Implementation of Wavelet Based Modified Buyer-Seller Watermarking Protocol (BSWP)

Ashwani Kumar*, S.P Ghrera**, Vipin Tyagi***
* Research Scholar **Prof. in CSE
Jaypee University of Information Technology, Waknaghat, Solan (HP) – INDIA
*** Prof. in CSE, Jaypee University of Engineering and technology, Raghogarh, Guna (MP) – INDIA

Abstract: - Wavelet based watermarking is a promising technology for embedding the information as an unperceivable signal into the digital contents. The main characteristics of wavelet are wavelets' excellent spatial localization and multi-resolution. Wavelet based modified buyer-seller watermarking protocols integrate multimedia, watermarking techniques, fingerprinting and cryptography for copyright protection, piracy tracing, and privacy protection of the digital content. In this paper we have implemented the wavelet based modified buyer-seller watermarking protocol. Our protocol focuses on managing the watermark. A binary watermarked image that is a logo is embedded in certain selected sub-bands of a 3-level DWT transformed of the original image. Then, the DWT sub - band is computed and the sequences of the watermark bits are embedded in the coefficients of the high frequency sub-bands. The quality of the watermarked image generated with wavelet based method is better, using the same watermark strength. To check the imperceptibility and robustness of the watermarked image, PSNR and NCC parameters are used. Furthermore the algorithm is robust against the various attacks such as JPEG Compression, Rotation, Gaussian Noise, Median Filter and Salt & Pepper Noise.

Key-Words: - Copyright Protection; Wavelet Transform; Fingerprinting; Cryptography;

1 Introduction

The rapid growth of computer networks increased use of multimedia data via the internet have resulted in fast and convenient exchange of digital information. Copyright marking [1] is a relatively a new technique for hiding information in multimedia content with the aim of tracing any traitor who redistributes the digital content illegally. Digital watermarking [2] has been proposed, complementing encryption techniques, to establish and prove ownership rights by embedding the seller’s information in the redistributed digital content. Digital multimedia has become innovative in the field of internet application and data securities because copyright protection and data integrity detection has become a vast concern. This technology works well and uses suitable tools to identify the source of the content, creator of the content, the owner of the content, distributor of the content or unauthorized consumer of a digital content such as document, image, video and audios.

The wavelet based modified buyer-seller watermarking protocol is one that combines encryption, digital watermarking, and other techniques to ensure rights protection for both the buyer and the seller in e-commerce. The first known buyer-seller watermark protocol was introduced by Memon et al. [3], and it was improved by Ju et al. [4]. Since the first introduction of the concept, several alternative design solutions have been proposed in [5, 6, 7, & 8]. In general the watermark is two types i.e. visible or invisible. A visible watermark typically consists of visible text message or a company logo indicating the ownership of the digital content. In contrast invisible watermarked content appears identical to the original. The only way to find out the existence of the invisible watermark is to examine the digital content with appropriate watermark detection and extraction algorithms.

The wavelet based modified buyer-seller watermarking protocol involves three steps. First, a seller embeds a watermark [9] that identifies the buyer into a digital product, such as a digital image. Second when a pirated copy is found by the unauthorized person the seller will detect the watermark of the pirated copy. At last, once the watermark of a specific buyer is identified, the seller will take the case to a court. Digital watermarking can be applied in the spatial and transform domains to achieve robustness and imperceptibility. Spatial domain techniques are easier to implement, but lacks in robustness, while transforming domain techniques embed the watermark in the host’s transform domain, are more sophisticated, robust and getting popularity when compared to spatial domain techniques [11]. The development of spatial domain techniques due to their weakness in robustness is generally not chosen by the researcher and the frequency domain algorithm [12] based on DCT or DWT is the focus of research. There are requirements and constraints in design effective watermarking algorithms the three fundamental areas are.

- **Imperceptibility:** Imperceptibility means the difference between the watermarked image and the original image should not noticeable by human eyes or the human vision system.
- **Robustness:** The ability of watermark to survive under normal image processing of digital content. The embedded watermark should survive after a number of common image processing operations such as cropping, scaling and lossy compression.
- **Capacity:** Capacity means the amount of information which we can embed into the original image, or you can say capacity is the number of bits embedded into the original image.

Digital watermarking [13] is a promising technology employed by various digital rights management (DRM) systems to achieve digital rights. Wavelet based watermarking techniques are gaining more popularity because DWT has a number of advantages over other transform such as it contain progressive low bit-rate transmission and quality scalability characteristics. A buyer-seller watermarking protocol is expected to solve the problems in [10, 14, 15].

The remainder of this paper is organized as follows. In the section II we have shown related work. Section III presented our work that is wavelet based modified buyer-seller watermarking protocol (BSWP). Section IV discussed the result analysis. Finally, section V provides the conclusion of this research paper.

