

A Robust and Oblivious Watermarking Method Using Wavelet Transform and Genetic Algorithm

Dr. K. Ramanjaneyulu, K.S.S. Manasa, G. Upendra

Professor, ECE,

PVP Siddhartha Institute of Technology, AP, India

Email-id: kongara.raman@gmail.com

Dept. of ECE,

PVP Siddhartha Institute of Technology, AP, India

Email-id: manasa.koduganti@gmail.com

Dept. of ECE,

PVP Siddhartha Institute of Technology, AP, India

Email-id: upendra.pvpsit@gmail.com

ABSTRACT

Watermark is embedded by modifying the third level mid frequency coefficients of the host image with multiple SFs. As many combinations of SFs are possible, it is difficult to obtain optimal solutions by trial and error method. Hence, in order to achieve the highest possible transparency and robustness, optimization of the scaling factors is necessary. This task employs Genetic Algorithm (GA) to obtain optimum SFs. GA can search for multiple solutions simultaneously over a wide range, and an optimum solution can be gained by combining the obtained results appropriately. The aim of the task is to develop an optimal watermarking technique based on DWT domain for grey-scale images. In this paper, a robust and oblivious image watermarking algorithm using maximum wavelet coefficient modulation is proposed. Simulation results show that performance of the proposed method is superior in terms of Peak Signal to Noise Ratio (PSNR) and Normalized Correlation Coefficient (NCC).

Index Terms: Digital Image Watermarking, Wavelet Transform, Genetic Algorithm, Copyright Protection, Peak Signal to Noise Ratio, Normalized Correlation Coefficient.

1 INTRODUCTION

Digital media has become the leading choice of format for storing audio, image, video and text information for multimedia applications on the internet. Media formats such as MP3, DVDs and JPEGs are widely available to millions of users. Many researchers are aware of the issues of copyright protection, image authentication, proof of ownership etc. Many solutions have been proposed to tackle these issues. Watermarking Technique is one of these solutions. In watermarking process, specific information called watermark is embedded imperceptibly into the original media object. Watermarking algorithm is referred to as an oblivious (also referred to as blind or public) if the original image and the watermark are not needed during extraction.

Three important issues are to be considered in this system. 1) Embedding process should not degrade the quality of the cover image and should be perceptually invisible to maintain its

protective secrecy. 2) The watermark must be robust enough to resist common image processing attacks and not be easily removable and only the owner of the cover to be able to extract the watermark. 3) The blindness is necessary in some applications in which the original image (and the watermark also) is not available at the time of extraction.

In this paper, a robust and an oblivious image watermarking scheme based on the maximum wavelet coefficient modulation is proposed. Rest of the paper is organized as: Section 2 provides review of related work. Section 3 covers the proposed method. In section 4, experimental results will be presented for the improved performance of the proposed method in comparison with the existing techniques. Robustness against the most common attacks is also presented. Finally, the section 5 discusses conclusion part.

2 Review of the related works

Watermarking can be done either in the spatial domain or in the transform domain. Watermarking in the spatial domain is simple but the watermarked image is hard to robust. Watermarking in the transform domain is secure and robust to

many attacks. Plenty of research of various researchers has been done on Image watermarking algorithms using Discrete Cosine Transform (DCT), Singular Value Decomposition (SVD) and Discrete Wavelet Transform (DWT). Among these, the DWT approach remains one of the most effective and easy to implement techniques for image watermarking [1]. The most important issue in DWT based image watermarking is how to choose the coefficients to be embedded. In [2][3][4], the watermark is embedded in the significant wavelet coefficients. Wang et al. [5] proposed a watermarking method which is based on multi-threshold wavelet coding (MTWC) and the successive sub-band quantization (SSQ) is used to search for the significant coefficients. The watermark is added by quantizing the significant coefficient in the significant band using different weights. In [6], two methods were proposed: one connects to watermark is embedded by modifying the triplets of significant coefficients according to a sequence of information bits and second one considers the rectangular blocks of coefficients, and each block is used to embed one watermark bit.

