

DIRECTIONAL BASED WATERMARKING SCHEME USING A NOVEL DATA EMBEDDING APPROACH

¹Y. RaghavenderRao, ²Dr.E.Nagabhooshanam, ³P. Nikhil

¹Associate Professor, Department of ECE, JNTUH College of Engineering,
Karimnagar, A.P, India,

Email Id: raghavendery_rao@rediffmail.com

² Prof., Department of ECE, Muffakhamjah College of Engg, Hyderabad, A.P. India,

Email Id:enb1234@rediffmail.com

Abstract:

Image watermarking has come to wide use in the recent past. It is by the authentication problems and limitation means that the setting accuracy of the image watermarking operation is minimized. Different types of integration schemes have been proposed in the past to improve efficiency and makes the embedding resistant against various attacks .Although transformation, spatial domain approaches have been developed PSNR improvements in image artifacts due to the fringes are still to be observed. To improvise the embedding, image artifacts in this paper a forward – based image embedding scheme is proposed.

Keywords:

Watermarking, Wavelet Transform, Directional filter, Attacks.

I. Introduction

With the advent of internet, copying and distribution of digital data has become effortless. This led to raise an issue for the copyright protection of digital data. Digital Watermarking for images, video and other kinds of digital data is the new tool for protection of data from copyright infringement. Here, an imperceptible signal “mark” is embedded into the original image, which signifies the ownership of the latter. After the watermark is embedded, it should be robust and should not be removable by any other person, either intentionally or unintentionally. Different watermarking techniques have already been proposed and are being applied successfully. Overview of watermarking techniques can be seen in [3].

Watermarking techniques are broadly classified into two categories: Spatial domain methods [4],[5] and Transform domain methods [6],[7]. Spatial domain methods have less complexity because we do not use any transform, but these are not robust in nature against attacks. Transform domain techniques of watermarking are highly robust than spatial domain watermarking techniques. This happens because the watermarked image is inverse wavelet transformed, watermark is irregularly over the image and it becomes difficult for the attacker to read or modify the image. When transform domain techniques are considered, DWT based techniques are more popular as DWT is advantageous over some other types of transform like as progressive and low bit-rate transmission, quality scalability and region-of-interest (ROI) coding

demand more efficient and versatile image coding that can be exploited for both, image compression and watermarking applications. The compression standard JPEG2000 is based on the discrete wavelet transform (DWT) to meet the requirements. Therefore, it is imperative to use the wavelet transform domain for most of the applications where watermarking is required. Wavelets are applied successfully to most of the image processing tasks like low bit-rate compression and also De-noising [8]. But they lack the important feature of directionality. So they are inefficient in retaining textures and other details of importance in those applications [3] [4]. Several efforts have been made towards developing geometrical image transforms. Wavelet transforms [1], complex wavelets [6], curve lets [2] and contour-lets [3] are a few examples. Watermarking finds it difficult to use such redundant information as the embedding process needs to be error free so as to achieve accuracy. It is observed that image watermarking is very effective in image embedding at edge regions, which leads to visual artifacts. To avoid the distortion observed in the image, the embedding process based on directional oriented image embedding is proposed. The rest of the paper is defined in 6 sections. Section 2 briefs the approach in watermarking schemes, the approach of directional filter operation and its embedding process is defined in section 3 and 4 respectively. The observation for the developed approach is outlined in section 5. A conclusion is presented in section 6.