2 Related Work

The possible solution for e-distribution of digital rights is based on a unique watermark for a transaction between seller and buyer. This has come to be known as buyer seller watermarking protocol. Since its inception in [16] many variants have been proposed. There are many buyer seller watermarking protocols which have been proposed using cryptography techniques. Qiao and Nahrstedt [16] first pointed out the customer’s rights problem in the watermarking protocols for piracy tracing. However their scheme is symmetric and doesn’t guarantee the buyer’s security. The intuitive idea of watermark-based fingerprinting has been implemented by a number of schemes using cryptographic techniques before the customer’s right problem was first identified in [5]. Recent researches show that a secure buyer seller watermarking protocol is protecting the participants’ digital content during transaction using digital watermarking technique and a public key cryptosystem.

However, DWT [17] has been used more frequently in digital image watermarking due to its time/frequency decomposition characteristics, which resemble to the theoretical models of the human visual system [18]. Ramin Eslami and Hayder Radha propose a new image coding scheme based on the proposed transform, the wavelet-based contourlet transform (WBCT) [20]. P. Kumhom et. al.’s proposed method is based on the wavelet packet transformation with the best basis [21] resulting from an entropy-based algorithm. We have implemented a wavelet based modified buyer seller watermarking protocol to fulfill the design requirements, different from the predecessors, our approach makes improvements in the many aspects such as anonymous communication between buyer and seller, and it supports multi-transaction and dispute resolution and avoid double watermark insertion. The protocol is based on public key encryption standard.

3 Wavelet based Modified Buyer Seller Watermarking Protocol (BSWP)

In our protocol we have used wavelets to provide more security for the buyer and the seller during the transmission of digital content. Our protocol focuses on managing the watermarks we do not design new method but simply use wavelets for embedding the watermarks. The trust model of our protocol is same as in [3, 7]. Here, we assure that our protocol is more robust and imperceptible compare to other previous protocol, because it uses wavelet special properties. In this wavelet based buyer seller watermarking protocol the seller provides the watermark embedding operation and sells the watermarked product to the buyer. The WCA device is integrated into the seller's computer system and it will generate the watermark with the help of DWT for the buyer. We have assumed that every seller in a transaction has unique watermarking embedded function algorithm in their software and all messages are transferred in a secure manner and digital content is still image. Discrete wavelet transforms (DWT) [9, 22, 23, 24, 25] is a signal analytic theory that can localize the signal in spatiotemporal.

We have modified the existing algorithm proposed by Corina Nafornita [19] for embedding the watermarks the algorithms used to embed the watermark in the high frequency sub-bands i.e. HL, LH and HH because they show better results in terms of imperceptibility. In our approach we have chosen high frequency selected sub-bands i.e. HL and LH this reduces the area of embedding the watermark leads in great robustness, imperceptibility and minimize the effect of various attacks. We have compared our approach with Corina Nafornita [19] and shows that the approach contains better result. Embedding of the watermark multiple times into the host image makes the scheme more robust.

3.1 Watermark Embedding Scheme

Let I be the original gray-level image and the watermark W an original watermark image. We start the watermarking process by applying 3-level DWT to the original image. Many DWT-based watermarking algorithms used to embed the watermark in the high frequency sub-bands i.e. HL, LH and HH because they show better results in terms of imperceptibility. But in this paper we embed the watermark into high frequency selected sub-bands i.e. HL and LH this reduces the area of embedding the watermark leads in great robustness as well. The watermark is repeatedly embedded of M >>1 times in the transform image. Since the watermark is embedded multiple times in every detail sub-band, this can be viewed as a form of transmitting the watermark in different sub-channels. It has been shown by Kundur et al. In [27] those diversity techniques can give very good results in detecting the watermark because that many watermark attacks are more appropriately modeled as fading like. Each repetition is denoted by W_r with r = 1, 2, M. The basic steps for embedding the watermark are given below.

Step 1: Perform 3-level DWT to the original image I. The original image is decomposed into 4 sub domains as HH, HL, LH, LL for 1-level DWT according to different frequency of the original image.

$$Y = DWT\,(I) = \{LL_L, HL_L, LH_L, HH_L, HL_{L-1}, .., HH_1\}$$

Step 2: Select HL_3 and LH_3 high frequency sub-bands of the original image I for embedding the watermark.

Step 3: Compute the threshold for each selected sub-band HL_3 and LH_3. Let the approximation coefficients be $a(m,,n)$ and the detail coefficients from the resolution level l and sub-band s be $d_{s,l}(m,n)$, where s Є {HL, LH} and l Є {1,…,L}. The threshold is computed using equation no. (1).

$$T_{s,l} = q_1\, max_{m,n}\{d_{s,l}(m.n)\} \tag{1}$$

Step 4: Let W of size 128×128 an original watermark image after applying 3-level DWT we get HL_3 and LH_3 high frequency sub-bands. For each sub-band that is HL_3, LH_3, if the detail coefficient is higher or equal to the above computed threshold, embed the watermark using the equation no. (2)

$$d^{w}_{s,l}(m,n) = d_{s,l}(m,n)[1 + \alpha w_r(i)] \tag{2}$$

Where α is a parameter used to control the level of the watermark.

