survive signal processing operations and counterfeit attempts. A high watermarking capacity is also another major requirement. In other words it should carry as many bits of information as possible. Watermark embedding methods are generally classified into spread spectrum (SS) based watermarking and quantization based watermarking. In spread spectrum based watermarking the marked signal is obtained by an additive modification. They are modestly robust, but have a low information capacity. In quantization based watermarking a set of features extracted from the host signal are quantized such that each watermark bit is represented by a quantized feature value. They have a high information capacity and also have low robustness to amplitude scaling attacks, geometric attack. Amplitude scaling attacks is nothing but that affect the amplitude or magnitude of image. This paper proposes a log polar mapping and quantization based watermarking, that exhibits greater robustness to different attacks, have high watermarking capacity and increased imperceptibility. In this method, watermark is embedded by quantizing the angle of gradient vectors having large magnitudes.

2. LITERATURE REVIEW
There are generally two types of Watermark embedding techniques and these are spread spectrum (SS) based watermarking and quantization based watermarking. In spread spectrum based watermarking the marked signal is obtained by an additive modification like by adding pseudorandom noise-like watermark into the host signal. They are modestly robust, but also have a low information capacity. In quantization based watermarking a set of features extracted from the host signal are quantized so that each watermark bit is represented by a quantized feature value. Also they have a high information capacity and have low robustness. I.J Cox et al. proposed a spread spectrum technique for watermarking, based on Discrete Cosine Transform (DCT) [1]. According to this method, to make the watermark robust, watermark is embedded in the most significant component of the image instead of least significant component. This yield more robust watermark since most of the signal processing operations tends to leave perceptually significant components unaffected. However Original unwatermarked image is required for the detection of the watermark and there is no way to distinguish whether the unwatermarked image available for decoding is the original unwatermarked image or the one obtained after removing the counterfeiter's watermark from the original image. Wang et al. proposed a wavelet based watermarking algorithm [4]. Here watermark is embedded into the middle frequency band. In this technique watermark is embeded into the middle frequency component so perceptual invisibility and robustness to compression is achieved. This scheme does not require original unwatermarked image for detecting the watermark. But random nature of the watermark helps in identifying the secret wavelet band and eventually one can remove the watermarking signal from that band. Kundur and Hatzinakos proposed a quantization based fragile watermarking approach for tamper proofing [5]. Here watermark is embedded in discrete wavelet domain of the image by quantizing the corresponding coefficient. Embedding watermark in discrete wavelet domain allows the detection of changes in image in localized spatial and frequency domain regions thereby helps to characterize signal modification like filtering, substitution of data and lossy compression. In addition, quantizing the coefficient to a pre-specified degree provides the flexibility to make tamper proofing technique as

sensitive to changes in the signal as desired. But this scheme fails to provide robustness to geometric attacks. Chen and Wornell introduced quantization index modulation (QIM) as a new class of data hiding [6]. This method embeds signal dependent watermark using quantization techniques. In this method amplitude of a single pixel or a vector of pixels are quantized. This scheme exhibits a larger watermarking capacity than spread spectrum techniques. But this scheme is fragile to even simplest attacks like amplitude scaling attacks. Gonzalez and Balado proposed a quantized projection method that combines quantization index modulation and spread spectrum technique [7].This method is based in quantizing a diversity projection of the host signal inspired in the statistics used for detection in spread spectrum algorithms. Even though this method helped to mitigate the effects of attacks it turned out to be suboptimal in terms of capacity. Ourique et al. proposed angle quantization index modulation where only the angle of a vector of image features is quantized instead of quantizing the amplitude of pixel values [8]. Embedding the watermark in the vectors angle makes the watermark robust to changes in the vector magnitude such as amplitude scaling attacks. But this method fails to show robustness against geometric attacks.