In [2][7][8], the significant coefficients, selected from global coefficients are used and showed robustness to many image attacks. But, the problem is that the order of extracting the significant coefficients in the extraction process should be exactly the same as those in the embedding process. Hence, they are not suitable for the blind watermarking.

W.H. Lin et al. [9] used DWT for watermarking a 512 x 512 gray scale image. They quantized the maximum wavelet coefficient of a variable sized block of a selected sub band. The watermark is a 32 x 16 binary image. Low embedding capacity and adjustment of the scheme parameters to satisfy some specified watermarking requirements (PSNR and NCC with attacks) are the limitations of their method.

From all these observations, this paper presents a blind and robust watermarking algorithm to embed a 32 x 32 binary watermark into a grayscale cover image using the local maximum wavelet coefficient modulation, which is a block based approach. Third level LH sub band is selected for embedding the watermark. Selected sub band is divided into various blocks of equal size. Number of blocks must be equal to the number of watermark bits. Maximum coefficient of a block is modulated depending on whether the watermark bit is 1 or 0. Energy of the maximum coefficient is increased if the watermark bit is 1 and makes the energy of the maximum coefficient close to the second maximum if the watermark bit is 0. During the extraction process, energy is subtracted from the maximum coefficient of a block. If the coefficient is still the maximum of the block then the decision is taken in favor of a 1, else in favor of a 0. The scheme is characterized with parameters to get control over the embedding and extraction process. Then, Genetic Algorithm (GA) [13-19] is used for parameter optimization. Optimization is required to satisfy the conflicting requirements of the Peak Signal to Noise Ratio (PSNR) and the Normalized Cross correlation (NCC). Experimental results shows that the proposed method is better than the existing methods [9][10][11][12] in terms of both PSNR and NCC.

3 Proposed Watermarking Scheme

In this section, proposed scheme is described in three sub sections. Section 3.1 deals with watermark embedding

procedure, watermark extraction is explained in section 3.2 and the application of GA for determining the optimum parameters of the scheme is given in section 3.3.

3.1 Watermark Embedding

In the proposed algorithm, a binary watermark image is embedded in a gray scale cover image. The transform used is DWT. The embedding strategy is based on the local maximum wavelet coefficient modulation. Third level mid-frequency sub-band, LH₃, of the cover image is selected for embedding binary watermark of size N_w . Divide the LH₃ sub band into N_w number of blocks. Now, compute the following.

$$(a) \quad MWC_{mean} = \frac{1}{N_w} \sum_{j=1}^{N_w} M_j \quad (1)$$

Where,

$$M_j = \max_j, \text{ if the watermark bit is '1'}$$

$$= \max_j \times t_1, \text{ otherwise} \quad (2)$$

\max_j = maximum wavelet coefficient of the j^{th} block

t_1 = scaling factor

$$(b) \quad a_j = t_2 \times \text{maximum} \{ |avg_j|, |MWC_{mean} \times t_3| \}$$

$$\text{for all } j = 1 \text{ to } N_w \quad (3)$$

Where,

avg_j = average coefficient value of the j^{th} block

t_2, t_3 are the scaling parameters

Modulate \max_j according to the Watermark bit

for all $j = 1$ to N_w as follows

$$\max_j^{new} = \max_j + a_j, \text{ if the watermark bit is '1'}$$

$$= \sec_j + a_j \text{ otherwise} \quad (4)$$

Where, \sec_j denotes the second maximum coefficient value of the j^{th} block t_3 is the scaling factor which is less than 1.

Get the modified LH₃ sub band by combining the modulated blocks. Obtain the three level inverse DWT using modified LH₃ sub band to get the watermarked image. The parameters / scaling factors; t_1, t_2 and t_3 ; are used to control the value of the PSNR.

3.2 Watermark extraction

Possibly attacked watermarked image is the only input image required for the extraction process as the scheme is oblivious watermarking method. Parameter t_4 value is required. Even if

the value of t_4 is not available, GA may be used to find its value. Extraction of watermark is done as follows.