Step 5: Repeat previous step M times, until every selected coefficient has been watermarked.

Step 6: Compute the IDWT from these new coefficients. We obtain the watermarked imageIw.

Step 7: Reshaping the decomposed image back to its normal dimension.

Step 8: Write the watermarked image to a file and display it

3.2 Watermark Extraction Scheme

The extraction process requires the original image I, or at least some significant vector extracted from the DWT of the cover work, specifically, the detail coefficients with a value above the computed threshold. The basic steps for extracting the watermark are given below.

Step 1: Perform 3-level DWT on the watermarked imageIw to decompose it into four non-overlapping multi-resolution coefficient sets: LL_3, HL_3, LH_3 and HH_3.

Step2: Select HL_3 and LH_3 high frequency selective sub-bands of the watermarked imageIw.

Step3: Determine the size of the wavelet coefficients $d_{筰,l}(m,n)$.

Step4: The estimate of each repetition of the watermark W from the watermarked and possibly distorted work $I^w$is extracted using the wavelet coefficients $d_{s,l}(m,n)$ that should contain a watermark bit.

$$w_r(i) = sgn\left(\frac{d^{\wedge}{}_{s,l}(m,n) - d_{s,l}(m,n)}{d_{s,l}(m,n)}\right)$$

The random guess is made, for the watermarked bit in the location (m,n) if $d^{\wedge}{}_{s,l}(m,n) = d_{s,l}(m,n)$ or if $d_{s,l}(m,n)$= 0.

Step 5: The original watermark is estimated from its repetitions using the majority rule i.e. the most common bit value is assigned for the recovered watermark bit.

Step 6: The watermark is reconstructed using the extracted watermark bits, and compute the similarity between the original and extracted watermarks.

4 Result Analysis

In this first section we have given the various parameters through which we can analyze the performance of the protocol. These parameters are PSNR, MSE and NC measurements.

4.1 Peak Signal-To-Noise Ratio (PSNR)

Peak Signal-To-Noise Ratio is generally used to analyze quality of image. It also describes how far two images are equal. PSNR is measuring the quality of the watermarked image by calculating the distortion between the watermarked and original image. In order to analysis the quality of the extracted watermark image and original watermarked image both subjective and objective measurements are used. For that we have used equation no. (3) and (4).

$$PSNR = 10 * \log\frac{255^2}{MSE} \qquad (3)$$

4.2 Mean Square Error (MSE)

The MSE represents the cumulative squared error between the compressed image and the original image. To compute the PSNR, first calculates the mean-squared error (MSE) using the following equation:

$$\mathrm{MSE} = \sum_{i=1}^{x} \sum_{j=1}^{y} \frac{(|A_{i,j} - B_{i,j}|)^2}{x * y} \qquad (4)$$

Where x is width of the image and y is height and $x * y$ is the no. of pixels.

4.3 Normalized Correlation Coefficient (NCC)

Normalized Correlation Coefficient is used for evaluating the robustness of the algorithm. For m × n greyscale image, the NC is defined as follow:

$$NC = \frac{\sum_{i=1}^{m} \sum_{j=1}^{n} A_{i,j} B_{i,j}}{\sum_{i=1}^{m} \sum_{j=1}^{n} A_{ij}^2} \qquad (5)$$

Where $A_{i,j}$ and $B_{i,j}$denote the pixel values in row i and line j of the original watermark and the exacted watermark respectively.

Here we have shown the various results of wavelet based modified buyer seller watermarking protocol. As we know from the previous section [28] the details of the image such as edges and textures are well confined into the HH, LH, and HL sub-bands of the DWT of the image. We chose only HL_3 and LH_3 sub-bands of the image of the watermarking process. The DWT based algorithm is tested for the various original and watermark images. Some results are given to evaluate the performance of the method. We have calculated PSNR and NCC values for that. The images Lena, Cameramen, Baboon and House are presented in Fig. 1. The presented method is implemented using MATLAB.

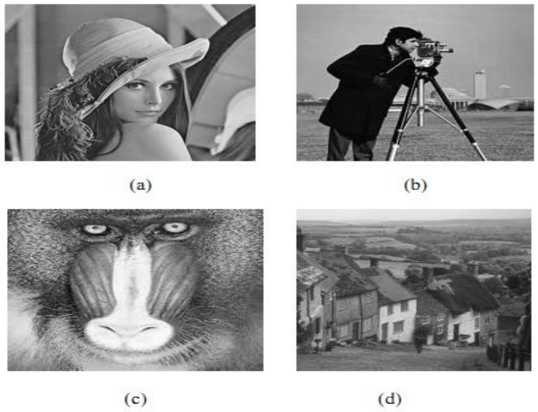


Fig .1 Original images used for simulations: Lena (a), Cameramen (b), Baboon (c) and House (d).

