International Journal of Research in Advent Technology, Vol.2, No.2, February 2014

E-ISSN: 2321-9637

A Novel Cover Image Encrypted Based Watermarking Algorithm for Enhanced Security

Mr. Rakhendra Kumar Ramtekkar [1], Mrs. Shikha Gupta[2]
Electronics & Telecommunication[1,2], Dr.C.V.Raman University, Bilaspur(C.G.)[1, 2]
Rakhendra776@rediffmail.com[1], Shikha.Mishra687@gmail.com[2]

Abstract- A novel digital watermarking algorithm has been proposed in this paper which is a combination of cover image encryption and wavelet domain based watermarking algorithm. Row and column shuffling based encryption method has been proposed for cover image encryption. Watermark is embedded in encrypted cover image by using wavelet domain approach.

Keywords : Digital watermarking[1], wavelets[2], row shuffling[3], column shuffling[4], embedding[5], spread spectrum[6], PSNR[7], correlation[8].

.

1. INTRODUCTION

Security of information is one of the prime issue in the present growing era of information technology. There is need to develop very efficient security system for preventing important and confidential information from being hacked by unauthorized person. With the advancement in the technology more and more computing power is available making it easier for the unauthorized person to break the older security system. Now a days internet is flooded with the copyrighted digital content. Anyone can access and steal these digital content. Therefore it is very necessary that there must be some

technique for authorizing the digital content. Digital watermarking is one of digital authentication technique [1] which can deal with this kind of problem. In a digital watermarking, digital signature, authorization sign or company's logo is embedded in a digital content by using some special algorithm. Only authorized person is able to detect / extract this watermark from the digital content and make decision about the digital content. There are various application of watermarking such as for copy right protection, prevention of unauthorized copying,f or image authentication and in medical field where it is used to hide information like patients name ,age and other significant information[2-4].A watermarking algorithm must satisfy properties like invisibility, robustness, security and readability [5][6].

Watermark can be embedded in a pixel or frequency component [7]. On the basis of working environment, digital image watermarking can be divided in to two parts (i) Frequency domain techniques (ii) Spatial domain techniques. Spatial domain techniques hide the watermark directly on the pixel while the frequency domain techniques.

[8],[9],[10],[11],[12],[13] hide the watermark in frequency component of image. In frequency domain technique, an image is divided in to different component using some algorithm. Discrete cosine transform(DCT), Discrete Fourier transform(DFT) and Discrete wavelet transform are some transform method which divides the signal into various frequency component. Frequency domain techniques modified the frequency component of the signal/image and when these modified frequency component is inversely transform then the watermarked image is formed [14],[15].

2. Discrete Wavelet Transform

In signal processing, Fourier transform is used to convert the time domain information to frequency domain information. Though Fourier transform tell us about the frequency component present in the signal but it is unable to show the time at which each frequency component occurs in signal[16].This drawback is overcome by the Discrete wavelet transform because it carries both frequency as well as time information and hence give more detail information of the signal[17].If DWT transform is applied to any image then it divides the image into different frequency component known as low frequency (LL), Mid frequency (LH,HL) and high frequency coefficient(HH).Due to this fact, DWT can be used for embedding the watermark. For this first of all the image is decomposed into different frequency coefficient and then selected frequency coefficients are used for embedding the watermark. This process modifies the selected frequency coefficients. Taking inverse transform of these modified frequency

coefficients give the watermarked image(an image into which the watermark is embedded).

3. Spread Spectrum Technique

Least significant method of watermarking is one of the simplest method of watermarking in which the least significant bit of each pixel of the cover image is replaced by the watermark bit. Apart from having the poor security ,this method is vulnerable to the image enhancement operation and hence rarely used in watermarking.

