International Journal of Engineering & Technology, 7 (4.36) (2018) 414-418

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Based Image Watermarking Algorithm Based on Qr Decomposition in Lifting Wavelet

[1]Shailesh Kumar Shrivastava, [2]Dr. S.K Mahendran

1Research Scholar (Bharathiar University)
National Informatics Centre, Govt. of India, Bihar,
2Assistant Professor, Department of Computer Science, Govt. Arts College
Udhagamandalam -643002, The Nilgris, India

Abstract

In this paper, a non-blind watermarking system based on lifting wavelet transform and QR factorization has been proposed. The variance between coefficients of lifting wavelet transform in a block of size 2 x 2 has been used to embed binary watermark and blocks are randomly shuffled. The system minimizes distortion of watermarked image. The performance of scheme has been tested on some standard images and the simulation results have been evaluated and compared with some traditional methods. The experimental result shows that the proposed system is robust against image processing attacks.

1. Introduction

In this era, transferring multimedia data (i.e. text, image, audio and video) over the Internet is a common practice. The digital images, which accounts for about 35% among multimedia data, are easiest way to transfer larger amount of information [12]. Protecting the illegal usage (such as tampering, unauthorized copying or copyright protection) of digital images has become a challenge for industry, government, and private agencies. Digital watermarking can be considered as a dominant technique to solve these problems. The process of embedding a watermark (may be text or image) into original image is called digital watermarking without compromising the quality of original image.

In general, there are two widely accepted methods of watermarking, (a) spatial-domain and (b) frequency–domain. The spatial-domain methods are simple to implement and faster but not robust. Watermarks can be easily removed from the original image, while, frequency-domain methods are complex but robust. In this method, watermarking is accomplished by altering the magnitude of coefficients of the host image [1] [4] [20]. The examples of traditional frequency-domain (a.k.a transform-domain) are discrete wavelet transform (DWT), singular value decomposition (SVD), discrete cosine transform (DCT), discrete Fourier transform (DFT), etc. The basic characteristics of watermarking scheme should hold security, robustness, perceptual transparency, and payload. The watermarking techniques can be categorized, on the basis of host image required throughout the watermark extraction or not, as blind, semi-blind or non-blind. If host image is not required to extract the watermark then it is blind whereas non-blind technique requires host image. In semi-blind technique some data or feature of host image is used to extract watermark.

There are several DWT based watermarking techniques available in literature such as [3] [9] [10]. A technique based on DWT that usages statistical approach to embed watermark was developed in [3] but failed to resist against JPEG compression attack. An improvement was made by Li et al. [11] in which coefficients of host image are clustered into wavelet super trees and watermark was embedded using two wavelet super tree. It worked effectively against JPEG compression attack but futile and less effective against filtering attacks. Lin et al. [13] proposed a scheme by quantizing the significant different between wavelet coefficients using adaptive threshold value. This method was able to resist against several attacks for given threshold value while increasing threshold value the method is unable to extract watermark for fewer attacks.

Moreover, lifting wavelet transform (LWT) was proposed by Sweldens which overcomes the shortcoming of tradition discrete wavelet transform [6]. This scheme simplifies the problem of reversibility by directly evaluating into integer domain. The performance of this scheme is better than DWT (in terms of time and space) therefore it is being widely used in image processing. There are several techniques were proposed such as [2] [6] [16]. In this paper, we have proposed a non-blind watermarking system based on significant variance in LWT coefficients and QR factorization. The main aim is to make the scheme robust and secure. In order to make the scheme secure, secrete key is used also watermark is embedded dynamically in LWT coefficients. While combining the significant variance with LWT coefficients and QR factorization makes the scheme more robust and secure.

2. Preliminaries

2.1. QR decomposition

A matrix M_{mxn} can be decomposed into orthogonal-triangular bases [8] (a.k.a QR decomposition) as:

$$M_{mxn} = Q_{mxn} R_{mxn} \quad (1)$$

Where Q_{mxm} is an orthogonal matrix (i.e. $Q^TQ = I$) and an upper triangular matrix R_{mxn}. The absolute values of the first row in upper triangular matrix R_{mxn} is greater than other rows and the relationship among pixels are represented by the first column of Q_{mxm} matrix. The computational time of QR factorization is much

Copyright © 2016 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

smaller than other factorizations (i.e SVD) [17] also QR factorization can resist against several attacks (i.e adding noise, median filtering, contrast enhancement and sharpening) [5] [15] [17] [19].