3. PROPOSED METHOD

An improved robust image watermarking using log polar mapping and angle quantization index modulation (AQIM) has been proposed. Using AQIM, watermark is embedded by quantizing the angle of gradient vectors with large significant gradient vectors. Embedding watermark in the vector angle of significant gradient vectors makes the watermark robust to changes in the vector magnitude such as amplitude scaling attacks. To make the watermark robust to rotation, translation and scaling attacks, Fast Fourier transform (FFT) followed by Log Polar mapping (LPM) is performed on the original unwatermarked image before embedding the watermark. LPM maps the image from Cartesian coordinates system to log polar coordinate system and since it is invariant to rotation and scaling, applying LPM will make the watermark robust to rotation and scaling attacks. FFT transforms the image from spatial domain to frequency domain and since it is invariant to translation, applying FFT will make the watermark robust to translation attacks. To keep the watermark imperceptible and to enhance the robustness, it is embedded in the gradient vectors having large magnitude. This is because the gradient vectors with large magnitude characterize the edges and textured regions in an image. The human visual system (HVS) is less sensitive to any changes to it. So watermark embedded in this area are highly invisible and also most of the signal processing operations tend to leave these areas thereby increasing the robustness of the watermark. Gradient vectors are obtained in terms of discrete wavelet transform (DWT). Thus the gradient vector at each pixel is first obtained in terms of the DWT coefficients. Then watermark is embedded by modifying the DWT coefficients corresponding to the gradient vectors. To increase the watermarking capacity, DWT is applied at multiple levels and at each level, watermark is embedded to gradient vectors with large magnitudes.

3.1 Angle Quantization Index Modulation (AQIM)

AQIM is an extension of the quantization index modulation (QIM) method.

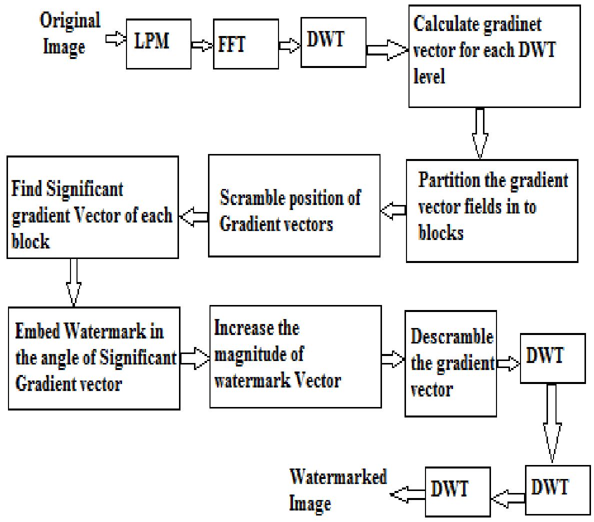


Fig1. Proposed Embedding Method

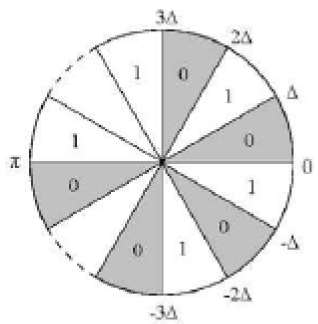
The quantization function, denoted by(θ) , maps a real angle θ to a binary number as follows:

$$Q(\theta) = \begin{cases} 0 & \text{if } \left\lfloor \frac{\theta}{\Delta} \right\rfloor \text{ is even} \\ 1 & \text{if } \left\lfloor \frac{\theta}{\Delta} \right\rfloor \text{ is odd} \end{cases}$$

Where the positive real number Δ represents the angular quantization step size and $\left\lfloor \frac{\theta}{\Delta} \right\rfloor$denotes the floor function, where the following rules are used to embed a watermark bit into an angle θ:

