An Improved Robust Image Watermarking using Angle Quantization Index Modulation

Athira Madanan, Antara Bhattacharya
Department of Computer Science and Engineering, G.H.R.I.E.T.W, Nagpur, India

Abstract

Digital watermarking is a technique for inserting ownership information to the digital data to prove the authenticity. It is also used for tamper proofing, broadcast monitoring, covert communication etc. This paper proposes a robust image watermarking scheme using angle quantization index modulation (AQIM). Using AQIM, the watermark is embedded by quantizing the angle of gradient vectors with large magnitudes. Gradient vectors are obtained in terms of Discrete Wavelet Transform (DWT) coefficients. Embedding watermark in the vector angle makes the watermark robust to amplitude scaling attacks. To increase the imperceptibility of watermark, watermark is embedded in the gradient vectors with large magnitudes. In order to increase the watermarking capacity multiple level DWT is employed. To keep the watermark robust to translation, rotation and scaling attacks, Fast Fourier transform followed by Log Polar mapping is performed on the original unwatermarked image before embedding the watermark.

1. Introduction

With the advent of internet and other multimedia technology, fast and inexpensive transmission of digital data became possible. This result in unauthorized copying and distribution of digital data that infringe the intellectual property right of the owners. Using some encryption technique to protect the data is a possible solution to the problem. But encryption does not provide over all protection. Once the encrypted data are decrypted they can be freely distributed or manipulated. Digital watermarking has been emerged as an effective solution to the problem. Digital watermarking is a technique for inserting ownership information to the digital data to prove the authenticity. It is also used for tamper proofing, broadcast monitoring, covert communication etc. Digital watermark can be visible 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 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 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. They have a high information capacity but have low robustness to amplitude scaling attacks. Amplitude scaling attacks are those attacks that affect the amplitude or magnitude of image features. This paper proposes a quantization based watermarking that exhibits greater robustness, high watermarking capacity and increased imperceptibility. The method embeds the watermark by quantizing the angle of gradient vectors having large magnitudes using angle quantization index modulation (AQIM).

2. Literature Review

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. That is 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. They have a high information capacity but 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 watermark is embedded in the most significant component of the image instead of least significant component in order to make the watermark robust. Watermark embedded using this method is more robust 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 scheme perceptual invisibility and robustness to compression is achieved by embedding watermark into the middle frequency component. 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

A robust image watermarking using angle quantization index modulation (AQIM) has been proposed. Using AQIM, watermark is embedded by quantizing the angle of gradient vectors with large magnitudes (significant gradient vectors). Embedding watermark in the vector angle 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. FFF 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. 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. 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. Any changes made to these areas are less sensitive to human visual system (HVS). 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 using 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 watermark is embedded to gradient vectors with large magnitudes at each level.

3.1 Angle Quantization Index Modulation (AQIM)

In AQIM [9], every angle θ is assigned a binary number, as follows:

$$Q(|\theta|) = \begin{cases} 0 \ \ if \ \lfloor |\theta| \rfloor \ is \ even \\ 1 \ \ if \ \lfloor |\theta| \rfloor \ is \ odd \end{cases} \qquad (1)$$

where Δ is a positive real number called angular quantization step size and denotes the floor function.

