Journal of Engineering and Applied Sciences 13 (11): 4001-4008, 2018
ISSN: 1816-949X

Using Discrete Wavelet Transformation Algorithm for Authentication Digital Image Watermark

Zahraa Jabbar Hussein
College of Nursing, University of Babylon, Hillah, Iraq

Abstract: Watermarking is one of the methods to hide secret information in multimedia contents. The main concept of watermarking is a pattern of bits placed into an image. Watermarking is also a type of steganography field in which some of the useful information can be hidden inside another innocent image. In this study, the watermarking is utilized for solving the authentication issue. In addition to utilizing Discrete Wavelet Transform (DWT) algorithm to develop image security by hiding the watermark image inside the original image to prove owner image. DWT can combine more than one image by using mathematical techniques and used to embed and extract the watermark image and low bit-rate transmission. Different type of attacks can be used in order to steal the ownership or destroy it such as rotation, dithering and cropping attack. This study expected to conclude a technique that is able to hide the secret information (message) inside the image by utilizing DWT to avoid all the different types of attacks and finally extract the secret data from the image. Two techniques have been used to achieve imperceptibility and robustness of the watermark against certain geometric and non-geometric attacks. DWT is the solo technique showed good imperceptibility with 80.128 value of PSNR while DWT-DCT showed greater improvement with 96.73 of the PSNR value. The proposed technique gave impressing performance against different attacks such as Gaussian noise, dithering and cropping. On the other hand, DWT-DCT experiences difficulties against compression and rotation techniques due to the nature of the attacks.

Key words: DWT, DWT-DCT, PSNR, cropping, rotation, attacks

INTRODUCTION

Digital image distribution facilitated through internet has both positive and negative sides especially concerning the original ownership of the digital image (Terzija, 2006). One of the positive sides of the distribution is that the owner of the image can quickly make known by sending into various addresses in the world and he or she can make known instantly (Jafri and Baqai, 2007; Mohanty *et al*., 2006). While the downside of the distribution is that if there is no copyright protection mechanism, the image like commercial or digital artwork will be easily copied and gain untrue ownership by others. The cost of such problem is high, especially, when the digital research is highly valuable (Yu *et al*., 2006).

Watermarking is one solution to protect copyrights on digital photos being produced (Lumini and Maio, 2001). With the implementation of (DIW) Digital Image Watermarking, the copyright of digital photos generated will be protected by inserting additional information as owner information originality and etc. into the picture digitally (Nguyen *et al*., 2009). Watermarking is one of the tools of information hiding method to secure data interspersed with other information in order to protect rights, copyrights, etc. Also, Discrete Wavelet Transform (DWT) represents a tool highly utilized in blind watermarking technique and escrow to transform domain watermarking. Wavelet-based watermarking is a popular approach because of its strength against malicious attacks

Literature review: The study began by exploring the various methods used in digital watermarking which are authentication, fingerprinting and digital rights. The study presents a novel digital watermarking technique that can confront wavelet-based compression and standard watermark attacks. The proposed technique is compatible with SNR scalable transmission character accompanied with most wavelet compression suites that the watermark might be verified at any SNR transmission. The study explored the use of DWT digital watermarking technique. The study tried to make comparisons between eight wavelet families when using blind, non-visible watermark in digital media. The study looked at the effectiveness of each wavelet family on the effect of mother wavelet, the ability of the embedded watermark to imperceptions and the extracted watermark to be read, PSNR and IQI (Image Quality Index) (Jiansheng *et al*., 2009). This study presents a digital watermarking algorithm that is based on Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) using the blocking technology human vision feature in which watermarking signal was inserted

in wavelet band with a high frequency (Hemalatha and Maneesha, 2016). Accompanying with the features of Discrete Fourier Transform (DFT), image edge is reversed by the use of Discrete Cosine Transform (DCT) in order to transform the image into the form of even function. DCT is considered as one of the most popular linear transformations in digital signal process technology (Dharwadkar and Amberker, 2010a, b). Use texture, so, the resolution is good and use two level DWT to the input image, each resolution level has three new features which are chanel depth, horizontal and vertical. But without using attack type, the image may be distorted by the attack and without using sub band coefficient, this coefficients may modify by channel noise.

MATERIALS AND METHODS

Designing algorithm is concerned with how to design a suitable algorithm having the ability to hide watermark photo inside the original one by utilizing a wavelet transform algorithm as well as applying stenography issues based on that image by using a private sequence key.