- If $Q(\theta) = \omega$, then θ takes the value of the angle at the centre of the sector it lies in.
- If $Q(\theta) \neq \omega$, then θ takes the value of the angle at the centre of one of the two adjacent sectors, whichever is closer to these rules can be expressed as

$$\theta^{w} = \begin{cases} \Delta\left\lfloor \frac{\theta}{\Delta} \right\rfloor - \frac{\Delta}{2}, if\ Q(\theta) = \omega \\ \Delta\left\lfloor \frac{\theta}{\Delta} \right\rfloor + \frac{\Delta}{2}, if\ Q(\theta) \neq \omega\ and\ \theta > \Delta\left\lfloor \frac{\theta}{\Delta} \right\rfloor - \frac{\Delta}{2} \\ \Delta\left\lfloor \frac{\theta}{\Delta} \right\rfloor - \frac{\Delta}{2}, if\ Q(\theta) \neq \omega\ and\ \theta \leq \Delta\left\lfloor \frac{\theta}{\Delta} \right\rfloor - \frac{\Delta}{2} \end{cases}$$



The angle quantization circle with a fixed quantization step Δ.

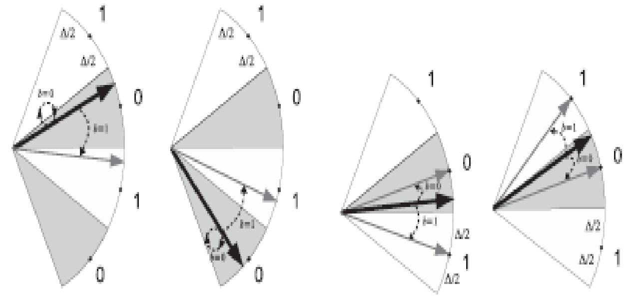


Fig 2: Illustration of AQIM rule

Illustration of different angle quantization watermarking methods: (a) AQWM and (b) AQIM. Vectors before and after watermarking are represented by "thick black" and "thin gray" arrows, respectively.

3.2 Watermark Embedding Method

1. Log Polar Mapping (LPM) is applied on to the image to be watermarked. Since LPM is invariant to rotation and scaling applying LPM will make the scheme robust against rotation and scaling attacks
2. Fast Fourier Transform (FFT) is applied the output of LPM. Since FFT is translation invariant applying FFT on the image will make the watermark robust against translation attack.
3. Employ 2D-DWT (Discrete Wavelet Transform) to estimate the gradient vectors at different levels.
4. At each level, we obtain the gradient vectors in terms of the horizontal, vertical, and diagonal discrete wavelet coefficients
5. To embed the bits of the watermark, the gradient field is partitioned into blocks. The number of blocks depends on the number of bits to be embedded.
6. Thus, bits can be embedded in the gradient field corresponding to more than one level.
7. The positions of the gradient vectors are uniformly scrambled at each scale.
8. The watermark bits are inserted into the significant gradient vectors of each block. Significant gradient vectors are gradient vectors with large magnitude.

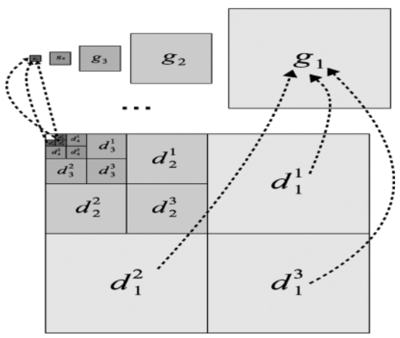


Fig.3: Illustration of five-level gradient field, obtained from five- level wavelet decomposition.

At level j and pixel position n, the gradient vector g can from the 2-D DWT coefficients of LH, HL, and HH sub bands as be obtained

$$g_j[n] = \frac{d_j^1[n]+d_j^3[n]}{2} + i\ \frac{d_j^2[n] - d_j^3[n]}{2}$$

Thus, the direction θj[n] and the magnitude rj[n] of the gradient vector can be expressed as

$$\tan(\theta_j[n]) = \left(\frac{d_j^2[n] - d_j^3[n]}{d_j^1[n]\ +\ d_j^3[n]}\right)$$

$$r_j[n] = \frac{1}{2}\sqrt{\left(d_j^1[n] + d_j^3[n]\right)^2 + \left(d_j^2[n]\ -\ d_j^3[n]\right)^2}$$