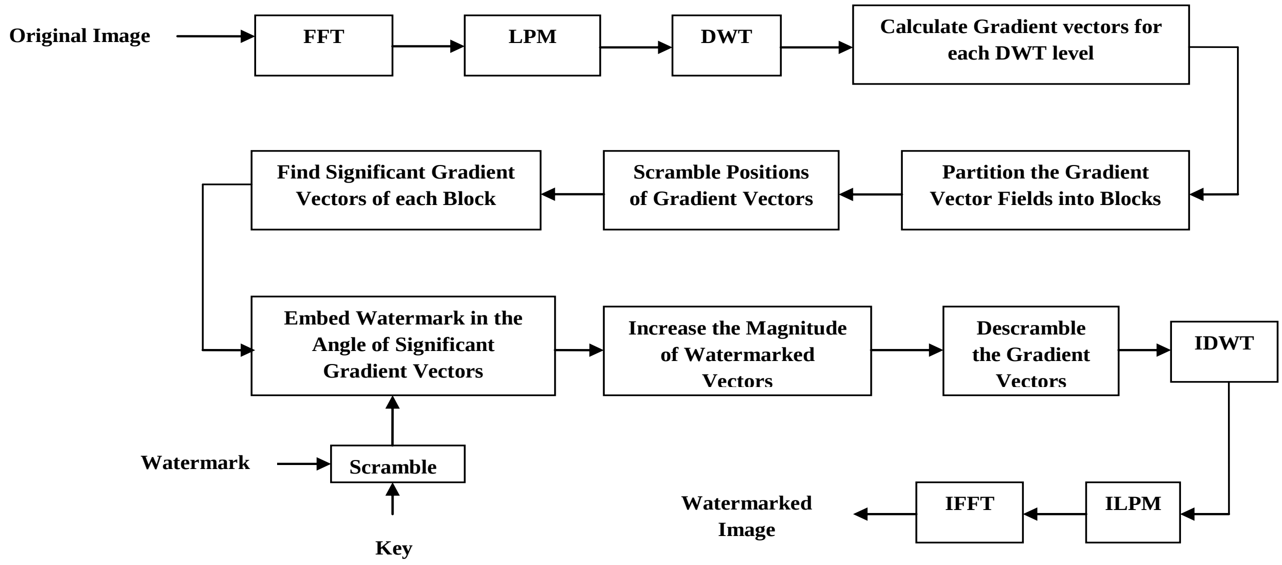

Original Image
FFT
LPM
DWT
Calculate Gradient vectors for each DWT level
Partition the Gradient Vector Fields into Blocks
Scramble Positions of Gradient Vectors
Find Significant Gradient Vectors of each Block
Embed Watermark in the Angle of Significant Gradient Vectors
Increase the Magnitude of Watermarked Vectors
Descramble the Gradient Vectors
IDWT
ILPM
IFFT
Watermarked Image
Watermark
Scramble
Key

Fig. 1. The proposed watermark embedding scheme.

To insert a watermark bit w ∈ {0, 1} in an angle θ, we use the following rules:
1. If Q (θ) = w, then θ takes the value of the angle at the center of the sector it lies in.
2. If Q (θ) ≠w, then θ takes the value of the angle at the center of one of the two adjacent sectors, whichever is closer to θ.
This can be formulated as:

$$|\boldsymbol{\theta}|^{w} =$$

$$\begin{cases} \Delta\left\lceil\frac{|\theta|}{\Delta}\right\rceil-\frac{\Delta}{2} \;\; \boldsymbol{if Q}(|\boldsymbol{\theta}|)=\boldsymbol{w} \\ \Delta\left\lceil\frac{|\theta|}{\Delta}\right\rceil+\frac{\Delta}{2} \;\; \boldsymbol{if\ Q}(|\boldsymbol{\theta}|)\neq \boldsymbol{w\ and} \\ \qquad\qquad \left\{|\boldsymbol{\theta}|>\left(\Delta\left\lceil\frac{|\theta|}{\Delta}\right\rceil-\frac{\Delta}{2}\right) \boldsymbol{or}\ |\boldsymbol{\theta}|\leq\Delta\right\} \\ \Delta\left\lfloor\frac{|\theta|}{\Delta}\right\rfloor-\frac{\Delta}{2} \;\; \boldsymbol{if Q}(|\boldsymbol{\theta}|)\neq \boldsymbol{w\ and} \\ \qquad\qquad \left\{|\boldsymbol{\theta}|\leq\left(\Delta\left\lceil\frac{|\theta|}{\Delta}\right\rceil-\frac{\Delta}{2}\right) \boldsymbol{or}\ |\boldsymbol{\theta}|\geq(\boldsymbol{\pi}-\Delta)\right\} \end{cases} \qquad (2)$$

where w denotes the watermark bit to be embedded (i.e., w=0 or 1). The watermarked angle θ^{w} and the change in the angle $d\theta$ can be obtained as

$$\theta^{w} = |\theta^{w}|\sin(\theta) \qquad (3)$$

$$d\theta = \theta^{w} - \theta \qquad (4)$$

3.2 Watermark Embedding Method

1. Fast Fourier Transform (FFT) is applied to the image to be watermarked. Since FFT is translation invariant applying FFT on the image will make the watermark robust against translation attack.