II. Image Watermarking

The past decade has seen an explosion in the use and distribution of digital multimedia data. PCs with Internet connections have made the distribution of digital data and applications much easier and faster. However, this has also had a serious effect on copyright encroachment, thereby creating a new demand for copyright protection of digital data [8,9]. To provide copyright protection for digital data, two complementary techniques have been developed: encryption and watermarking. Encryption can be used to protect digital data during the transmission process from the sender to the receiver. However, after the receiver has received and decrypted the data, it becomes identical to the original data and is no longer protected. Watermarking can complement encryption by embedding a secret imperceptible signal, a watermark, into the original data in such a way that it always remains present. Generally digital image watermarking has certain requirements, the most important being robustness and invisibility. Robustness means that the embedded watermarks cannot be removed by intentional or unintentional digital data changing called attacks. Although robustness can be obtained based on significant modifications to the host data, such modifications are noticeable and thus do not satisfy the requirement of invisibility. As such, a tradeoff is needed between the different requirements so that an optimal watermarking can be developed for each type of application. Watermarking is novel method of hiding data and identifying information present in digital multimedia. Watermarking of digital images is our area of interest. Even digital audio, video and documents can also be watermarked, image watermarking has more importance. Digital watermarking has more fame when it comes to the point of adding undetectable marks which involve author or copyright information. So when taken into consideration of all the applications, watermarking techniques are evaluated based on the criterion like invisibility, recoverability and also robustness. In applying watermarks to images, our focus would be on invisibility, recoverability, and robustness of the watermark. All of these are complicatedly linked. The less the image is affected by attacks, the easier it is to confiscate the watermark; recoverability is reliant on robustness, because the watermark must still be existing even after morphological attacks and other external attacks. Attacks may be accidental or they may be intentional, but all the watermarked images are prone to attack. Attacks also may be the attempts to change the image in order to wipe out the watermark and to preserve the image. Since watermarks may be hidden copyrights, these type of attacks are extremely undesirable and unwanted. To overcome these limitations a robust watermarking scheme is required. The attacks observed and the artifacts introduced results in lowering embedding efficiency. To achieve better embedding, wavelet based image coding is been

developed. Though Transform based coding approach is developed to minimize visual artifacts the edge preserving requirements are need to be developed.

III. Wavelet based watermarking scheme

Among various wavelet based coding approach Dote's [9] based coding approach is observed to have lower complexity in coding and embed the watermark in lower bands. The watermarking scheme based on this approach works on a multilevel wavelet transformation technique. The original image and the watermarked image are transformed into wavelet domain. This approach selects 5th level transformation for host image and 1st level for watermark. The original image and the watermarked image are transformed into wavelet domain. The developed technique in [7] is depicted in the Fig.1.

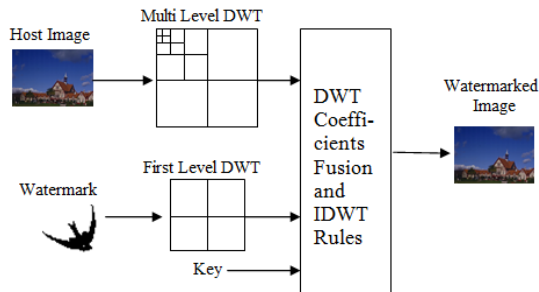


Fig. 1 Dote's coding approach using multilevel image fusion.

For the extraction, the watermark is retrieved by applying inverse procedure at each resolution level using the same secret key. Estimated the watermark by averaging the extracted watermarks and the extracted ones are normalized for binary values. In order to find out similarity between embedded and extracted watermarks the host and the marked images are observed perceptually. The correlation coefficients between the extracted watermark images at different signal to noise ratios (SNR) values were calculated. The correlation coefficient's' is used for similarity measurement, and the SNR is evaluated.

$$\rho(w, \hat{w}) = \frac{\sum_{i=1}^N w_i \hat{w}_i}{\sqrt{\sum_{i=1}^N w_i^2} \sqrt{\sum_{i=1}^N \hat{w}_i^2}}$$

$$SNR(W, \hat{W}) = 10 \log_{10} \frac{\sum_{i=1}^N w_i^2}{\sum_{i=1}^N (W_i - \hat{W}_i)^2}$$

Where N is the number of pixels present in the watermark, w and w □ are the original and extracted watermarks, respectively. The related measure of PSNR (in db) between host and marked image is computed using

$$PSNR = 20 \log_{10} [255/RMSE]$$

Where

$$RMSE = \sqrt{\frac{1}{M * N} \sum_{i=1}^M \sum_{j=1}^N [\tilde{f}(m, n) - f(m, n)]^2}$$

for the 8-bit gray level image.