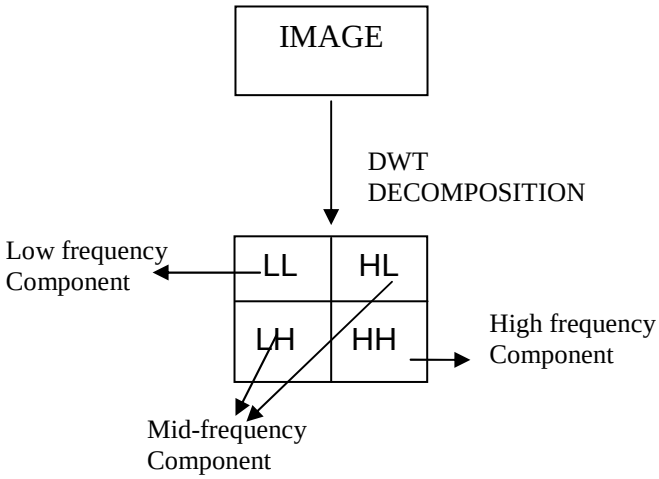


Figure 1

The above mentioned limitations can be overcome by spread spectrum techniques[8] in which the watermark bit is spread in all over the frequency coefficient of the selected frequency band using psudo random sequence which acts

4. random row and column shuffling based encryption method

The algorithm steps for row and column based random shuffling encryption method are as follows-

Step 1: First of all generate the random number matrix of dimension 1xR from 1 to R where R is number of rows in cover image using random number generator using Key1

Step 2: Now take two consecutive element of random number matrix as the number of row and interchange their position.

Step 3 : Repeat this operation till all the elements of random number matrix gets exhausted.

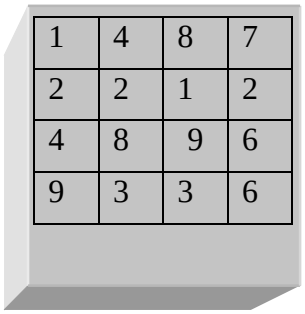
Step 4: Repeat step 2 and step 3 for column also. Here we can generate the different random number matrix for column operation or the previous random matrix of Row shuffling can also be used.

Step 5: After step 4 the image is encrypted by shuffling the row and column randomly whose order is decided by the random number generator initialized by Key1.

Suppose the Random matrix(Generated by Key1) is given by

[1 4 3 2]

The process is shown in Figure for an artificial image of 4x4 dimensions.



Original Image

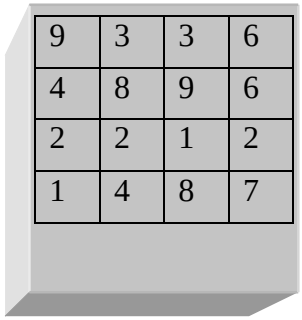


Image after Row shuffling
(By replacing first and 4th row
and then 2nd and 3rd row)

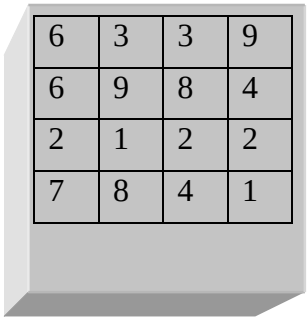


Image after column shuffling
(By replacing first and 4th column
and then 2nd and 3rd column)

Figure 2 Encryption Process

Decryption Process:

Step1 : Read the encrypted image.

Step2: Apply the reverse shuffling of column by generating the random number generator initialized by the same Key1 as used in encryption process.

Step3: Apply the reverse shuffling of Row by generating the random number generator initialized by the same Key1 as used in encryption process.

Step 4 : After the step 3, Decrypted image is recovered.

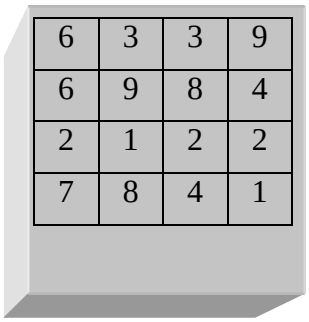
If this operation is repeated for 3 to 4 times using different Key, a very secure encryption could be achieved.

Generate the random matrix (generated by same key 1 as used in encryption process)

[1 4 3 2]

Reverse the matrix

[2 3 4 2]



Encrypted Image

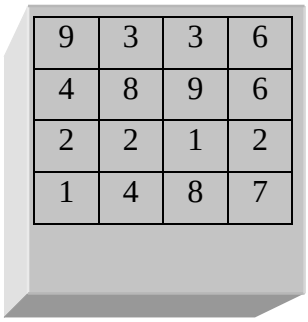
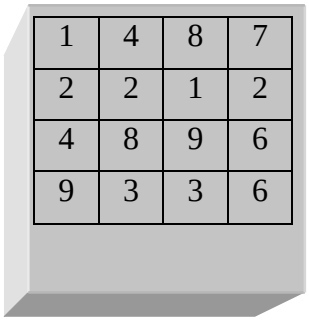