2. Log Polar Mapping (LPM) is performed on the output of FFT . Since LPM is invariant to rotation and scaling applying LPM will make the scheme robust against rotation and scaling attacks.

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 wavelet coefficients.

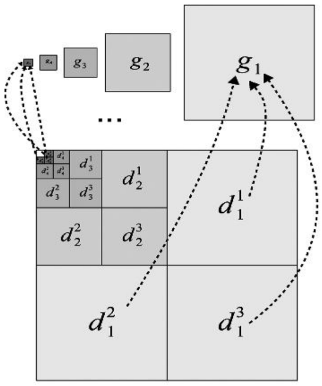


Fig. 2. Illustration of five-level gradient field, obtained from five- level wavelet decomposition where each gradient vector g_j corresponds to the three wavelet coefficients d_j^1, d_j^2, d_j^3

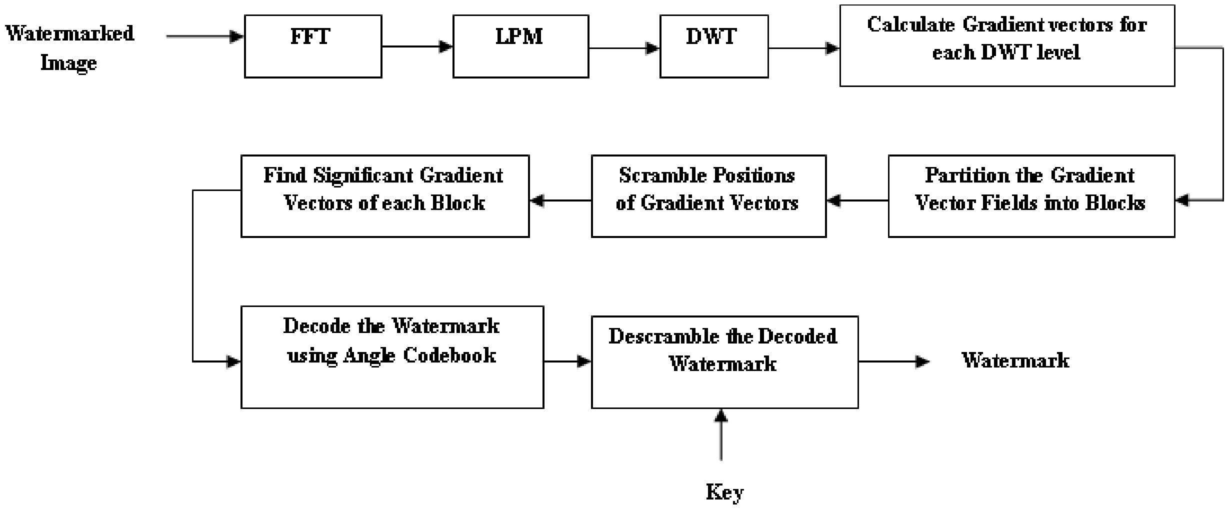

Watermarked Image
FFT
LPM
DWT
Calculate Gradient vectors for each DWT level
Partition the Gradient Vector Fields into Blocks
Scramble Positions of Gradient Vectors
Find Significant Gradient Vectors of each Block
Decode the Watermark using Angle Codebook
Descramble the Decoded Watermark
Watermark
Key

Fig. 3. The proposed watermark decoding scheme

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

$$g_j[n] = \left(\frac{d_j^1[n]+d_j^3[n]}{2}\right) + i\left(\frac{d_j^2[n]-d_j^3[n]}{2}\right) \qquad (5)$$

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

$$\tan(\theta_j[n]) = \left(\frac{d_j^2[n]-d_j^3[n]}{d_j^1[n]+d_j^3[n]}\right) \qquad (6)$$

$$r_j[n] = \frac{1}{2}\sqrt{\left(d_j^1[n]+d_j^3[n]\right)^2 + \left(d_j^2[n]-d_j^3[n]\right)^2} \qquad (7)$$

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. Thus, bits can be embedded in the gradient field corresponding to more than one level.