The target image can be obtained from the database and any still image can be used in order to be protected by using the proposed methods. Analyzing and testing an image watermarking software on various numbers of photos and for comparing them positively on the same groups of sample photos that need to be utilized always become crucial processes. The signal processing viewed pictures as interesting and this involving size, brightness/contrast, synthetic, blur, textured/smooth zone, sharp with straight edges, etc. Moreover, a wide range of contents and types can be covered by them. It is indicated that getting a thorough list of picture's classes is impossible because stock photo companies experienced difficulties in setting up an accepted index. Nevertheless, it is possible to get back the principle themes that are at least popular among the most commonly used libraries in the press for keeping a wide range of pictures involving shapes, colors, lightning, patterns and textures.

It is pointed out that there are some image databases which have already been available for research concerning image processing. A good example of such database is the USC-SIPI Image Database in which the 'classics'; Lena, baboon, peppers, etc. are possible to be available. These databases are often utilized by researchers carrying out studies on digital watermarking. In fact, it is proved that copyright protection is viewed to be hypocritical to some extent several images from copyrighted material in the database are involved in process of scanning while the 'origin of many remains anonymous. Thus, in this study, a wide variety of other photographs were found, in addition to obtaining the authorization to utilize them freely in studies regarding watermarking involving publication in journals or proceedings as long as the photographer get a credit. Therefore, the database is separated into volumes based on the basic features of the pictures. In each volume, images have different sizes such as 256×256, 512×512 or 1024×1024 pixels. The black and white images take 8 bits/pixel while the color images take 24 bits/pixel.

Watermark Insertion: This approach has significantly attracted the attention of both industrial and academic fields. Digital watermarking techniques have been widely created for the purpose of having an efficient tool against plagiarism inappropriate utilization of image or illegal change of contents. However, the main restriction in image watermarking for a watermark embedded into the cover image is the robustness against manipulations involving varieties of analogy and digital processing operations. Moreover, another recognized constraint is keeping the perceptual similarity between the original, the embedding capacity and the watermarked images (Dharwadkar and Amberker, 2010a, b).

In cases of finding the signal that is large enough, these intervals can be divided evenly again and again. The original signal with a specific resolution or scale is represented by each iteration. The Haar wavelet's mother wavelet function ψ(t) can be indicated by Eq. 1 and 2 mentioned earlier (Fig. 1):

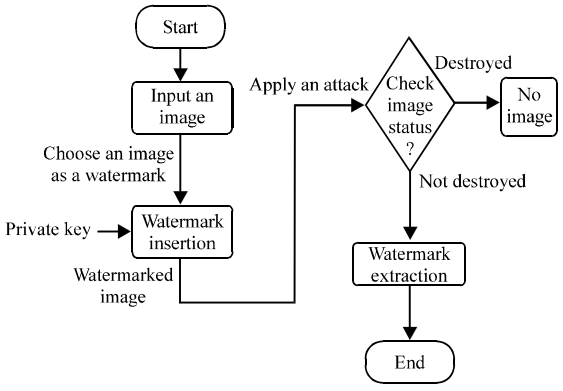


Fig 1: The flowchart of the entire methodology used in this research. On the left side, it shows watermark insertion and watermark extraction on the right side after applying the attack against the watermarked image. However, watermark insertion and extraction will be explained in details later in this

$$\Psi(t)=\begin{cases}1 & 0\le t<\frac{1}{2}\\ -1 & \\ 0 & \frac{1}{2}\le t<1\end{cases}$$

It's scaling function $\phi(t)$ can be indicated as:

$$\phi(t)=\begin{cases}1 & 0\le t<1\\ 0 & \text{Otherwise}\end{cases}$$

Algorithm 1:

Step 1: DWT is used to divide the grayscale cover image into 4 orthogonal multi-resolution sub-bands, i.e., LL1, HL1, LH1 and HH1. Choose LH1 for the next step. The DWT splits an image into diagonal (HH), vertical (LH) and horizontal (HL) detail components in addition to a lower resolution approximation image (LL)

Step 2: DWT is used again to sub-divide the sub-band LH1 and obtain smaller 4 sub-bands or LH2 at the second level and by choosing the LH2 sub-band. It is important to notice that other sub-band can be chosen and might lead to different results. As shown in Fig. 2