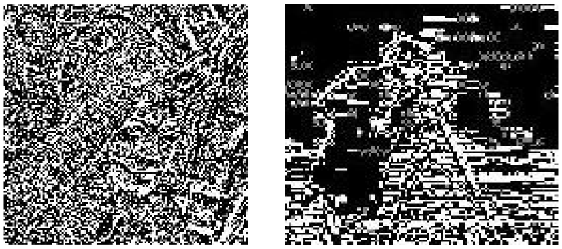
The watermark was an original binary gray scale JUIT logo. The Daubechies 10pt wavelet was used to produce the wavelet coefficients. The following parameters were used, number of resolution levels L = 3, the strength of the watermark α = 0.1, and we chose only HL_3 and LH_3 high frequency sub-bands for embedding the watermark. The performances of the protocol [29, 19] are compared with the results of the method proposed by Cox in [2]. The watermarked images using the our protocol were not significantly distorted from the originals, whereas for the method presented by Cox et al. the difference was clearly visible, even upsetting. Table 1 contains the values of PSNR for each image and used watermark embedding coefficient α= 0.01.

Table 1PSNR [dB] values as a measure of the noise introduced by the watermark.

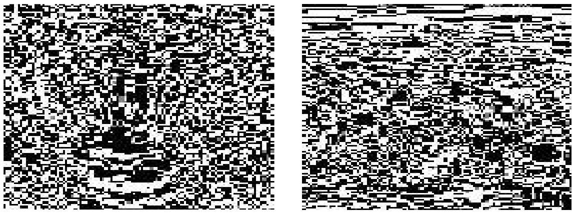
PSNR Image	Our Method	C. Nafornita' Method	Cox's Method
Lena	46.33dB	45.39dB	27.19 dB
Cameraman	44.55 dB	43.35 dB	25.35 dB
Baboon	45.39dB	44.18dB	26.44 dB
House	45.67 dB	45.35 dB	25.75 dB

Table 1

From the Table 1, we can see that the performance of our algorithm i.e. wavelet based buyer seller watermarking protocol, is better than pervious Cox's method [2] and C. Nafornita' method [19]. The difference between the watermarked and the original image is presented in Fig. 2 (a) to (d). From the difference images, it is clear that the watermark was embedded in the edges and textures. For instance, for the Lena image, the watermark affects the details such as the feathers of the hat. It has been demonstrated on four different images that the watermarking process has clearly not affected their visual quality. Further, the robustness of the protocol scheme is analyzed. The extraction of the watermark is made in two ways as from all levels, using a majority and from the coarsest level only.



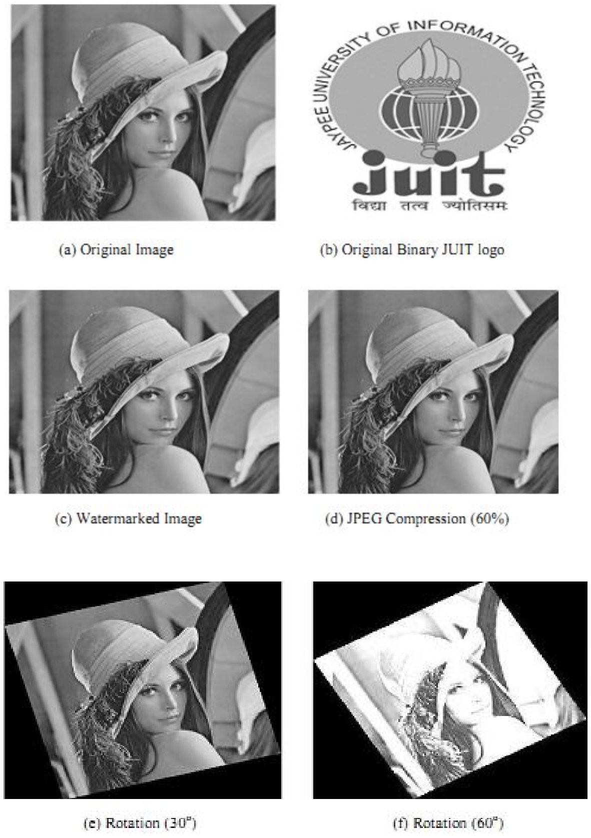
(a) (b)