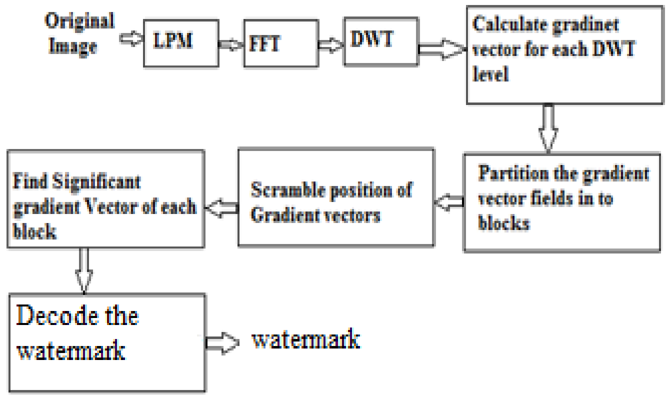


Fig.4: Proposed decoding method

9. Scrambling is used to ensure that each block contains at least one significant gradient vector.
10. The significant gradient vectors of each block are calculated.
11. In each block, one bit of the watermark is embedded in the angle of the most significant gradient vectors, using angle quantization index modulation (AQIM).
12. The watermarked gradient fields at each scale are descrambled, using the descrambling method. By using the periodicity property of the transform, the original image can be recovered from the scrambled image
13. The watermarked wavelet coefficients are obtained from the watermarked gradient vector
14. Inverse wavelet transform is applied on the watermarked wavelet coefficients.
15. Then inverse FFT is applied and finally, the watermarked image is obtained after applying the inverse LPM.

3.3 Watermark decoding method

The watermark bits are decoded using the reverse encoding steps. At the transmitter side, each watermark bit is embedded into the most significant gradient vectors of each block. At the receiver side, we decode the watermark bit of the most significant gradient vectors. Preference given to the watermark bit extracted from a large gradient vector must be more than that given to a watermark bit extracted from a small vector.

3.4 Scrambling and descrambling method

Scrambling method should be a geometric transform that uniformly distributes the position of gradient vectors. There are so many scrambling methods have been proposed. Among those Fibonacci transformation [9], Arnold cat transformation

[10], Gray code transformation [11] are widely used. In this paper Arnold Cat map is used for scrambling the position of gradient vectors as it is computationally feasible and is as the follows:

Let be an $\begin{bmatrix} x \\ y \end{bmatrix}$ n x n matrix, the Arnold Cat Map transformation is given by

$$\Gamma: \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod n :$$

i.e. $\Gamma: x, y \rightarrow x + y, x + 2y \bmod n$

After several iteration of this map, the iterated images eventually return to the original image.

4. SIMULATION RESULTS

To evaluate the performance of the proposed method, take gray-scale test images "Peppers," "Baboon," "Barbara," and "Lena." All test images are of size 512 X 512, a 256 bit "cameraman" as watermark is embedded in the gradient fields at multiple levels where 128 bits are embedded in level 1, 64 bits in level 2 and remaining 64 bits in level 3. The gradient field at each level is divided into blocks where size of the block depends on the number of bits to be embedded in that block. For embedding 64,32,32 bits in level 1,2 and 3 block size of 8×8, 4×8 and 2×4 is used.

4.1 Comparison between Single-Scale GDWM and Multiscale GDWM

To increase the watermark capacity embeds the watermark at multiple scales. To compare the single-scale version with the multiscale version, we average the results of embedding 256-bit pseudorandom binary watermarks in the images Peppers, Baboon, and Lena. To simulate the single-scale GDWM (SSGDWM), all 256 bits are embedded at wavelet scale 1, using blocks of size 4 X 4. In the multiscale GDWM (MS GDWM i.e. LPM & AQIM), we embed 128, 64, and 64 bits at wavelet levels 1, 2, and 3, respectively. The BER (%) results of the proposed SSGDWM and proposed methods, under different types of attacks are shown in Table I.