Step 3: LH2 is subdivided into 4×4 blocks

Step 4: (For DWT-DCT algorithm only), DCT transform is used at every block in the candidate sub-band

Step 5: The watermark is vectorized and re-formulated into zeros and ones

Step 6: Two different uncorrelated pseudorandom sequences is generated. The first sequence is utilized for embedding the watermark bit 0 (PN_0) while the rest of sequence is utilized for embedding the watermark bit 1 (PN_1). Each of these two pseudorandom sequences should have a number of elements that equal those of mid-band elements of the (DCT-transformed DWT sub-bands)

Step 7: The two produced uncorrelated pseudorandom sequences, PN_0 and PN_1 are added together with the aid of a gain factor k, inside the DCT converted 4×4 blocks that have been a candidate from the DWT sub-bands of the grey scale cover image. Embedding process is carried out on the DCT coefficients only on its middle band. If that D is indicated to be the middle band matrix of DCT coefficients, hence, the hiding operation can be given as followings: When 0 bit is given to the value of the watermark then:

$$D' = D + k * PN\_0 \quad (1)$$

where, k is a key.
Alternatively, when 1 bit is given to the value of the watermark then:

$$D' = D + k * PN\_1 \quad (2)$$

Step 8: Reformulate the watermarked image by applying inverse DCT (for the DWT-DCT algorithm) and applying inverse DWT. In other words, performing the inverse of all transforms that has applied in previous stepsdf

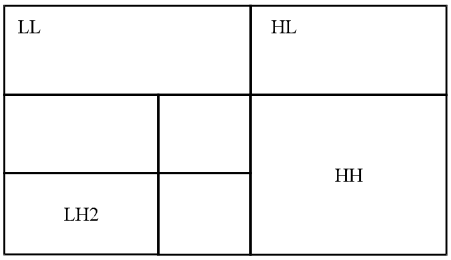


Fig. 2: Determining the sub-band LH2 using DWT

Watermark extraction: The ownership can be read from the original image. When some authority needs to extract the watermark image and find the original owner (of the original image). In this state, we need to use the wavelet transform techniques such as DWT and DWT-DCT. Those techniques can be used for the extraction of the watermark as follows.

Algorithm 2:

Step 1: Decomposing the attacked image into 4 orthogonal multi-resolution sub-bands which are HL1, HH1, LL1 and LH1 by applying DWT transform

Step 2: Applying DWT further to LH1 in order to obtain other smaller 4 sub-bands and selecting the sub-band of LH2

Step 3: Dividing the sub-band of the LH2 into 4×4 blocks

Step 4: Performing DCT transformation (for DWT-DCT) for each block in the candidate sub-band of LH2 with extracting the coefficients of the middle band for each block

Step 5: Two different uncorrelated pseudorandom sequences are generated again. Each of these two pseudorandom sequences should have a number of elements that equal to those of sub-bands of the mid-band of the DCT-transformed DWT. Moreover, the same seed that was utilized at the first place in the process of watermark embedding should be utilized for the Regeneration of the PN_0 and PN_1 (two pseudorandom sequences)

Step 6: For every block in the LH2 sub-band, perform calculations for the correlation between the two produced pseudorandom sequences (PN_0 and PN_1) and the coefficients of mid-band. The extracted watermark bit is considered 0 when the correlation with the PN_1 was lower than that with PN_0 if not, it is indicated to be 1

Step 7: Utilize the extracted bits to obtain the watermark, in addition to evaluating the robustness of the algorithm by determining the correlation between the original and expected watermark. Figure 3 and 4 demonstrates the original image (Lena) and original image watermark data (copyright) used in this study to prove the ownership image

Figure 5 shows that extracting watermark images by using DWT and DWT-DCT sequence, by using a secret key and using extract algorithm applied after the attack on the watermark image and that attack, do not effect on the ownership image.