Decompose the possibly attacked watermarked image using third level DWT and obtain the sub bands. Divide the LH₃ sub band into N_w number of blocks. Then, Compute the following.

$$(a) MWC_{mean}^{\circ} = \frac{1}{N_w} \sum_{j=1}^{N_w} \max_j^{\circ} \quad (5)$$

Where, \max_j° denotes the maximum coefficient of j^{th} block.

$$(b) Mean_{block} = \frac{1}{N_w} \sum_{j=1}^{N_w} |avg_j^{\circ}| \quad (6)$$

Where, avg_j° is the average coefficient value of the j^{th} block excluding \max_j°

Detect the watermark bit using the following detection rule for all $j = 1$ to N_w

$$\begin{aligned} \text{Watermark bit} &= 1, \text{ if } (\max_j^{\circ} - t_4 \times a_j^{\circ}) \geq \sec_j^{\circ} \\ &= 0, \text{ otherwise} \end{aligned} \quad (7)$$

Where,

t_4 is the scaling factor,

$$a_j^{\circ} = \text{maximum} (|avg_j^{\circ}|, |Mean_{block}|, k_1, k_2) \quad (8)$$

$$k_1 = \max_j^{\circ} / MWC_{mean}^{\circ} \quad (9)$$

$$k_2 = avg_j^{\circ} / Mean_{block} \quad (10)$$

In Eq. (7), \sec_j° represents the second maximum value of the j^{th} block. The parameter / scaling factor, t_4 , is used to control the value of the NCC.

3.3 Optimization of parameters using GA

GA can be used for watermarking applications [16], based on the fact that effective watermarking has two conflicting requirements, PSNR and NCC. These two requirements are related to each other and therefore the watermarking algorithm described above must be optimized. Optimization search space and the fitness function are described as follows.

Search space: The values of the four scaling factors (t_1 , t_2 , t_3 and t_4) are the key that, if chosen properly, will result in optimal imperceptible and robust watermarking. It is the role of the GA to find such values, where the GA's search space must include all possible values for the four scaling factors.

The fitness function: Two common performance evaluation metrics, PSNR and NCC, are combined to form the

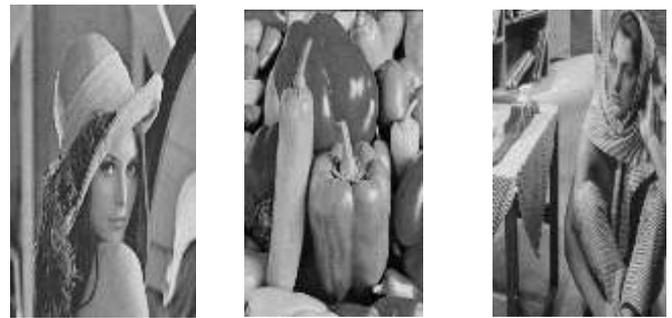
fitness function. The fitness function is formed by combining the two metrics as follows.

$$fit_l = PSNR_l + \frac{1}{P} \sum_{k=1}^p (NCC_{k,l} \times \alpha_k) \quad (11)$$

Where, l denotes GA generation number, p denotes the total number of attacks used in the optimization process, $NCC_{k,l}$ represents NCC value with attack k and α_k represents weighting factor for NCC.

4 Experimental Results

Three different cover images are used for experimentation. They are Lena, Peppers and Barbara (512×512 pixels, 8 bits/pixel) which are shown in Fig. 1 (a), Fig. 1 (b) and Fig. 1 (c) respectively. MATLAB 7.0 and Checkmark 1.2 are used for testing the robustness of the proposed scheme. Two dimensional DWT with 'Haar' wavelet filters is used. Genetic Algorithm (GA) with a population size of 20 chromosomes, a crossover rate of 0.8 and a Gaussian mutation function (with a scale 1.0 and shrink 1.0) are used.