Image after column shuffling
(By replacing first and 4th column
and then 2nd and 3rd column)



Final Decrypted Image after Row shuffling
(By replacing first and 4th row
and then 2nd and 3rd row)

Figure 3 Decryption process

5. Spread Spectrum Technique

Least significant technique is one of of the simplest spatial domain technique of embedding the watermark in cover image by substituting the least significant bit of cover image with the watermark bit .Main drawback of this technique is its poor security and its vulnerability to image manipulation or image enhancement. Due to these limitation it is rarely used for watermarking purpose. These drawbacks are overcome by frequency domain technique *known as* spread spectrum technique[8].In this technique each and every bit is spread to all the frequency coefficient of the chosen frequency band using random noise generated by Pn-sequence. Since these random noise has very good correlation property therefore extraction of watermark is also possible while maintaining the good security.

6. PROPOSED METHOD

6.1 Embedding Process

The main idea of this algorithm is to encrypt the cover image and then embed the watermark on this encrypted cover image by using spread spectrum technique. The encryption process just shuffle the row and column of the cover image randomly, the pixel value remain intact but get displaced to other random position. The randomness is decided by the initialization key of the pseudo random generator. Since pixel value remain same in the encrypted cover image therefore these pixel value can be modified by the embedding operation without posing any problem. In the extraction process since this algorithm uses correlation to extract the watermark from the watermarked image therefore it is necessary to encrypt the watermarked image for extracting the watermark .If correlation is taken for watermarked image without encrypting it then it will become impossible to recover the watermark. This process make it necessary to encrypt the watermarked image

for extracting the watermark and hence make it more secure method.

First of all the cover image is encrypted using random row shuffling and column shuffling as described earlier in this paper. After encrypting the cover image using row and column shuffling, blue channel of the cover image is extracted and DWT decomposition is performed on this blue channel. The reason for choosing blue channel for embedding is that any minor change in the pixel of blue channel has least effect in image quality due to blue color being the least perceptual to human eye[4].The DWT decomposition divide the blue channel into four frequency component LL,LH,HL,HH. After that LH and HL frequency component is chosen and extracted for embedding the watermark using the spread spectrum techniques. Watermark is embedded on mid frequency component (LH,HL) of the blue channel using equation (1)

$$WI(I,j)=I(i,j) + \alpha \times pn(i,j) \quad \text{if } W=0$$
$$=I(i,j) \quad \text{if } W=1 \qquad \dots (1)$$

Where

I(i, j) =Mid frequency DWT coefficient of Cover image.

IW(i,j) = Modified Mid frequency DWT coefficient of Cover image.

α = Gain Factor

W = Watermark bit

pn(i,j) =Pseudo-random sequence

The value of α is very crucial in this algorithm and hence need to be chosen verycarefully. The robustness and invisibility of watermark depends upon this factor. Selecting too much higher value of α will degrade the quality of cover image while selecting too much low value of α will make it difficult to recover the watermark correctly.Once embedding operation is finished in the mid frequency component of blue channel, all the blue channel mid frequency component gets modified and then inverse DWT operation is performed to get back the encrypted cover image. The last step of embedding operation is to perform decryption algorithm to get back the original cover image.

The whole process is shown in Figure1.