2.2. Lifting wavelet transform

The lifting wavelet transform scheme, proposed by Sweldens [6] overcomes the shortcoming of tradition discrete wavelet transform. This scheme simplifies the problem of reversibility by directly evaluating into integer domain. The performance of this scheme is better than DWT (in terms of time and space) therefore it is being widely used in image processing (i.e. image compression [7], watermarking [14] [18]). The signal decomposition in LWT is achieved through following three steps:

- **Split** - In this step the given signal S(n) is divided into non overlapping odd $S_o(n)$ and even $S_e(n)$ samples as:

$$S_e(n) = S(2n),\ S_o(n) = S(2n + 1) \quad (2)$$

- **Predict** - The samples obtained in previous step can be used to predict each other if they are correlated by abstracting the difference G(n) as:

$$G(n) = S_o(n) - P[S_e(n)], \quad (3)$$

where P(.) is the predict operator and G(n) is high-frequency component that is used to define error between original sample and predicted value.

- **Update** - The even samples $S_e(n)$ are updated using update operator U(n) to reconstruct the abstract difference G(n), which represents low-frequency component L(n) that is coarse approximation of the original signal S(n) as follows:

$$L(n) = S_e(n) + U(G(n)) \quad (4)$$

3. Proposed Watermarking Technique

In this section our proposed technique in wavelet domain is presented. To evaluate our algorithm, we have compared it with DCT and SVD, two known methods in watermarking. To evaluate the performance, a similarity measure between the original watermark (W) and the extracted watermark (W') is computed by using the normalized correlation (NC) and the quality measure between original and watermarked image is measured by PSNR as shown in eq 5 & 6 respectively:

$$NC = \frac{\sum_{i=1}^{n} w_i w_i'}{\sum_{1}^{n} w_i^2} \quad (5)$$

$$PSNR = 10\log_{10}\frac{255}{\sqrt{MSE}} \quad (6)$$

$$MSE = \frac{1}{N \times N}\sum_{i=1}^{n}\sum_{j=1}^{n}\left[I_o(i,j) - I_w(i,j)\right]^2 \quad (7)$$

where NxN is the size of image, I_o is original image and I_w is watermarked image.

3.1. Watermark Embedding Algorithm

This section discusses the watermark embedding process. The host image is transformed using LWT to obtain low-frequency and high-frequency sub-bands. The coefficients of low-frequency sub-band (i.e. LL-band) are grouped into block of size 2x2. These blocks are randomly shuffled using secrete key. The variance is calculated for each block. If the variance of block B_i is less than mean of variance then block is considered as significant otherwise insignificant. QR factorization is performed on significant blocks and coefficients of R matrix is modified using equation 8. Watermarked bits are also shuffled using secret key for security purpose. Inverse-QR factorization in performed to reconstruct the block and inverse-LWT is performed to obtain watermarked image. The schematic diagram of watermark embedding process is illustrated in figure 1 The steps to embed watermark is as follows:

i. Decompose the host image (I) using LWT.
ii. Coefficients of LL sub-band is obtained.
iii. Group coefficients into non-overlapping blocks (B_i) of size 2x2.
iv. Randomly shuffle all blocks using key (k_1).
v. Select significant block
vi. Perform QR factorization on each significant block to obtain Q and R matrices.
vii. Convert the watermark image (W) bits into vector of length (l) and shuffle randomly using key (k_2), to obtain W'.
viii. For all watermark bits in W' use equation 8 to obtain R'.
ix. Perform inverse QR factorization to reconstruct the block (with Q and R').
x. Reshuffle all blocks to its original index.
xi. Perform inverse LWT.
xii. Watermarked image (I_w) is obtained.

$$\begin{cases} R'(1,1) = R(1,1) - (R(1,1) \mod S) + T1, & \text{if } W = 1 \\ R'(2,1) = R(2,1) - (R(2,1) \mod S) + T2, & \text{if } W = 0 \end{cases} \quad (8)$$