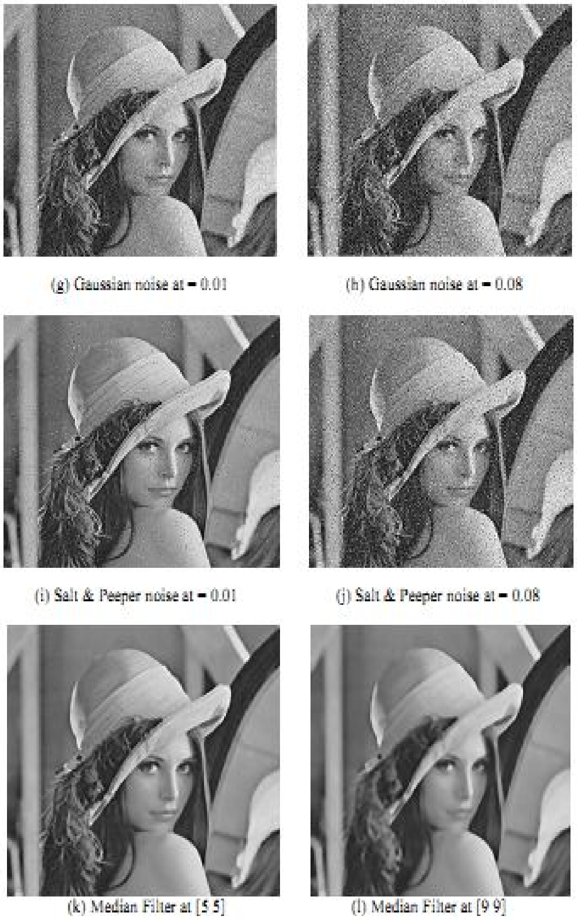
(c) (d)

Fig. 2 Difference images between watermarked image and original image, for Lena (a), Cameraman (b), Baboon (c), and House (d), respectively, for the presented method [29].

Here we have given the results of our method against the various types of attacks. We have compared our result with the results of the method proposed by Ben Wang in [30]. For instance, we have taken only the Lena image for producing our result. So we have taken of 512 × 512 8bit grayscale image Lena image and 128 × 128 8-bit grayscale watermark original binary JUIT logo. The embedding coefficient α= 0.01. The robustness are tested under 5 types of attacks i.e. JPEG Compression, Rotation, Gaussian noise, Salt & Peeper noise and median filter. The images with attacks are shown in Figure 3.



(a) Original Image
(b) Original Binary JUIT logo
(c) Watermarked Image
(d) JPEG Compression (60%)
(e) Rotation (30°)
(f) Rotation (60°)



(g) Gaussian noise at = 0.01

(h) Gaussian noise at = 0.08

(i) Salt & Peeper noise at = 0.01

(j) Salt & Peeper noise at = 0.08

(k) Median Filter at [5 5]

(l) Median Filter at [9 9]

Fig. 3 Images with various types of attacks.

The watermarks extracted from the images above are shown correspondingly in Figure 4.

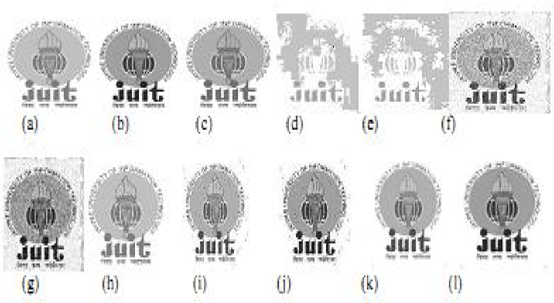
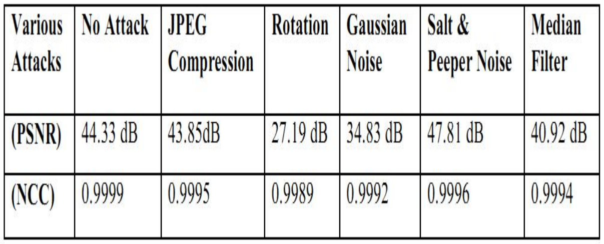


Fig. 4 Watermarks extracted from the attacked Images.

Table 2 shows the corresponding PSNR and NCC measurement of wavelet based modified buyer-seller watermarking protocol.

Table 2. The corresponding PSNR and NCC values of the algorithms.



Various Attacks	No Attack	JPEG Compression	Rotation	Gaussian Noise	Salt & Peeper Noise	Median Filter
(PSNR)	44.33 dB	43.85dB	27.19 dB	34.83 dB	47.81 dB	40.92 dB
(NCC)	0.9999	0.9995	0.9989	0.9992	0.9996	0.9994

Table 2

The Table 2 shows that the algorithm has great robustness against the various types of attacks. Salt & Peeper noise gives very impressive results. Additional, the watermarking algorithm is robust to most of the image processing attacks. Thus the watermarking algorithm can be used for protecting the copyrights of digital content.