4.2 Performance comparison of LPM & AQIM method with DWT

To evaluate the performance of the proposed method, we embed binary watermarks image of Cameraman of size 256 in the gray-scale test images "Peppers," "Baboon," "Barbara," and "Lena." All test images are of size 512 X 512.

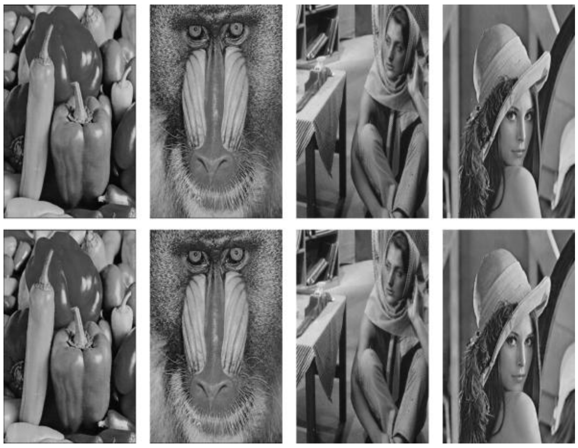


Fig 5: (Upper row) Original test images "Peppers," "Baboon," "Barbara," and "Lena." (Lower row)Watermarked test images using the proposed LPM & AQIM method, with a 256-bit watermark embedded

4.3 Robustness To Attacks

To evaluate the robustness of the proposed scheme, each watermarked image is distorted by Gaussian filtering, median filtering, Scaling, Gaussian noise, salt & pepper noise, and rotation. After the attacks, each watermark is extracted and is compared with the original watermark in terms of BER. The BER (%) results of the proposed DWT and Proposed methods, under different types of attacks are shown in Table II.

4.3.1 Robustness against Amplitude Scaling Attack:

The BER results of the SSGDWM and Proposed schemes under amplitude scaling attacks are shown in Table I and DWT and Proposed method are shown in table-II. It can be seen that the proposed methods are very robust to this attack. This is due to embedding the watermark in the angles of the gradient vectors

4.3.2 Robustness against Gaussian Filtering:

The watermarked mage is filtered by Gaussian filters with different standard deviations and filter lengths. Table I and II shows the BER results of test images attacked by Gaussian filters with size W x W, where W ε {3, 5}. As expected, since the Gaussian filter changes only the magnitude of the gradient vectors, the proposed method is robust to this attack.

Table-I. PSNR (dB) &.BER (%) Results of SSGDMand LPM

Image	Method	Parameter	Without Attack Extraction	Amplitude Scale=2	Gaussian Filter		Rotation		Salt & Pepper Noise	Cropping
					3 x 3	5 x 5	-0.5	0.5		
Peppers	SSGDWM	PSNR	66.7725	58.4111	61.8991	61.7017	52.0533	52.5518	61.7017	66.7725
		MSE	0.013672	0.09375	0.041992	0.043945	0.40527	0.36133	0.043945	0.013672
	LPM & AQIM	PSNR	66.7725	58.4111	61.8991	61.7017	52.0533	52.5518	61.5128	66.7725
		MSE	0.013672	0.09375	0.041992	0.043945	0.40527	0.36133	0.045898	0.013672
Baboon	SSGDWM	PSNR	66.4729	58.6434	60.7519	60.5995	51.8191	52.022	61.5128	66.4729
		MSE	0.014648	0.088867	0.054688	0.056641	0.42773	0.4082	0.045898	0.014648
	LPM & AQIM	PSNR	66.4729	58.6434	60.7519	60.5995	51.8191	52.022	61.7017	66.4729
		MSE	0.014648	0.088867	0.054688	0.056641	0.42773	0.4082	0.043945	0.014648
Barbara	SSGDWM	PSNR	67.8199	58.1906	61.8991	61.7017	51.879	52.3792	62.106	67.8199
		MSE	0.010742	0.098633	0.041992	0.043945	0.42188	0.37598	0.040039	0.010742
	LPM & AQIM	PSNR	67.8199	58.1906	67.8199	67.8199	51.879	52.3792	61.6062	67.8199
		MSE	0.010742	0.098633	0.010742	0.010742	0.42188	0.37598	0.044922	0.010742
Lena	SSGDWM	PSNR	67.0944	58.0219	61.5128	61.3318	51.7502	52.7561	61.4214	67.0944
		MSE	0.012695	0.10254	0.045898	0.047852	0.43457	0.34473	0.046875	0.012695
	LPM & AQIM	PSNR	67.0944	57.8996	67.0944	67.0944	51.8092	52.4704	61.5128	67.0944
		MSE	0.012695	0.10547	0.012695	0.012695	0.42871	0.36816	0.045898	0.012695