The coding approach based on Dotes's method using wavelet transform embed the information in complete lower band but this approach may loss image information as they are embed at a

very lower level, also the image bounding sensitive regions may get more effective as the embedding is done in non-measured manner. To preserve the image quality of embedded and embedding image the regions for embedding need to be decided and solution need to be developed. In this paper a directional based filter coding is presented.

IV. Directional Watermarking scheme

To provide orientation based coding approach for image bounding regions a directional based filtration approach to the conventional wavelet based watermarking is proposed. Directional filter banks (DFB) [11] decompose the frequency space into wedge-shaped partitions as shown in Fig. 2.

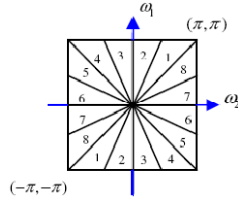


Fig.2. Directional filter bank frequency partitioning using 8 directions

Eight directions were used, where directional sub-bands of 1, 2, 3, and 4 represent horizontal directions (directions between -45° and +45°) and for the vertical directions (directions between 45° and 135°). The DFB approach is realized using iterated quincunx filter banks as illustrated in

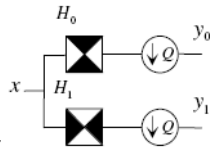


Fig. 3. defined by

Figure.3. Quincunx filter bank. H0 and H1

At the first level of the filter bank, a quincunx filter bank (QFB) is applied. The quincunx sampling matrix is

$$Q = \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}$$

The image is further decomposed by using two other QFBs at the outputs y₀ and y₁. Hence four outputs corresponding to the four directions of the filter bands are achieved. At higher level QFBs are employed in conjunction with resampling matrices. The resampling coefficients used per direction is as presented below,

$$R_h = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \text{ and } R_v = \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix}$$

Applying these resampling operations to the outputs of the QFB, a normalized oriented image is derived. For the obtained directional bands a normalized magnitude values are computed defined by,

$$N = \|y_i\|^2$$

The band density have higher pixel density in such directions are kept unmodified and band have lower normalized values are embedded with the watermark coefficients. This embedding is made on the directional band density hence the image are least effected on the directional variations. Coefficients satisfying the thresholding based criterion

$$N = \|y_i\|^2 > th$$

is used where the threshold (th), is defined by

$$th = 1/3 [(\sum_{i=1}^m \cdot \sum_{j=1}^n \cdot x_{i,j}) / m \times n]$$

The proposed approach of watermarking is as illustrated below,

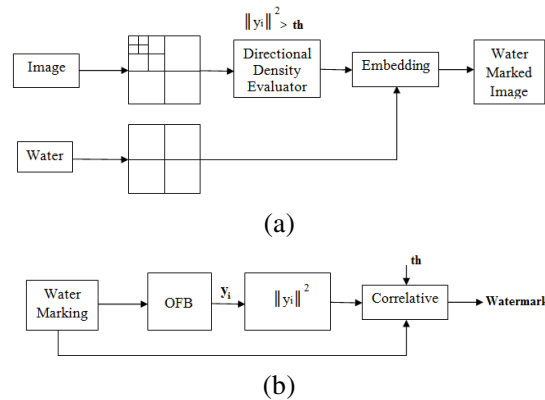


Figure4: (a) Proposed Orientational embedding encoding unit (b) Decoding unit

For the regeneration of the embedded watermark a reverse process of embedding is used. The watermarked image is processed with the DFB and the normalized magnitude value is computed. The bands having lower than the normalized magnitude value is taken as the watermark coefficients. To evaluate the operational performance of proposed approach a simulative analysis is carried out on Matlab[®] tool and the obtained results are as presented.