Figure 4 (a) to (c) shows the detector's response to the watermarked Lena image under several types of attacks, which is very similar to Cox [2] and C. Nafornita [19] results. We have compared [2, 19] with our BSWP on the same set of test data. If we set the threshold value in the detection process at 0.5 we have the followings.

Median filter attack: For Lena watermarked images, the attack by median filtering with filter size larger than M=5 leads to a correlation smaller than 0.7. When we increase filter size M=9 leads a correlation smaller than 0.6. In fact only the detector C. Nafornita allows filtering with filter size M=5.

Salt & Peeper Noise: For Lena watermarked images, the attack by salt & peeper noise at=.01. The detector response in the BSWP method is above 0.5, having a considerably better performance than the detectors C. Nafornita and Cox et al. method. When we apply salt & peeper noise attack at=.08 the performance of our method is less than 0.5 but better when compare other two.

Gaussian Noise: For Lena watermarked images, the attack by Gaussian noise at=.01. The correlation coefficient is smaller than 0.7 when compared to detector response C. Nafornita and Cox. When we apply Gaussian noise attack at=.08 leads correlation coefficient is smaller than 0.5.

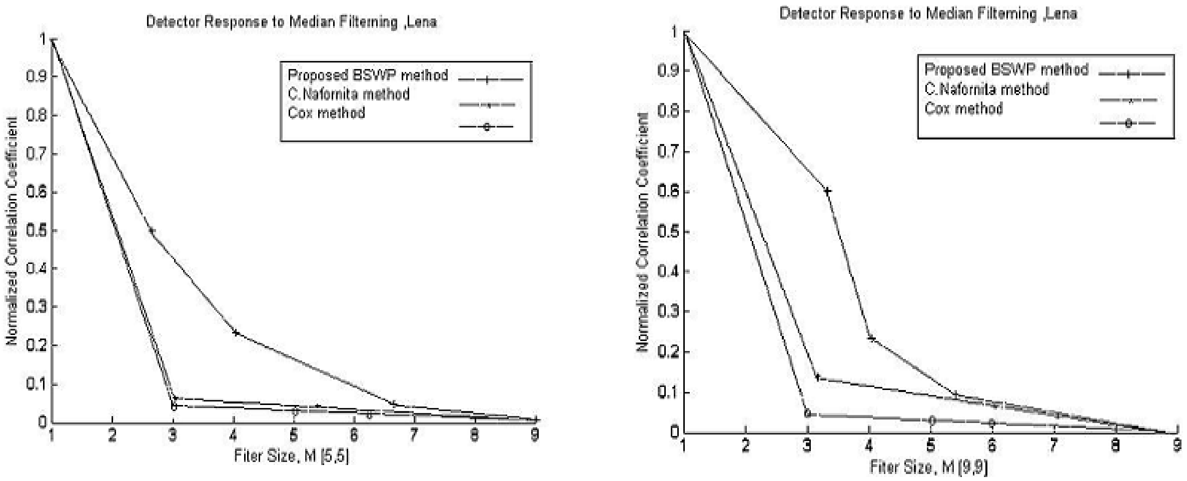


Fig. 4 (a) The detector's response to the watermarked Lena image under Median Filtering attack when filter size M=5 and M=9.

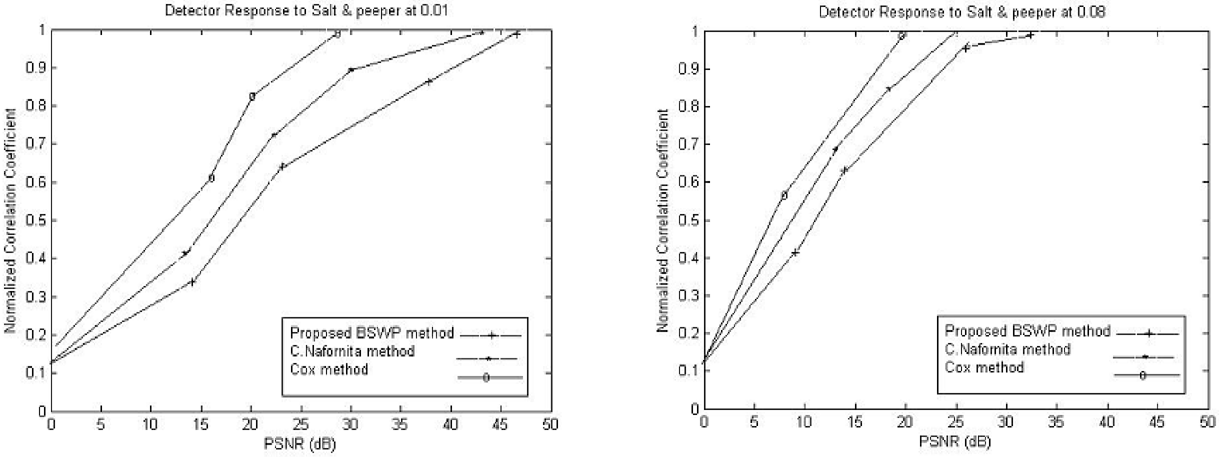


Fig. 4 (b) The detector's response to the watermarked Lena image under Salt & Peeper noise at=0.1. and at=0.8.