6. The positions of the gradient vectors are uniformly scrambled at each scale. The watermark bits are inserted into the significant gradient vectors of each block. Significant gradient vectors are gradient vectors with large magnitude. Scrambling is used to ensure that each block contains at least one significant gradient vector.

7. The significant gradient vectors of each block are calculated.

8. For security reasons, the binary watermark message is scrambled using a secret key.

9. 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).

10. The correct detectability of the watermarked gradient vectors is enhanced by increasing their magnitudes relative to the insignificant (unwatermarked) vectors.

11. 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.

12. The watermarked wavelet coefficients are obtained from the watermarked gradient vectors.

13. Inverse wavelet transform is applied on the watermarked wavelet coefficients.

14. Then inverse LPM is applied and finally, the watermarked image is obtained after applying the inverse FFT.

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. Several image 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. Arnold's cat map is defined as the following:

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

$$\Gamma: \begin{bmatrix}x\\y\end{bmatrix} = \begin{bmatrix}1 & 1\\1 & 2\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix} \bmod \mathrm{n} \qquad (8)$$

$$\text{i.e. } \Gamma: (x, y) \rightarrow (x + y, x + 2y) \bmod \mathrm{n} \qquad (9)$$

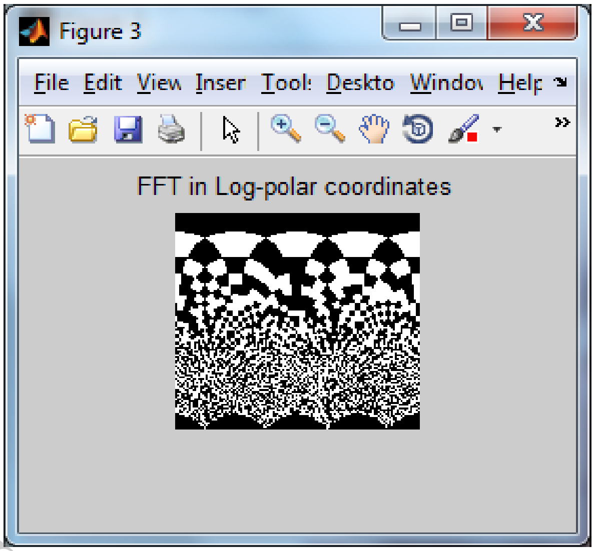
After several iteration of this map, the iterated images eventually return to the original image.

4. Simulation Results

To embed binary watermark in the input image length-10 Symlet wavelet is used. For an input image of size 512×512, a 128 bit watermark is embedded in the gradient fields at multiple levels where 64 bits are embedded in level 3, 32 bits in level 4 and remaining 32 bits in level 5. 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 3,4 and 5 block size of 8×8, 4×8 and 2×4 is used.

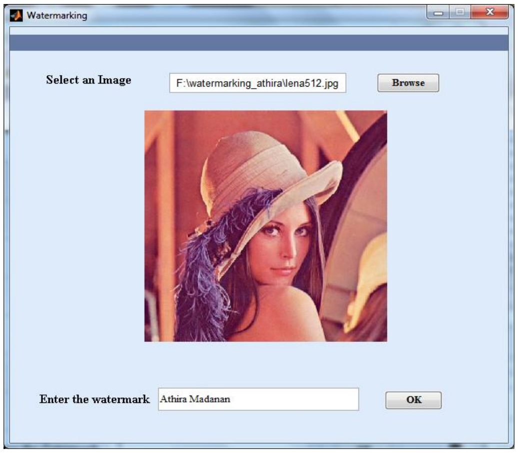
.

Fig. 4. Interface to insert watermark, with "Lena" as input image.