Table-II. PSNR (dB) &.BER (%) Results of DWT and LPM & AQIM under different types of attack

Image	Method	Parameter	Extraction Without Attack	Amplitude Scale=2	Gaussian Filter		Rotation Attack		Salt & Pepper Noise	Cropping Attack
					3 x 3	5 x 5	-0.5	0.5		
Peppers	DWT	PSNR	13.913	13.913	13.9126	13.9126	13.3693	13.3459	13.9151	11.328
		MSE	15.8867	15.8867	15.8874	15.8874	16.7744	16.8137	15.8834	20.5732
	LPM & AQIM	PSNR	66.7725	58.4111	61.8991	61.7017	52.0533	52.5518	61.5128	66.7725
		MSE	0.013672	0.09375	0.041992	0.043945	0.40527	0.36133	0.0459	0.013672
Baboon	DWT	PSNR	13.913	13.913	13.9126	13.9126	13.1645	13.1654	13.8848	12.1524
		MSE	15.8867	15.8867	15.8875	15.8875	17.1214	17.12	15.9317	18.9452
	LPM & AQIM	PSNR	66.4729	58.6434	60.7519	60.5995	51.8191	52.022	61.7017	66.4729
		MSE	0.014648	0.088867	0.054688	0.056641	0.42773	0.4082	0.04395	0.014648
Barbara	DWT	PSNR	13.913	13.3398	13.9126	13.9126	13.3649	13.3398	13.9154	12.2117
		MSE	15.8867	16.8241	15.8874	15.8875	16.7818	16.8241	15.8829	18.833
	LPM & AQIM	PSNR	67.8199	58.1906	67.8199	67.8199	51.879	52.3792	61.6062	67.8199
		MSE	0.010742	0.098633	0.010742	0.010742	0.42188	0.37598	0.04492	0.010742
Lena	DWT	PSNR	13.913	13.913	13.9126	13.9126	13.4476	13.4305	13.9254	11.7904
		MSE	15.8867	15.8867	15.8874	15.8874	16.6435	16.6721	15.867	19.6434
	LPM & AQIM	PSNR	67.099	57.8996	67.0944	67.0944	51.8092	52.4704	61.5128	67.0944
		MSE	0.010742	0.10547	0.012695	0.012695	0.42871	0.36816	0.0459	0.012695

4.3.3 Robustness against Rotation Attack

The rotation attack is a practical but challenging attack for blind watermarking. Due to the bit-ordering errors in the watermarked image before and after rotation, even a small image rotation could significantly increase the BERs of the extracted watermark bits. Table I & II shows the BER results of SSGDWM and MSGDWM under rotation attacks, where each test image is rotated by + 0.5° & -0.5° It is noted that the proposed methods show robustness to rotation (and translation) attacks. This is because the conventional wavelet transform is invariant to rotation (and translation).