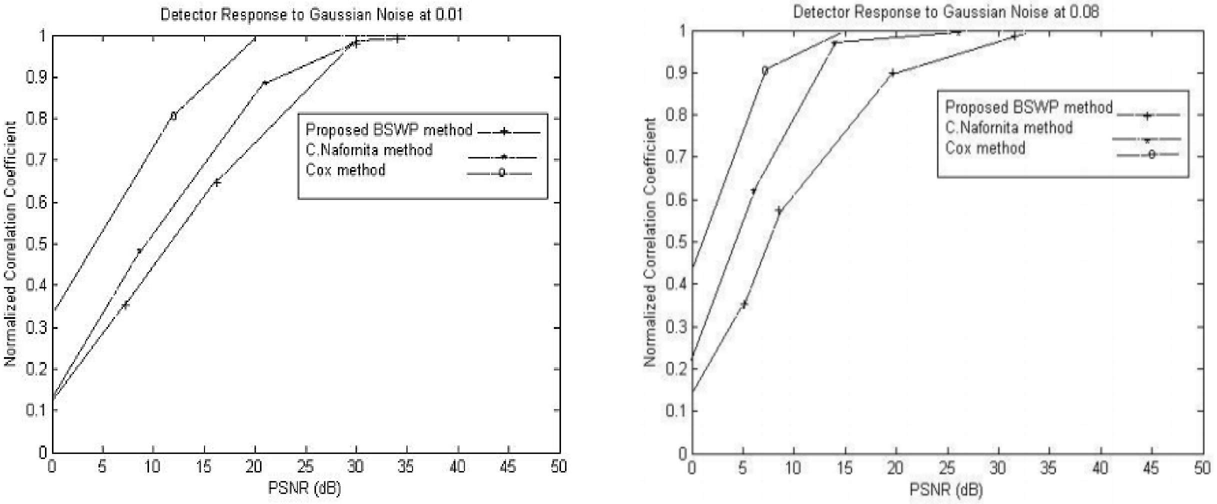


Fig.4 (c) The detector's response to the watermarked Lena image under Gaussian noise at=0.1. and at=0.8.

5 Conclusion

In this paper a wavelet based modified buyer-seller watermarking protocol (BSWP) is implemented. The wavelet-based watermarking method that embeds the watermark in coefficients selected in such a manner that the visible impact on a human observer is not very high. By embedding the watermark bits into the edges and textures i.e. HL_3 and LH_3 sub-bands of the image we make use of the human visual system. Our method is also image dependant. It is clarified that the wavelet based transform such as DWT, is better than other transform in terms of imperceptibility, robustness and capacity. DWT may have a positive impact on the performance of the watermarking system. The protocol focuses on managing the watermarks we do not design new method but simply use wavelets for embedding the watermarks. In this paper watermarking is done by embedding the watermark in the special high frequency selective sub-bands of 3-levels DWT transformed of an original image. Implementation results show that the imperceptibility of the watermarked image is acceptable. The security of this protocol is depending upon the embedding and extraction of watermark.

References:

[1] F. Mintzer and G. W. Braudaway, "If one watermark is good, are more better?" IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP ’99), vol. 4, Phoenix, Ariz, USA, pp. 2067–2069, 1999.

[2] I. J. Cox, J. Kilian and T. Shamoon, "Secure spread spectrum watermaking for multimedia," IEEE Transaction of Image Processing, vol. 6, no. 12, pp. 1673-1687, IEEE Computer Society, 1997.

[3] N. D. Memon and P. W. Wong, "A buyer-seller watermarking protocol," IEEE Transactions on Image Processing, vol. 10, no. 4, pp. 643-649, 2001.

[4] H.-S. Ju, H.-J. Kim, D.-H. Lee, and J.-I. Lim, "An anonymous buyer-seller watermarking protocol with anonymity control," Information Security and Cryptology - ICISC, pp. 421-432, 2002.

[5] J.-H. P. Jae-Gwi Choi, Kouichi Sakurai, "Does it need trusted third party? Design of buyer-seller watermarking protocol without trusted third party," Cryptography and Network Security, LNCS 2846, pp. 265-279, 2003.

[6] B.-M. Goi, R. C.-W. Phan, Y. Yang, F. Bao, R. H. Deng, and M. U. Siddiqi, "Cryptanalysis of two anonymous buyer seller watermarking protocols and an improvement for true anonymity," Cryptography and Network Security, LNCS 2587, pp. 369-382, 2004.