V. Result observation

In our investigation, the performance evaluation is based on three performance metrics; these are imperceptibility, execution time, and robustness against common signal processing operations. Each of these metrics is described in the forthcoming sections. An important way of evaluating watermarking algorithms is to compare the amount of distortion introduced into the original image by introducing a watermarking algorithm. In order to measure the quality of the image at the output of the decoder, mean square error (MSE) and peak to signal to noise ratio (PSNR) ratio measurement which measures the maximum signal to noise ratio found on an image has been used as an objective measure for the distortions introduced by the watermarking system are often used.

Distortion Measures:

1. Mean squared error

The Mean squared error (MSE) of an estimator is one of the way to quantify the amount by which an estimator differs from the true value of the quantity being estimated. Mean Squared Error is also called squared error loss. MSE measures the average of the square of the "error." The error is the amount by which the estimator differs from the quantity to be estimated.

$$MSE = \frac{1}{M \times N} \sum (I_w - I)^2$$

2. Signal to noise ratio

Signal-to-noise ratio compares the level of a desired signal (such as Image) to the level of background noise. The higher the ratio, the less noticeable the background noise is. Signal to noise ratio (SNR) effectively measures the quality of the watermarked image as compared to the

original image. This difference is represented as an error function that shows how close the watermarked image is to the original image and it is written as:

$$e(x, y) = I(x, y) - I_w(x, y)$$

The larger the value of $e(x, y)$ the greater is the distortion caused by the watermark and the attacks.

$$SNR = \frac{\frac{1}{N} \sum I_w^2}{MSE}$$

Which represents the size of the error relative to the input signal, alternatively on the logarithmic scale,

$$SNR(db) = 10 \log_{10}(SNR)$$

3. Peak signal to noise ratio

Peak signal-to-noise ratio, often abbreviated PSNR, is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale. The PSNR is most commonly used as a measure of quality of reconstructed image.

$$PSNR(db) = 10 \log_{10} \left(\frac{I_{peak}^2}{MSE} \right)$$

Where I_{peak} is the peak values of the input signal (usually 255 the maximum value of luminance level).

We use peak signal to noise ratio to evaluate the quality of image after embedding the watermark. In general a processed image is acceptable to human eye if its PSNR is greater than 30 db and greater the PSNR greater the image quality.

4. Similarity Factor

The similarity factor determines the similarity of pixel intensities between the original image and the watermarked image and also between the original watermark and the extracted watermark. An objective measure of similarity between the original image/watermark and the extracted watermark/watermarked image in the following way:

$$SIM = \frac{\sum_i \sum_j I(i,j) * I_w(i,j)}{\sum_i \sum_j (I_w(i,j))^2}$$

The similarity factor is approximately nearer to 1 for better imperceptible image quality

5. Payload

Capacity is an important property because it has a direct negative impact on watermark robustness. Higher capacity (the amount of information being embedded) causes lower watermark robustness. Capacity can be assessed by calculating the ratio of capacity to reliability. This can be done empirically by fixing one parameter (e.g. payload size) and determining the other parameter (e.g. error rate). Those results can then be used to estimate the theoretical maximum capacity of the watermarking system under consideration

$$\text{Capacity of Embedding} = \frac{\text{No. of bytes of hidden data}}{\text{No. of bytes of cover image}}$$

6. Robustness

Robustness property can be evaluated by applying various kinds of “normal” signal distortions and attacks that are relevant for the target application. The robustness can be assessed by measuring detection probability of the watermark after signal distortion.

7. Bit Correct Rate (CR)

A quality estimation parameter to check the robustness of the extracted watermark, named the Correct Rate (CR) is computed as an index to the objective quality of the image. The bit correct ratio (BCR) is defined as the ratio of correct extracted bits to the total number of embedded bits and can be expressed using the formula

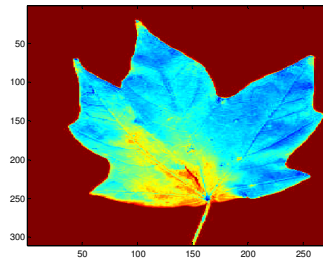
$$\text{CR} = \frac{\text{No. of Correctly detected Watermarked bits}}{\text{Total No. of Watermark bits}}$$

The Bit correct rate should be equal to 1.