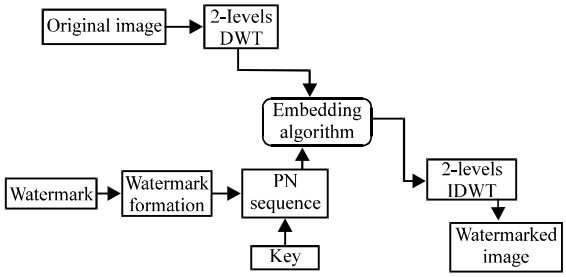


Fig 3: Explains how to embed watermark and key by using DWT and DWT-DCT algorithm with the original image. This algorithm could define embedding Algorithm. The same operation is done using DWT-DCT with performing DCT transform after DWT transform before embedding operation and IDCT after embedding operation

Fig. 4: Lena host image (original image+watermark)

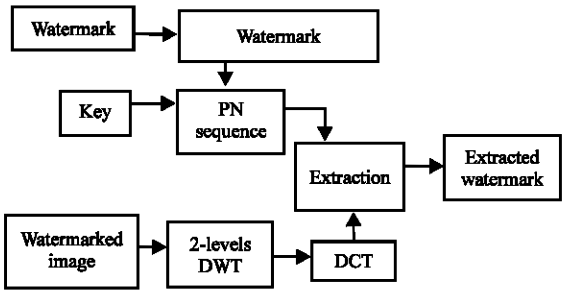


Fig. 5: Combined DWT-DCT watermark extraction procedures

The proposed algorithm is applied to a 512×512 image, 'Lena' as the cover image and 50×20 grayscale image as the watermark with the word "copyright" written in it.

Furthermore, the evaluation of any watermark algorithm is usually done with respect to imperceptibility which is the ability of the algorithm to keep the cover image undistorted and can be determined by utilizing the Peak Signal to Noise Ratio (PSNR). The other parameter that can be used to evaluate the watermark algorithm is the robustness which is the immunity of the watermark against different types of attacks. In this study, it will be shown that the algorithm is robust against few types of attacks such as gaussian noise, rotation, cropping, dithering and compression. These attacks are not frequently used in real life but they are representative and general, since, some of them are degrading attack, i.e., Gaussian noise or is dis-positioning geometrical attacks, i.e., cropping. Others are watermark removals such as compression which led to measure the similarity between the original grey scale watermark image and that extracted from the attacked grayscale still cover image by using the correlation. PSNR can be measured using the formula:

$$PSNR = 10.\log_{10}\left(\frac{MAX^2}{MSE}\right)$$

$$PSNR = 20.\log_{10}\left(\frac{MAX_I \text{ pixel value}}{\sqrt{MSE}}\right)$$

Where MSE is the Mean Square Error which isthe cumulative squared error between the original imageand modified one while PSNR is a measure of the peak error and MAX is the value of the maximum pixel. Correlation ρ can be obtained utilizing Eq. 2:

$$P(\omega,\hat{w}) = \frac{\sum_{i=1}^{N} \omega i \hat{w} i}{\sqrt{\sum_{i=1}^{N} \omega_i^2}\sqrt{\sum_{i=1}^{N} \hat{w}_i^2}}$$

where, ρ is the correlation of the embedded watermark w and extracted watermark w while N is the watermark image dimension.

RESULTS AND DISCUSSION

From the definition, the ability of the algorithm of keeping the cover image undistorted is known as the imperceptibility of the algorithm that can be measured by utilizing Peak Signal to Noise Ratio (PSNR). The original image, watermark and original image+watermark by using DWT are shown in Fig. 6 but the same images with the use of DWT_DCT transform are shown in Fig. 7.

By evaluating imperceptibility of the algorithm using DWT transform and DWT_DCT transform by measuring PSNR, DWT gave 80.128 while DWT_DCT gave 96.73. This indicates that improvement can be obtained using DWT_DCT.

Robustness: From the definition, robustness can be explained as the immunity of the watermark against different types of attacks and can be used to evaluate both algorithms, i.e. with DWT only and with DWT-DCT.

Robustness evaluation using DWT: Developed simulation is implemented to inspect the immunity of the algorithm against popular types of attack such as Gaussian noise, Rotation, Dithering, Compression and Cropping. Table 1 explains the immunity against Gaussian noise attack using DWT only. After many iterations, the algorithm shows good robustness against this type of attack. Attack factor refers to the degree of attack in other words, attack factor means how much the attack is affecting the watermark image. Wears, correlation refers to the correlation of the watermark before and after the attack is applied which is the mean that evaluates the robustness of the algorithm.The correlation function measures the correlation value compared with a detection threshold. Using that threshold value, the image is considered to be watermarked if the value of the correlation exceeds that of the threshold.