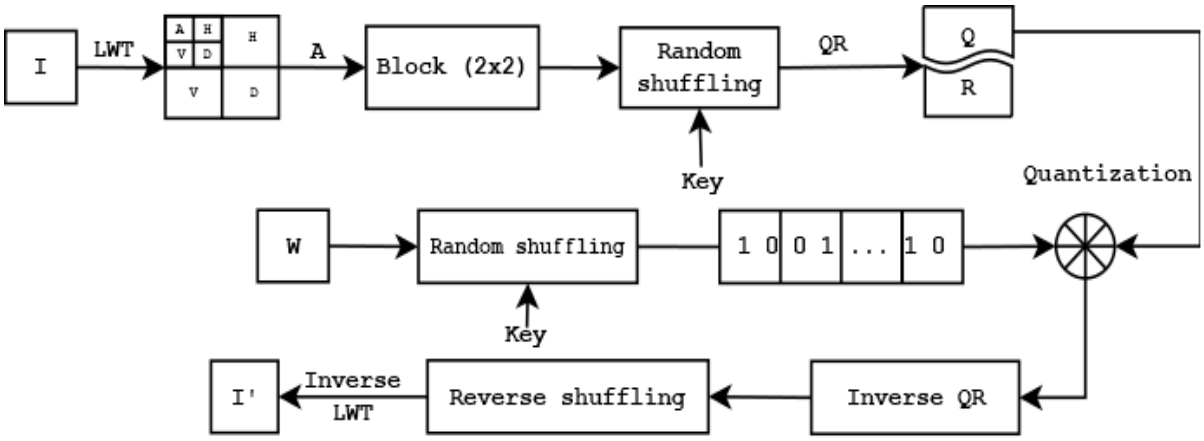


Figure 1: Block diagram of watermark embedding process

3.2. Watermark Extraction Algorithm

This section describes watermark extraction process. The watermarked and host images are transformed using LWT to obtain low and high frequency sub-bands. The coefficients of low-frequency sub-band are grouped into block of size 2x2. Random shuffling of blocks using secrete key (used in embedding process). Select significant block (from both host and watermarked images) and compare these blocks to obtain watermark bits. The schematic block diagram, for extraction process of watermark is shown in figure 2 and the algorithm to extract watermark is as follows.

i. Decompose the host (I) & watermarked image (I_w) using LWT.
ii. Coefficients of LL sub-band are obtained.
iii. Group coefficients into non-overlapping blocks (B_i) of size 2x2.
iv. Randomly shuffle all blocks using key (k_1).
v. Select significant block.
vi. Perform QR factorization on each significant block to obtain Q and R matrices.
vii. Initialize W' to the size l.
viii. For all significant blocks in B_{hi} & B_{wi}. Compare to obtain watermarked bits.
ix. Reshuffle all the bits of W' to its original index and reshape.
x.
xi. Watermark is obtained.