FFT in Log-polar coordinates

Fig. 5. Image after applying Log polar mapping on the Fast Fourier transform of the input image "Lena"



Select an Image F:\watermarking_athira\lena512.jpg

Enter the watermark Athira Madanan

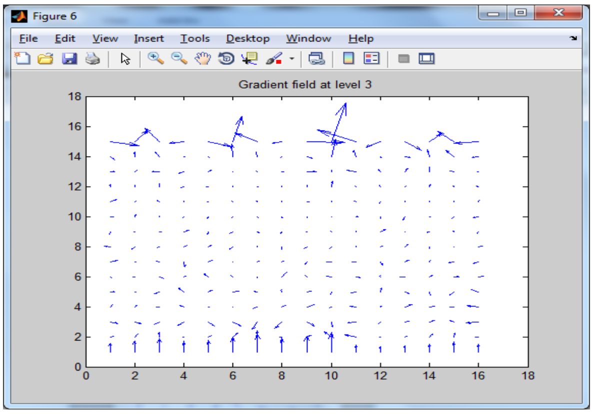


Fig. 6. Gradient field at level 3

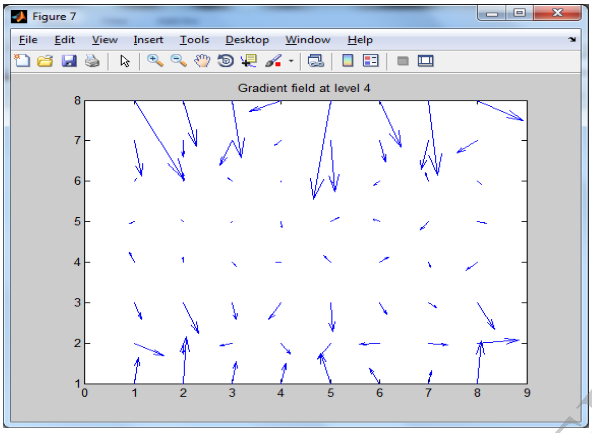


Fig. 7. Gradient field at level 4

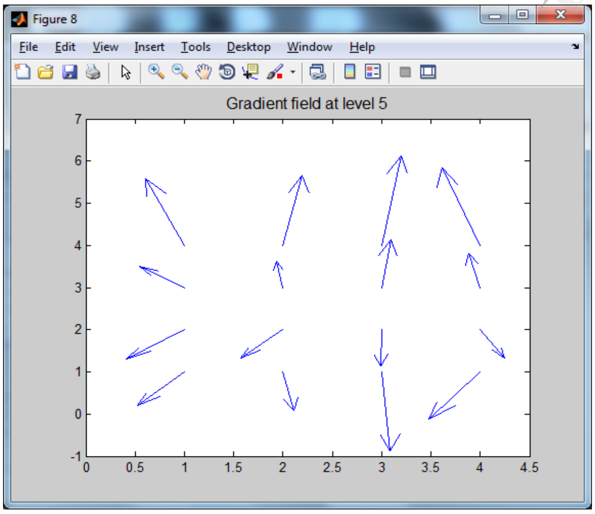


Fig. 8. Gradient field at level 5

5. Conclusion

A robust image watermarking scheme using angle quantization index modulation (AQIM) is been proposed. Using (AQIM) the watermark bits are embedded in the angle of gradient vectors with large magnitudes. To embed the watermark in the vector angle, the gradient vectors in terms of the wavelet coefficients is calculated. The gradient angle is then quantized by modifying the DWT coefficients that correspond to the gradient vector. Embedding watermark in the vector angle makes the watermark robust to amplitude scaling attacks. To increase the imperceptibility of watermark, watermark is embedded in the gradient vectors with large magnitudes. In order to increase the watermarking capacity multiple level DWT is employed. To keep the watermark robust to translation, rotation and scaling attacks, Fast Fourier transform followed by Log Polar mapping is performed on the original unwatermarked image before embedding the watermark. The proposed method yields superior robustness to different types of attacks, with increased imperceptibility of watermark and exhibit a high watermarking capacity.

10. 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] 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.

[4] 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, 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] F. Perez-Gonzlez and F. Balado, “Quantized projection data hiding,” in *Proc. Int. Conf. Image Process.*, 2002, vol. 2, pp. 889–892.

[8] 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

[9] 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.

[10] C. Ming and P. Xi-jian, “Image steganography based on arnold transform,” *Comput. Appl. Res.*, vol. 1, pp. 235–237, 2006.

[11] 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. 2, pp.708–711.