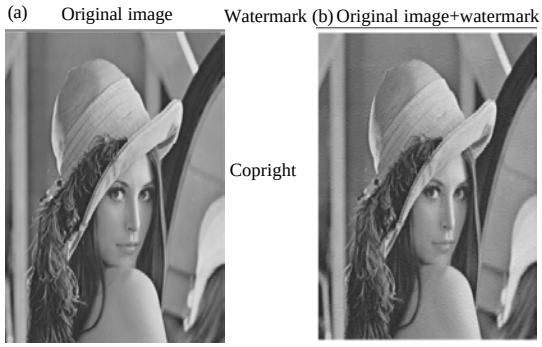


Fig. 6: Algorithm using (DWT) only: a) The (PSNR) = 80.128 and b) Computation time = 1.60

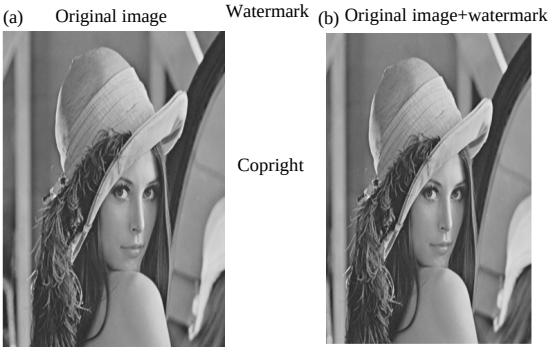


Fig. 7: Algorithm using joint between (DWT and DCT): a) The (PSNR) = 96.73 and b) Computation time = 1.108

Table 1: Robustness evaluation of DWT algorithm against gaussian noise attack

Type of attacks	Attacks factor	Correlation	Extracted watermark using DWT
Gaussian noise	0.1	0.70	
	0.2	0.70	
	0.4	0.64	
	0.6	0.52	
	0.8	0.46	

In rotation attack, the correlations of the original watermark and the extracted one were very degraded because of displacement process of the watermark points that done by the attack. However, correlation results show negative magnitude when the attack value is very high (Table 2). Under dithering attack, the algorithm survives to provide good results against this type of attacks.

In case of compression attack, an algorithm with DWT only shows stable results that make DWT the preferred transform to be used with that type of attacks, since, the watermark can be extracted and gives the desired correlation result verses compression attack (Table 3 and 4).

The robustness against cropping attack is suffering from taking parts away from the cover image.

Table 2: Robustness evaluation of DWT algorithm against rotation attack

Type of attacks	Attacks factor	Correlation	Extracted watermark using DWT
Rotation	30	0.01	
	60	0.006	
	90	-0.006	
	180	-0.02	

Table 3: Robustness evaluation of DWT algorithm against dithering attack

Type of attacks	Attacks factor	Correlation	Extracted watermark
Dithering	5	0.707	
	10	0.709	
	12	0.660	
	14	0.660	

Nevertheless, correlation results still promising and the algorithm retains robust and stable. It is better to put the watermark in an important place in the cover image to avoid the possibility of taking the watermark away under cropping process (Table 5).

Robustness evaluation using DWT_DCT: DWT_DCT algorithm cut boundary frequencies (high frequency and low frequency) and take a medium frequency of the image and DWT_DCT includes the fact that the utilisations of frequency transform are common in image compression.

As the situation with DWT, DWT-DCT algorithm suffers a great degradation under rotation attack for the same reason of changing the place of watermark points.

Table 4: Robustness evaluation of DWT algorithm against compression attack

Type of attacks	Attacks factor	Correlation	Extracted watermark using DWT
Compression	20	0.687	
	40	0.687	
	60	0.70	
	80	0.698	

Table 5: Robustness evaluation of DWT algorithm against cropping attack

Type of attacks	Attacks factor	Correlation	Extracted watermark using DWT
Cropping	50	0.71	
	100	0.66	
	150	0.61	
	200	0.51	

For that reason, preprocessing operation is needed for the cover image to rearrange the image before the extracting process (Table 6).

In case of dithering, DWT with DCT shows great improvement and provide better immunity against this type of attacks comparing with DWT only which makes it more desirable for this type of attacks, since, it provides clear extracted watermark (Table 7).