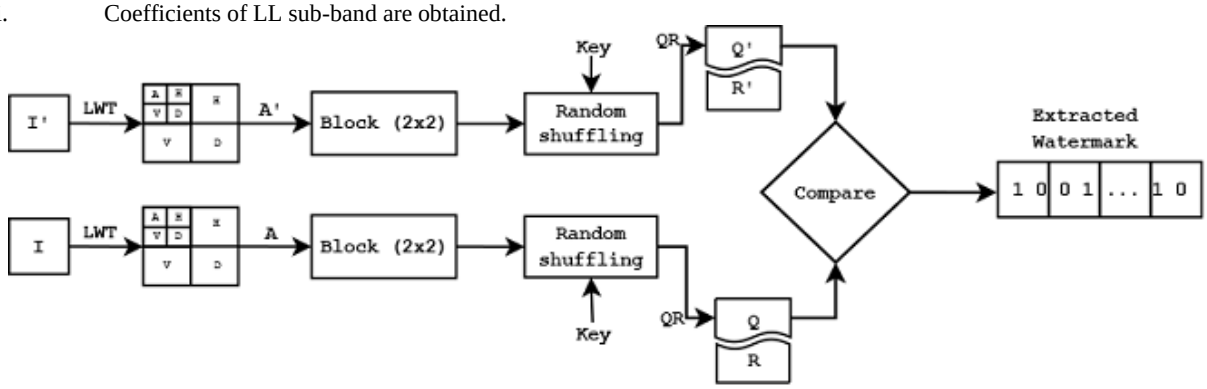


Figure 2: Block diagram of watermark extraction process

4. Results and discussion

In this section, experimental results of the proposed system are discussed. We have used four standard grayscale images (i.e. lena, cameraman, liftingbody, mandi) as experimental subjects, and binary watermark of size 32 x 16 as shown in figure 3 & 4 respectively. In figure 5, watermarked images and corresponding extracted watermark are shown without applying any attack. The results of watermarked image, in terms of PSNR value is shown in table 2. In order to test the performance, in terms of robustness and reliability, we have performed some fundamental geometric and non-geometric attacks such as Gaussian filter, speckle noise, salt and pepper noise, rotation, and scaling. In table 2, the results of subject image Lena under different attacks and extracted watermark are shown in terms of PSNR and NCC values. In table 3, NCC and corresponding PSNR of extracted watermark for various attacks on different images are shown.



(a) **Lena** (b) Lena

(c) Lena (d) Lena

Figure 3: Benchmark Images



(a)



(e)

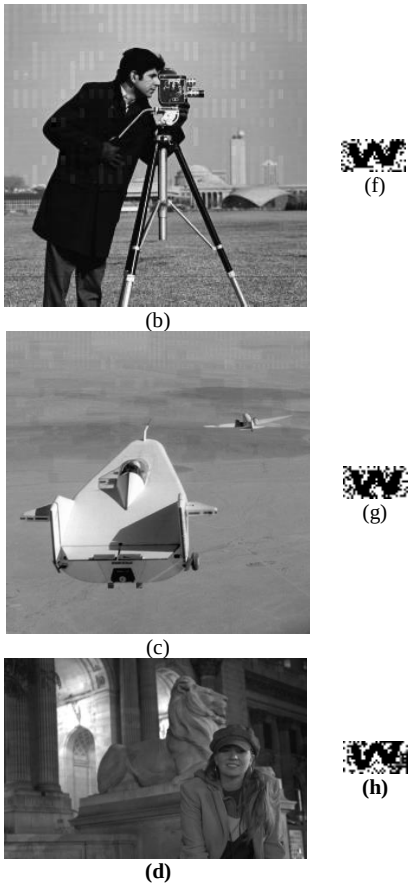


Figure 4: Watermark Image

Table 1: PSNR values of watermarked Images

Image	PSNR
Lena	40.58
Cameraman	38.68
Liftingbody	47.24
Mandi	64.17

Table 2: PSNR and NCC values with different attacks

Attack	PSNR	NCC	Extracted Watermark
Speckle	51.9205	0.7902	
Salt & Pepper	51.8569	0.7823	
Scaling	89.5601	0.7271	
Gaussian	56.2369	0.7523	
Rotation	54.1256	0.8562	

Table 3: PSNR and NCC values with different attacks

Image/Attack	Speckle	Salt & pepper	Scaling	Gaussian	Rotation
NCC Values					
Lean	0.7902	0.7823	0.7212	0.7523	0.8562
Cameraman	0.6923	0.6542	0.6969	0.7023	0.7123
Liftingbody	0.7256	0.7563	0.7012	0.6901	0.8823
Mandi	0.6223	0.5689	0.6396	0.7012	0.6222
PSNR Values					
Lean	51.1205	51.8569	58.5601	56.2369	54.1256
Cameraman	50.2323	54.8801	60.2145	58.9456	50.5236
Liftingbody	58.4512	54.1258	60.2356	48.23	52.2378
Mandi	42.1245	40.4569	42.4512	43.7832	40.0121

Table 4: Comparison of results

Attack/NCC	Phadikar et al. [16]	Li et al. [11]	Proposed Scheme
Gaussian	0.5231	0.70	0.7114
Speckle	0.7143	-	0.7076
Scaling	-	0.35	0.6890
Rotation	-	0.46	0.7682

The significant difference between watermarked image without & with attacks can be observed through histogram plots (figure6a-e) which clearly indicate that most of the information is localized towards the centre, though the watermarked image is distorted. Verma et al. [21], has shown the significant difference between traditional and lifting wavelet transforms in case of watermarked image is distorted.