(a) Lena (b) Peppers (c) Barbara

Fig. 1 Cover Images of size 512 × 512

The peak signal-to-noise ratio (PSNR) is used to evaluate the quality between an attacked image and the original image. PSNR is defined as follows:

$$PSNR = 10 \log_{10} \frac{255 \times 255}{\frac{1}{M \times N} \sum_{x=1}^M \sum_{y=1}^N [f(i, j) - g(i, j)]^2} \text{ dB} \quad (12)$$

Where, M and N are the height and width of the image, respectively. $f(i, j)$ and $g(i, j)$ are the pixel values located at coordinates (i, j) of the original image, and the attacked image, respectively. After extracting the watermark, the normalized correlation coefficient (NCC) is computed using the original watermark and the extracted watermark to judge the existence of the watermark and to measure the correctness of an extracted watermark. It is defined as

$$NCC = \frac{\sum_{i=1}^m \sum_{j=1}^n [w(i, j) - w_{mean}] [w^{\circ}(i, j) - w_{mean}^{\circ}]}{\sqrt{\left(\sum_{i=1}^m \sum_{j=1}^n [w(i, j) - w_{mean}]^2 \right) \left(\sum_{i=1}^m \sum_{j=1}^n [w^{\circ}(i, j) - w_{mean}^{\circ}]^2 \right)}} \quad (13)$$

Where, m and n are the height and width of the watermark, respectively. The symbols $w(i, j)$ and $w^\circ(i, j)$ are the bits located at the coordinates (i, j) of the original watermark and the extracted watermark respectively. The symbols w_{mean} and w_{mean}° are the mean values of the original watermark and the extracted watermark respectively.

Genetic Algorithm is executed to find the optimum values for the scaling factors of the proposed scheme. Scaling factors used in the proposed algorithm are t_1, t_2, t_3 and t_4 . Scaling factors can be adjusted according to PSNR and NCC requirement. The required values (target values for GA process) must be included in the fitness function written for GA. Assume that the required values for PSNR and NCC are 42 and 1 respectively. PSNR depends upon the scheme parameters t_1, t_2 , and t_3 . NCC depends on t_4 . But, PSNR and NCC are not independent. Hence, it is not possible to fix the values for both PSNR and NCC. In addition, one can specify the weights as per requirements. As the required value of NCC is very small in comparison with the required PSNR, a weight 20 is used for NCC. $[(42-PSNR) + 20(1-NCC)]$ is used as the fitness function in the GA process. GA minimizes the fitness function and produces the optimum values for PSNR, NCC, and scaling factors. We can also specify one or more image attacks against which robustness is required for the watermark. In these experiments, JPEG attack with quality factor 40 is specified for GA. Table 1 shows the results of GA with different cover images. Optimum values for PSNR, NCC and scaling factors (scheme parameters) are shown, after observing GA results for five generations.

Table 1 Results of GA based optimization against the JPEG attack with QF=40. Cover image is Lena.

Attack: JPEG-40 Fitness Function: $(42-PSNR)+20(1-NCC)$ Initial range for Parameters: [0.1-1.0, 0.5-1.0, 0.1-1.0, 0.05-1.0]				
Cover Image	Fitness Value	PSNR In dB	NCC	Scaling Factors [t1, t2, t3, t4]
Lena	1.50	41.99	0.93	[0.3140, 0.7962, 0.8903, 0.6206]
Peppers	3.14	41.80	0.85	[0.4017, 0.5404, 0.8020, 0.3730]
Barbara	2.92	41.71	0.87	[0.8335, 0.6549, 0.4174, 0.4410]

Original watermark image is shown in Fig. 2 (a). Fig. 2 (b) shows the unattacked watermarked Lena. Fig. 2 (c) shows the attacked (JPEG, quality factor 40) watermarked Lena. The extracted watermark is shown in Fig. 2 (d). Scaling factors

used for watermarking are $t_1=0.3140, t_2=0.7962, t_3=0.8903$ and $t_4=0.6206$.