Table 6: Robustness evaluation of DWT_DCT algorithm against gaussian noise attack

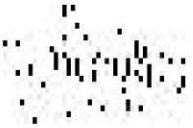
Type of attacks	Attacks factor	Correlation	Extracted watermark using DWT_DCT
Gaussin noise	0.1	0.9700	
	0.2	0.9600	
	0.4	0.8200	
	0.6	0.6000	
	0.8	0.4257	

Table 7: Robustness evaluation of DWT_DCT algorithm against rotation attack

Type of attacks	Attacks factor	Correlation	Extracted watermark using DWT_DCT
Rotation	30	0.010	
	60	0.006	
	90	-0.006	
	180	-0.020	

Table 8: Robustness evaluation of DWT_DCT algorithm against dithering attack

Type of attacks	Attacks factor	Correlation	Extracted watermark using DWT-DCT
Dithering	5	0.98	
	10	0.97	
	12	0.86	
	14	0.86	

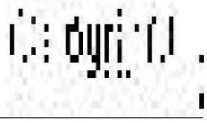
Table 9: Robustness evaluation of DWT_DCT algorithm against compression attack

Type of attacks	Attacks factor	Correlation	Extracted watermark using DWT_DCT
Comression	20	0.0109	
	40	0.062	
	60	0.068	
	80	0.40	

Expectedly, the extracted watermark faces huge loss under compression attack. The mother of fact is that compression is using DCT transform which makes it difficult for DWT_DCT to provide good results (Table 8).

Finally, DWT_DCT shows better immunity against cropping attack and the extracted watermark appears clearly with the unnoticed loss which makes secured and desirable for this type of attack (Table 9 and 10).

Table 10: Robustness evaluation of DWT-DCT algorithm against cropping attack

Type of attacks	Attacks factor	Correlation	Extracted watermark using DWT_DCT
Cropping	50	0.96	
	100	0.93	
	150	0.86	
	200	0.65	

CONCLUSION

In the digital world, there are many techniques that are used to transfer data between two entities but the main problem is how to send data in a secure environment. Digital images are widely used and must create a secure algorithm to protect it from any attack. Watermarking is one of the security techniques that are used to send an image in secure space. In this study, the design algorithm is related to watermark and by using DWT and DWT_DCT to keep ownership rights by hiding ownership image in other image and keeping them safe from any type attack of.

REFERENCES

Dharwadkar, N.V. and B.B. Amberker, 2010a. An efficient non-blind watermarking scheme for color images using discrete wavelet transformation. Intl. J. Comput. Appl., 2: 60-66.

Dharwadkar, N.V. and B.B. Amberker, 2010b. Watermarking scheme for color images using wavelet and transform based texture properties and secret sharing. Intl. J. Signal Process., 6: 93-100.

Hemalatha, R.K. and P. Maneesha, 2016. Unified embedding method for color image steganography. Proceedings of the International Conference on Information Communication and Embedded Systems (ICICES), February 25-26, 2016, IEEE, Chennai, India, ISBN:978-1-5090-2553-4, pp: 1-5.

Jafri, S.A.R. and S. Baqai, 2007. Robust digital watermarking for wavelet-based compression. Proceedings of the 9th IEEE International Workshop on Multimedia Signal Processing (MMSP'07), October 1-3, 2007, IEEE, Crete, Greece, ISBN:978-1-4244-1273-0, pp: 377-380.

Jiansheng, M., L. Sukang and T. Xiaomei, 2009. A digital watermarking algorithm based on DCT and DWT. Proceedings of the International Symposium on Web Information Systems and Applications, May 22-24, 2009, Academy Publisher, Guwahati, India, ISBN: 978-952-5726-00-8, pp: 104-107.

Lumini, A. and D. Maio, 2001. Approach to Digital Image Watermark. University of Bologna, Bologna, Italy.

Mohanty, S.P., P. Guturu, E. Kougianos and N. Pati, 2006. A novel invisible color image watermarking scheme using image adaptive watermark creation and robust insertion-extraction. Proceedings of the 8th IEEE International Symposium on Multimedia (ISM'06), December 11-13, 2006, IEEE, San Diego, California, USA., pp: 153-160.

Nguyen, T., S. Lam and M. Hoffman, 2009. Watermarking for authentication and verification. MSc Thesis, The University of California, California, USA.

Terzija, N., 2006. Robust digital image watermarking algorithms for copyright protection. PhD Thesis, University of Duisburg-Essen, Germany.

Yu, Y., R.A. Shenoi, H. Zhu and L. Xia, 2006. Using wavelet transforms to analyze nonlinear ship rolling and heave-roll coupling. Ocean Eng., 33: 912-926.