8. Execution Time

Another tool for evaluation of algorithm is measurement of the amount of time required to embed a watermark into the original image, and then extract it afterwards. In our analysis, actual time in CPU cycles will be treated as a measure of execution time. This experiment is designed to determine the computational cost of each watermarking algorithm.

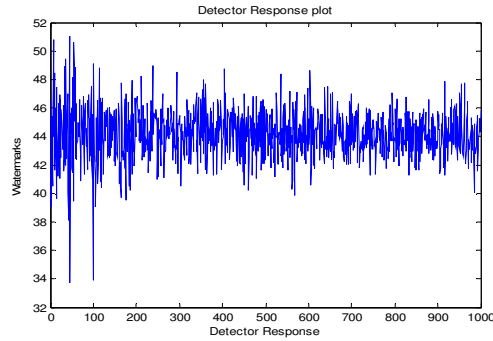
Original Image



Watermarked Image

Binary BEP map





Samples	Without DF		With DF	
	PSNR	SSIM	PSNR	SSIM
1	37.2	0.7	40.2	0.9
2	35.5	0.6	43.5	1
3	36.2	0.5	45.2	0.8
4	32.7	0.4	39.7	0.7

VI. Conclusion

This paper present an orientation based watermarking scheme in wavelet domain. The visual artifacts due to embedding at edge regions are minimized by the application of directional filters in processing. The embedding approach for watermark embedding is developed based on normalized directional band density and embedded watermarking based on directional density for sub bands. By the proposed approach it is observed that the PSNR under various attacks are minimized.

References

- [1] Langelaar, G.C., Setyawan, I., Legendijk, R.I., 2000. Watermarking digital image and video data. IEEE signal Process. Magazine (September), 20-46.
- [2] A. G. Bors and I. Pitas., “ Image watermarking using DCT domain constraints”, Proc. of IEEE Int. Conf. on Image Processing, vol. 3, pp. 231-234 (1996)
- [3] R.G. van Schyndel, A. Z. Tirkel, and C. F. Osborne, “A digital watermark”, Proc. of Int. Conf. in Image Processing, vol. 2, pp. 86-90, (1994).
- [4] J. Ohnishi and K. Matsui, “Embedding a seal into a picture under orthogonal wavelet transformation,” Proc. of Int. Conf. on Multimedia Comp. and Systems, pp. 514-521(1996-6).
- [5] D. Kunder and D. Hatzinakos, “ A robust digital image watermarking method using wavelet-based fusion”, Proc. of IEEE Int. Conf. on Acoustics, Speech and Sig. Proc., vol. 5, pp. 544-547 Seattle, Washington (1997-5).
- [6] D. Kunder and D. Hatzinakos.”Digital watermarking using multiresolution wavelet decomposition. In Proceedings of IEEE ICAPSSP '98, volume 5, pages 2969 – 2972, Seattle, WA, USA, May 1998.
- [7] SanghyunJoo, YounghoSuh, Jaeho Shin, and Hisakazu Kikuchi, “A New Robust Watermarking Embedding into Wavelet DC Components”, ETRI Journal, Volume 24, No. 5, October 2002.

- [8] Yasuhiko Dote, and Muhammad ShafiqueShaikh “A Robust Watermarking Method for Copyright Prot. of Digital Images using Wavelet Trans.” Trans. of the Institute of Electrical Engineering of Japan, vol. 122, No.2, Jan. 2003.
- [9] T. T. Nguyen and S. Oraintara, “A multi-resolution directional filter bank for image applications,” in proc. of IEEE International Conference on Acoustics, Speech, and Signal Processing, vol. III, pp. 37-40, 2004.
- [10] S. Park, M. J. T. Smith, and R. M. Mersereau, “Improved structures ofmaximally decimated directional filter banks for spatial image analysis,”IEEE Trans. Image Processing, vol. 13, no. 11, pp. 1424-1431, Nov.2004.