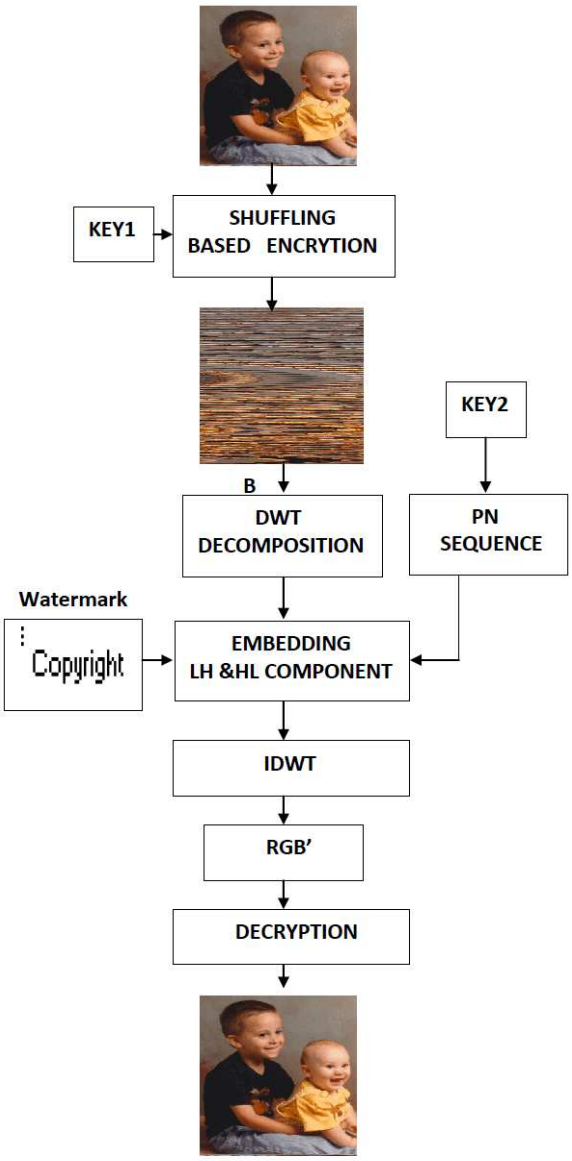


Figure 7

The steps of Embedding algorithm are as follows-

Step 1 Read the Cover image.

Step 2 Encrypt the cover image by apply random row and column based shuffling.The randomness is decided by the Key1.

Step3 Select the blue channel of the encrypted cover image.

Step 4 Apply DWT decomposition on blue channel and get all the frequency component (LL,LH,HL,HH)`

Step 5 Select the mid frequency component(LH and HL).

Step 6 Embed the watermark using equation 1.the PN-sequence is initiated by Key2.

Step 7 Apply inverse DWT transform to get back the modified blue channel.

Step 8 Combine Red channel, Green channel and modified Blue channel to get back the encrypted cover image.

Step 9 Apply reverse shuffling to get back the original cover image with embedded watermark(Watermarked image).

6.2 Extraction Process

The extraction algorithm begins by inputting the watermarked image to the system.This watermarked image is encrypted by random row and column shuffling whose randomness is decided by the random number generator seeded by the same Key1 which is used for encrypting the cover image in embedding process.The encrypted image is then DWT decomposed to get the mid frequency component(LH,HL).These mid frequency component then correlated with pn-sequence seeded by the same Key2 which is used in embedding process. Since in this algorithm both key1 and key2 is required to extract the watermark therefore it is more secure than the simple spread spectrum based method.

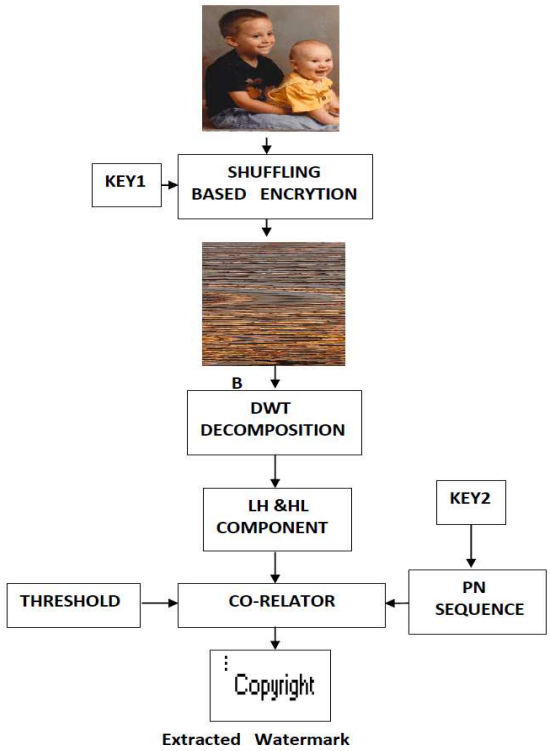


Figure 8

The steps of Extraction algorithm are as follows-

1.Read the Watermarked image.

2.Encrypt the watermarked Image using random row and column shuffling.The randomness is decided by the pseudo random number generator seeded by the Key1.

3. separate out the blue channel from the Encrypted watermarked image.