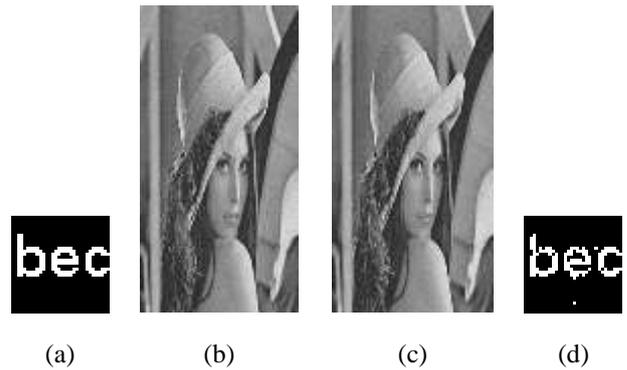


Fig.2 (a) Original Watermark Image
(b) Watermarked Lena, PSNR=41.9914 dB
(c) Attacked watermarked Lena with JPEG-40 attack, PSNR=34.9652 dB
(d) Extracted watermark, NCC=0.9253

JPEG is one of the most frequently used formats in connection with the Internet and digital cameras. The JPEG quality factor is a number between 0 and 100 and associates a numerical value with a particular compression level. When the quality factor is decreased from 100, the image compression is improved, but the quality of the resulting image is significantly reduced. Varied quality factors are applied in the experiments, and the results are shown in Table 2 for the Lena image. The proposed method can detect the existence of a watermark through quality factors greater than 10. The results show that the value of NCC is greater than 0.50 with JPEG quality factor greater than 15.

Table 2 NCC of the watermark images extracted from JPEG attacked Lena watermarked images with different values for quality factors

JPEG Quality Factor (QF)	NCC
10	0.44
20	0.82
30	0.89
40	0.93
50	0.92
60	0.89
70	0.96
80	0.99
90	1.00
100	1.00

Other attacks like median filter, Gaussian filter, average filter (low pass filter), sharpening filter, histogram equalization scaling, cropping, salt and pepper noise etc., are also applied to the watermarked images and the corresponding results are shown in Table 3. The proposed method can effectively resist all those attacks.

Table 3 NCC of the watermark images extracted from Lena watermarked images with various other attacks

Type of Attack	NCC
Median Filter (3 x 3)	0.88
Gaussian Filter (3 x 3) Variance = 0.5	0.91
Average Filter (3x3)	0.72
Sharpening filter	0.82
Histogram Equalization	0.84
Scaling 50%	0.83
Cropping 25%	0.58
Salt & pepper noise (0.001)	0.92

For average (low pass) filtering attack, a 3x3 mask is used. The median filter is a non linear spatial filter which is usually used to remove noise spikes from an image. The watermarked image is attacked by median filtering with a 3x3 mask. The cropping operation (lossy operation) deletes some portion of the image. The extracted watermark is still recognizable even after 25% of cropping. The watermarked image is attacked by salt and pepper noise with a noise density of 0.001. The extracted watermark is still recognizable. The proposed method is compared with Wang and Lin's [10], Li et al.'s [11], Lien and Lin's [12] and Lin et al. [9] methods in terms of PSNR and NCC (using the Lena as the cover image). Results

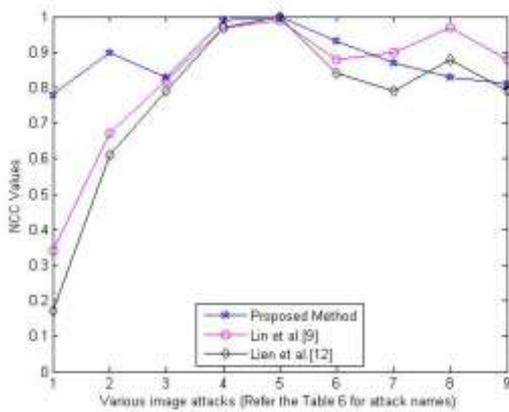
of those existing methods are found in [9]. Size of the watermark image (Logo) is 32×16 in those methods. For comparison purpose, a watermark with the same size is embedded using GA based proposed method and obtained the results. Comparison results are shown in Table 4 and in Fig. 3 in the graphical form. Performance of the proposed method is better than the other methods against JPEG compression and Gaussian filter attacks. But, this method is slightly inferior in comparison with the methods in [9] and [12] against sharpening and scaling attacks. The proposed method can detect the existence of a watermark through JPEG quality factors greater than 10. NCC value obtained against JPEG (Quality factor 10) attack with the proposed method is 0.78. But, the NCC value against the same attack for the existing methods is less than or equal to 0.34. Similarly, proposed method is better in terms of perceptual quality (PSNR) of the watermarked image. Optimum value obtained for PSNR with the proposed scheme is 42.92 dB when 32×16 size watermark is embedded. Optimization is performed against JPEG, average filter and high pass filters. Obtained parameter values are $t_1=1.1710$, $t_2=1.1879$, $t_3=0.6047$ and $t_4=1.0058$.