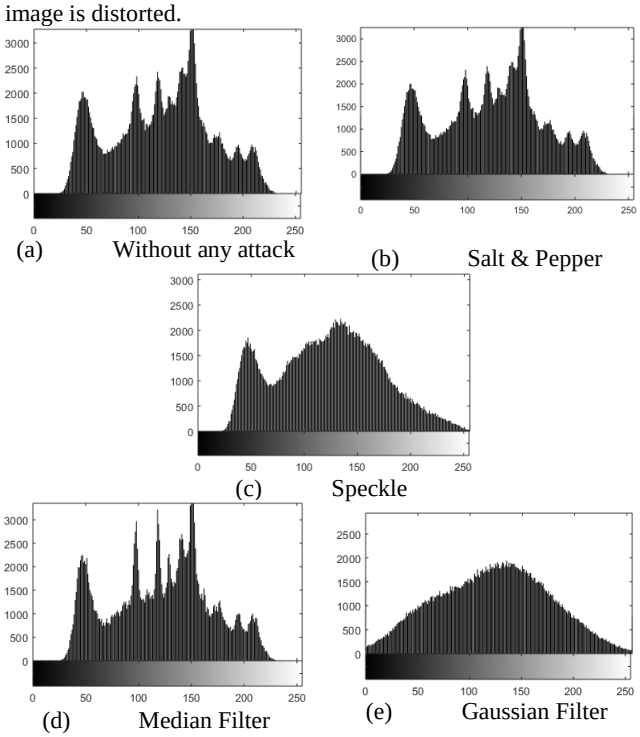


Figure 5: Watermarked Image & Extracted Watermark

Moreover, We have also compared our results with different existing techniques such as [11] & [16] shown is table 4. On comparing our technique using NCC (average values) for different attacked watermarked images shows that it is more robust against scaling and Gaussian filter attacks. The results shown in table 3 are much better than techniques proposed in [11] & [16].

5. Conclusion

In this paper, a non-blind watermarking scheme based on variance of lifting wavelet coefficient is proposed. The benefits of LWT over traditional wavelet transform are utilized to enhance the performance. The quantization of significant variance for embedding and extraction process of binary watermark. The results shows that the proposed technique is more robust against different geometric and non-geometric attacks such as Gaussian filter, rotation, scaling, speckle, and salt \& pepper noise. We have also employed security measures to shuffle blocks of host image as well as watermark bits, which adds extra layer of security and robustness. We have also compared our results with previously proposed techniques and found that the performance of our technique is much better. In spite of various advantages the proposed technique has some limitations. The performance is less efficient against intentional attacks or higher angle of rotation.

References

[1] Gaurav Bhatnagar and Balasubramanian Raman. A new robust reference watermarking scheme based on dwt-svd. *Computer Standards & Interfaces*, 31(5):1002-1013, 2009. Specification, Standards and Information Management for Distributed Systems.

[2] Amit Bohra, Omar Farooq, and Izharuddin. Blind self-authentication of images for robust watermarking using integer wavelet transform. *AEU -International Journal of Electronics and Communications*, 63(8):703 707, 2009.

[3] KeunDuck Byun, Sangjin Lee, and HyungJun Kim. A watermarking method using quantization and statistical characteristics of wavelet transform. In *Sixth International Conference on Parallel and Distributed Computing Applications and Technologies (PDCAT'05)*, pages 689{693, Dec 2005.

[4] Ding-Yun Chen, Ming Ouhyoung, and Ja-Ling Wu. A shift-resisting public watermark system for protecting image processing software. *IEEE Transactions on Consumer Electronics*, 46(3):404-414, Aug 2000.

[5] Hong-yuan Chen and Yue-sheng Zhu. A robust watermarking algorithm based on qr factorization and dct using quantization index modulation technique. *Journal of Zhejiang University SCIENCE C*, 13(8):573{584, Aug 2012.

[6] Ingrid Daubechies and Wim Sweldens. Factoring wavelet transforms into lifting steps. *Journal of Fourier Analysis and Applications*, 4(3):247-269, May 1998.