4.3.4 Robustness against Salt & Pepper Noise:

Salt & pepper noise is the most commonly used long-tailed noise in image processing. Since such noise is not additive, it is hard to remove without incurring changes to the image itself. Table I & II shows the BER results when salt & pepper noise is added to the watermarked images, with probability 0.08

4.3.5 Robustness against Cropping Attack:

Cropping is the most commonly used long-tailed noise in image processing. Table I and II shows the BER results of test images attacked by Cropping. The proposed method is robust to this attack.

5. CONCLUSION

This method embeds the watermark at multiple scale in the direction (angle) of significant gradient vectors. To embed the watermark in the gradient direction, this method find the gradient vector in terms of the wavelet coefficients in sub bands LH, HL, and HH. The gradient angle is then quantized by modifying the DWT coefficients that correspond to the gradient vector. To embed the watermark in each gradient angle, LPM and AQIM is used. To extract the watermark correctly and identify the gradient vectors that were watermarked and the embedding order; this method propose scrambling the positions of the gradient vectors uniformly over the wavelet transform of the image. In this method, the PSNR values are increased drastically as compared to DWT shown in table-I & Table- II.

6. REFERENCES

[1] J. Cox, J. Kilian, F.T. Leighton, and T.Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Trans. Image Process., vol.6, no.12, pp.1673-1687, Dec.1997.

[2] Ramkumar, M., Akansu, A.N., Alatan, A.A., "A Robust Data Hiding Scheme For Digital Images Using DFT", in IEEE ICIP, vol 2, pp 211-215, October 99.

[3] Y. Wang, J. F. Doherty, and R. E. Van Dyck, "A wavelet-based watermarking algorithm for ownership verification of digital images," IEEE Trans. Image Process., vol. 11, no. 2, pp. 77-88,

[4] Lin, C-Y, Wu, M, Bloom, JA, Cox, IJ, Miller, ML & Lui, YM 2001, "Rotation, Scale and Translation Resilient Watermarking for Images", IEEE Transactions on Image Processing, vol. 10, no. 5, pp. 767-782. Feb. 2002.

[5] D. Kundur and D. Hatzinakos, "Digital watermarking for telltale tamper proofing and authentication," Proc. IEEE, vol. 87, no. 7, pp. 1167-1180, Jul. 1999.

[6] B. Chen and G.W. Wornell,"Quantization index modulation: A class of provably good methods for digital Watermarking and information embedding," IEEE Trans. Inf. Theory, vol. 47, no. 4, pp. 1423-1443, May 2001.

[7] J. Zou, R.K.Ward, and D.Qi, "A new digital image scrambling method based on Fibonacci numbers," in Proc. Int. Symp. Circuits and Syst., May 2004, vol. 3, pp. 965-968.

[8] C. Ming and P. Xi-jian,"Image steganography Based on Arnold transform," Comput. Appl.res, vol 1 pp235-237,2006

[9] J. Zou and R. K. Ward, "Introducing two new image scrambling methods," in IEEE Pacific Rim Conf. Comm.,Comp. and Signal Proces., Aug. 2003, vol 2pp, 708-711.

[10] D. E. Manolakis and J. N. Ellinas, "A robust watermarking scheme based on edge detection and contrast sensitivity function," in *Proc. Int Conf. Comp. Vision Theory and Applications*, Barcelona, Spain, 2007.

[11] F. Ourique, V. Licks, R. Jordan, and F. Perez-Gonzalez, "Angle qim: A novel watermark embedding scheme robust against amplitude scaling distortions," in *Proc. IEEE Int. Conf. Acoust., Speech,and Signal Process*. (ICASSP '05), Mar. 2005, vol. 2, pp. ii/7

[12] Joseph J.K., O. Ruanaidh and Thierry Pun "Rotation, Scale and Translation Invariant Digital Image Watermarking" Centre Universitaire d'Informatique, Universite de Geneve, 24 rue General Dufour, CH-1211 Geneve 4, Switzerland

[13] Lin, C-Y, Wu, M, Bloom, JA, Cox, IJ, Miller, ML & Lui, YM 2001, "Rotation, Scale and Translation Resilient Watermarking for Images", *IEEE Transactions on Image*