[7] C.-L. Lei, P.-L. Yu, P.-L. Tsai, and M.-H. Chan, "An efficient and anonymous buyer-seller watermarking protocol," IEEE Transactions on Image Processing, vol. 13, no. 12, pp. 1618-1626, 2004.

[8] J. Zhang, W. Kou, and K. Fan, "Secure buyer-seller watermarking protocol," In IEEE Proceedings Information Security, pp. 15-18, 2006.

[9] Ashwani Kumar, Vipin Tyagi, Mohd Dilshad Ansari, Kapil Kumar, "A practical buyer-seller watermarking protocol based on discrete wavelet transform." International Journal of Computer Applications, vol. 20, no. 8, pp. 46-51, 2011.

[10] Ashwani Kumar, Mohd Dilshad Ansari, Jabir Ali, Kapil Kumar, "A new buyer-seller watermarking protocol with discrete cosine transform." CNC, CCIS 142, pp. 468-471, 2011.

[11] Potdar, V., S. Han and E. Chang, "A survey of digital image watermarking techniques," in Proc. of the IEEE International Conference on Industrial Informatics, pp. 709-716, 2005.

[12] Chan, C. and L. Cheng, "Hiding data in Images by simple LSB substitution," Pattern Recognition, vol. 37, no. 3, pp. 469-474, 2004.

[13] Tyagi, Vipin, and J. P. Agarwal. "Digital Watermarking." Computer Society of India (26.09. 2008) (2008).

[14] Mina Deng, Bart Preneel, "On secure and anonymous buyer-seller watermarking protocol," Third International Conference on Internet and Web Applications and Services, pp. 524-529, 2008.

[15] P. W. Wong and N. Memon, "Secret and public key image watermarking schemes for image authentication and ownership verification," IEEE Transactions on Image Processing, vol. 10, no. 10, pp. 1593–1601, 2001.

[16] Jung-Chun Liu, Chu-Hsing Lin, and Li-Ching Kuo” A robust full band image watermarking scheme” Proceedings on IEEE, 2006.

[17] Tay, P. and J. Havlicek, "Image watermarking using wavelets," in Proc. of the IEEE Midwest

Symposium on Circuits and Systems, pp. 258-261, 2002.

[18] Wolfgang, R., C. Podilchuk and E. Delp, "Perceptual watermarks for digital images and video," Proc. of the IEEE, vol. 87, no. 7, pp. 1108-1126, 1999.

[19] Corina Nafornita, "Digital watermarking in the wavelet domain."

[20] Ramin Eslami and Hayder Radha, "Wavelet-based contourlet transform and its application to image coding," in Proceedings of the IEEE International Conference on Image Processing (ICIP'04), IEEE Signal Processing Society, pp. 3189–3192, 2004.

[21] P kumhom,son-bit,k chamnongthail, "Image watermarking based on wavelet packet transform with best tree," Ecti Transactions on Electrical-eng, Electronics, and Communications, vol. 2, no. 1, pp. 23-35, 2004.

[22] Jung-Chun Liu, Chu-Hsing Lin, and Li-Ching Kuo" A robust full band image watermarking scheme" Proceedings on IEEE .2006.

[23] X. G. Xia, C. G. Boncelet, G. R. Arce, "A multiresolution watermark for digital images," Image Processing Proceedings. International Conference, vol. 1 pp. 548–551, 1997.

[24] M. Kutter, S. K. Bhattacharjee, T. Ebrahimi, "Towards second generation watermarking scheme," Image Processing, ICIP 99. Proceedings, vol. 1 pp. 320–323, 1999.

[25] Ali Al-Haj, "Combined DWT-DCT digital image watermarking," Journal of computer science, vol. 3, no .9, pp. 740-746, 2007.

[26] Saied Amirgholipour Kasmani, Ahmadreza Naghsh-Nilchi, "A new robust digital image watermarking technique based on Joint DWT-DCT transformation," Third International Conference on Convergence and Hybrid Information Technology, pp. 42-54, 2008.

[27] D. Kundur, D. Hatzinakos, "Diversity and attack characterization for improved robust watermarking," IEEE Transactions on Signal Processing, vol. 49, no. 10, pp. 2383-2396, 2001.

[28] C. Nafornita, M. Borda, A. Kane, "A wavelet-based digital watermarking using subband adaptive thresholding for still images," microCAD, pp. 87-92, 2004.

[29] Corina Nafornita, "A wavelet-based watermarking for still images," Scientific Bulletin of Politehnica University of Timisoara, tom vol. 49, no. 63, Electronics and Telecommunications, fascicola 2, Symposium of Electronics and Telecommunications Etc, pp. 126-131, 2004.

[30] B. Wang, J. Ding, Q. Wen, X. Liao, and C. Liu, "An image watermarking algorithm based on DWT DCT and SVD," Proceeding of IC-NIDC, pp. 1034-1038, 2009.