4. Decompose the Blue channel of watermarked image into LL,LH,HL,HH frequency component using DWT.

5. Separate out the LH and HL (Mid frequency) component.

6. Using Key2,generate pn-sequence.

7. Calculate the correlation matrix1 by correlating the HL coefficient and pn sequence generated in each step.

8. Calculate the correlation matrix2 by correlating the LH coefficient and pn sequence generated in each step.

9.Compute the mean correlation matrix by using formula given below

Correlation matrix=(Correlation matriox1+Correlation matrix2)/2.

8. Set each pixel of watermark to zero or one as per the rule given below-

WM=0 if correlation >mean correlation

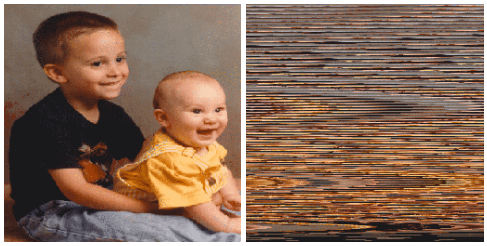
=1 if correlation <mean correlation

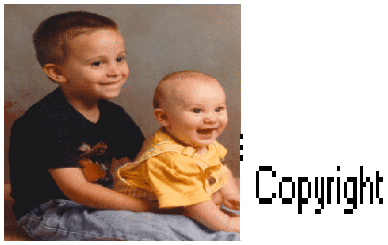
7. EXPERIMENTAL RESULT

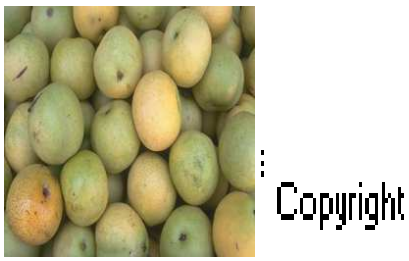
Proposed method has been implemented in a PC with 2GB RAM and core2duo processor and running MATLAB ver 7.9.0.the performance of proposed method is tested by computing the PSNR between actual watermark and extracted watermark.In order to see the effect of gain factor and size of the cover image on extracted watermark, PSNR between actual watermark and extracted watermark has been computed and is depicted in Table1.The effect of gain factor on the quality of original image has also been examined by calculating the PSNR between original Image and Watermarked image which summarized in Table2.The execution time of proposed method for different size of cover image is also computed and given in Table4.

It is evident from these table that the quality of the extracted watermark is decreased as we decrease the gain α from .8 to .2 which can be verified by decreasing value of PSNR in Table1.

Figure 9 Watermark







abcd

Figure 10 (a) Original Image (b) Watermark after Scanning Encryption (c) Watermarked Image (d) Extracted Watermark

The gain factor α also affect the quality of the original image which is clear by Table 3 in which the PSNR between original and watermarked image is increasing as we decrease the gain factor from .8 to .2.Low value of gain factor gives better quality of the watermarked image with respect to original image.

Table 2 clearly shows the effect of size of cover image on the quality of the extracted watermark and the watermarked image by keeping the gain factor constant (in this case it is set to .5).

This analysis clearly shows that the performance of the proposed method is very good under different conditions of parameter. Moreover encrypting the watermark before embedding enhance the security of the watermark to such an extent which is difficult to break.

Table 1:PSNR Between Original and Recovered watermark

S.N.	K	PSNR between Original and Recovered Watermark (For Lenna Image)
1.	0.7	34.49
2	0.6	33.12
3	0.5	31.89
4	0.4	30.72
5	0.3	26.39
6	0.2	21.18
7	0.1	15.64

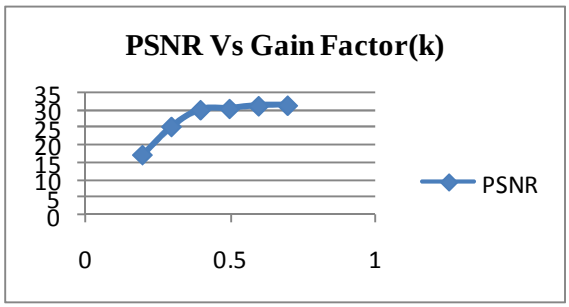


Figure 11 Comparison between Original and Recovered Watermark

Table 2: PSNR Between Original and Watermarked Image

S.N.	K	PSNR between Original and Watermarked Image (For Lenna Image)
1	0.7	62.1534
2	0.6	63.1764
3	0.5	64.1156
4	0.4	65.2393
5	0.3	66.6170
6	0.2	72.1344
7	0.1	72.1329