[7] Wenbing Fan, Jing Chen, and Jina Zhen. Spiht algorithm based on fast lifting wavelet transform in image compression. In Yue Hao, Jiming Liu, Yu-Ping Wang, Yiu-ming Cheung, Hujun Yin, Licheng Jiao, Jianfeng Ma, and Yong-Chang Jiao, editors, *Computational Intelligence and Security*, pages 838-844, Berlin, Heidelberg, 2005. Springer Berlin Heidelberg.

[8] J. G. F. Francis. The qr transformation a unitary analogue to the lr transformation|part 1. *The Computer Journal*, 4(3):265-271, 1961.

[9] Jianyong Huang and Changsheng Yang. Image digital watermarking algorithm using multiresolution wavelet transform. In *2004 IEEE International Conference on Systems, Man and Cybernetics (IEEE Cat. No.04CH37583)*, volume 3, pages 2977-2982 vol.3, Oct 2004.

[10] Mingyan Jiang, Guoping Xu, and Dongfeng Yuan. A novel blind watermarking algorithm based on multiband wavelet transform. In *Signal Processing, 2004. Proceedings. ICSP '04. 2004 7th International Conference on*, volume 1, pages 857-860 vol.1, Aug 2004.

[11] Enping Li, Huaqing Liang, and Xinxin Niu. Blind image watermarking scheme based on wavelet tree quantization robust to geometric attacks. In *2006 6th World Congress on Intelligent Control and Automation*, volume 2, pages 10256-10260, 2006.

[12] N. Lin, J. Shen, X. Guo, and J. Zhou. A robust image watermarking based on dwt-qr decomposition. In *2011 IEEE 3rd International Conference on Communication Software and Networks*, pages 684-688, May 2011.

[13] W. H. Lin, S. J. Horng, T. W. Kao, P. Fan, C. L. Lee, and Y. Pan. An efficient watermarking method based on significant difference of wavelet coefficient quantization. *IEEE Transactions on Multimedia*, 10(5):746-757, Aug 2008.

[14] Khaled Loukhaoukha, Jean-Yves Chouinard, and Mohamed Haj Taieb. Multi-objective genetic algorithm optimization for image watermarking based on singular value decomposition and lifting wavelet transform. In Abderrahim Elmoataz, Olivier Lezoray, Fathallah Nouboud, Driss Mammass, and Jean Meunier, editors, *Image and Signal Processing*, pages 394-403, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.

[15] Yashar Naderahmadian and Saied Hosseini-Khayat. Fast watermarking based on qr decomposition in wavelet domain. In *Proceedings of the 2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, IIH-MSP '10, pages 127-130, Washington, DC, USA, 2010. IEEE Computer Society.

[16] A. Phadikar, S. P. Maity, and M. K. Kundu. Quantization based data hiding scheme for efficient quality access control of images using dwt via lifting. In *2008 Sixth Indian Conference on Computer Vision, Graphics Image Processing*, pages 265-272, Dec 2008.

[17] Wei Song, Jian-jun Hou, Zhao-hong Li, and Liang Huang. Chaotic system and qr factorization based robust digital image watermarking algorithm. *Journal of Central South University of Technology*, 18(1):116-124, Feb 2011.

[18] T. Sree Sharmila and K. Ramar. Efficient analysis of hybrid directional lifting technique for satellite image denoising. *Signal, Image and Video Processing*, 8(7):1399-1404, Oct 2014.

[19] Qingtang Su, Yugang Niu, Gang Wang, Shaoli Jia, and Jun Yue. Color image blind watermarking scheme based on qr decomposition. *Signal Processing*, 94:219-235, 2014.

[20] T. Tachibana, M. Fujiyoshi, and H. Kiya. An image-quality guaranteed watermarking scheme with spreading spectrum of watermark. In *IEEE International Symposium on Communications and Information Technology, 2004. ISCIT 2004.*, volume 1, pages 330{334 vol.1, Oct 2004.

[21] Vivek Singh Verma and Rajib Kumar Jha. Improved watermarking technique based on significant difference of lifting wavelet coefficients. *Signal, Image and Video Processing*, 9(6):1443{1450, Sep 2015.