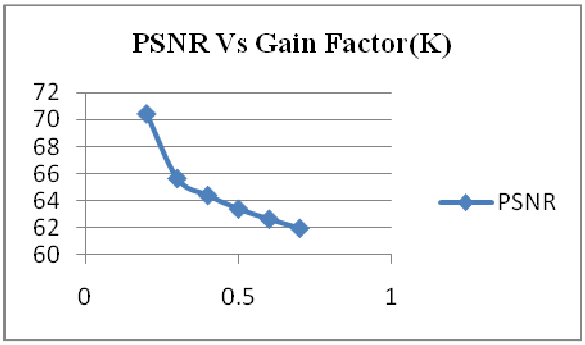


Figure 12 Comparison Between Original and Watermarked Image

Table 3:PSNR comparison for Different size of Image

S.N.	Image Size	PSNR Between Original and Watermarked Image	PSNR Between Original and Recovered Watermark
	For k=.5 and for Lenna Image		
1	512x512	35.4762	72.7865
2	256x256	32.8767	65.2231
3	128x128	30.4532	48.5444
4	64x64	23.7767	39.2781

Table 4:Execution Time Comparison

S.N.	Image Size	Execution Time (In second)
1	512x512	85
2	256x256	66
3	128x128	54
4	64x64	46

References

[1] F.Hartung and M. Kutter, "Multimedia Watermarking Techniques," in proc. of the IEEE, vol. 87, no. 7, pp. 1079-1107, July 1999.

[2] F. Hartung and M. Kutter, "Multimedia watermarking techniques," Proceedings of the IEEE, Volume 87, Issue7, 1999, pages1079-1107.

[3] F. Hartung and M. Kutter, Stefan Katzenbeisser and FabienA. P. Petitcolas, editors, Information Hiding Techniques for Steganography and Digital watermarking,Artech House, 2000.

[4] Juergen Seitz, Digital Watermarking for Digital Media,Information Science Publishing, 2005.

[5] Ming-Shing Hsieh, Din-Chang Tseng, Member, IEEE,and Yong-Huai Huang "Hiding Digital Watermarks Using Multi resolution Wavelet Transform", IEEE Transactions on Industrial Electronics, Volume 48, Issue 5, pages 875-882, Oct. 2001.

[6] Sin-Joo Lee, Sung-Hwan Jung, "A Survey of watermarking techniques applied to multimedia", IEEE Transactions on Industrial Electronics, Volume 1, pages 272-277, 2001.ISSN :

[7] Ali Al-Haj "Combined DWT-DCT Digital Image Watermarking," Journal of computer science 3 (9),740-746,ISSN, 2007.

[8] Arvind Kumar Parthasarathy and Subhash Kak "An Improved Method of Content Based Image Watermarking "IEEE Transaction on broadcasting, Vol. 53, No. 2, June 2007, PP 468-479.

[9] Ibrahim Nasir, Ying Weng, Jianmin Jiang, "A New Robust Watermarking Scheme for Color Image in Spatial Domain"

[10] Deepa Kundur and Dimitrios Hatzinakos, "Digital watermarking using multiresolution wavelet decomposition"

[11] Peter Meerwald, " Digital image watermarking in the wavelet Transform domain " P.Hd thesiss

[12] Chirawat Temi, Somsak Choomchuay, and Attasit Lasaku "A Robust Image Watermarking Using Multiresolution Analysis "Wavelet- Proceedings of ISCIT2005.

[13] D. Taskovski, S. Bogdanova, M. Bogdanov, " Digital Watermarking in wavelet domain"

[14] Xiang-Gen Xia, Charles G. Boncelet and Gonzalo "Wavelet Transform based watermark for digital Images", R. Arce : OPTICS EXPRESS, 7 December 1998 / Vol. 3, No. 12, PP 497-511

[15] Maha Sharkas, Dahlia ElShafie, and Nadder Hamdy ,"A Dual Digital-Image Watermarking Technique", Transaction on Engineering, computing and technology, Vol 5, April 2005 ISSN 1305-5313.

[16] Rafael C. Gonzalez, R.E.Woods, Steven:, "Digital image processing using MATLAB:"

[17] Vallabha V Hampiholi, " Multiresolution Watermark Based on Wavelet Transform for Digital images"