5 Conclusions

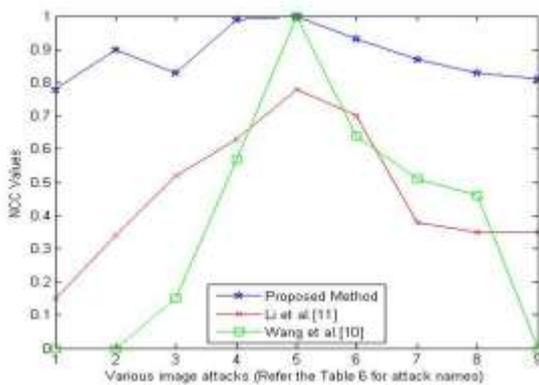
In this paper, a novel and an oblivious watermarking method is proposed based on GA and using maximum wavelet coefficient modulation. Perceptual quality of the watermarked image is good and the watermark can effectively resist JPEG compression and various other attacks like Gaussian filter, median filter, and average filter etc. Advantage of the proposed scheme is the effective use of GA to obtain the optimum response in terms of both PSNR and NCC. Experimental results show that the performance of the scheme is better than the existing schemes in terms of the embedding capacity, PSNR and NCC. In addition to copyright protection, the proposed scheme can also be applied to data hiding and image authentication.

Table 4 Performance comparison of the proposed method with the methods of Wang and Lin's [10], Li et al.'s [11], Lien and Lin's [12] and Lin et al [9]. (Using Lena as the cover image and 32×16 Logo)

S. NO	Attacks	Wang and Lin [10] (PSNR = 38.2 dB) NCC	Li et al [11] (PSNR= 40.6 dB) NCC	Lien and Lin [12] (PSNR= 41.54 dB) NCC	Lin et al [9] (PSNR= 42.02 dB) NCC	Proposed method (PSNR= 42.92 dB) NCC
1	JPEG (QF=10)	NA	0.15	0.17	0.34	0.78
2	JPEG (QF=20)	NA	0.34	0.61	0.67	0.90
3	JPEG (QF=30)	0.15	0.52	0.79	0.82	0.83
4	JPEG (QF=70)	0.57	0.63	0.97	0.97	0.99
5	JPEG (QF=90)	1.00	0.78	1.00	0.99	1.00
6	Gaussian Filter	0.64	0.70	0.84	0.88	0.93
7	Median Filter (3x3)	0.51	0.35	0.79	0.90	0.87
8	Sharpening Filter	0.46	0.38	0.88	0.97	0.83
9	Scaling (50%)	NA	0.35	0.79	0.88	0.81



(a) With Lin et al. [9] & Lien et al. [12]



(b) With Li et al. [11] & Wang et al. [10]

Fig. 3 Performance comparison of the proposed method with the existing methods

References

- [1] P.Meerwald and A.Uhl, "A Survey of Wavelet-domain watermarking Algorithms," Proceedings of the SPIE, Electronic Imaging, Security and Watermarking of Multimedia Contents III, pp.505–516, 2001.
- [2] R.Dugad, K.Ratakonda and N.Ahuja, "A new wavelet-based scheme for watermarking images," Proceedings of the IEEE ICIP, Chicago, pp.419–423, 1998.
- [3] J.R.Kim and Y.S.Moon, "A robust wavelet-based digital watermarking using level-adaptive Thresholding," Proceedings of the IEEE ICIP, Kobe, pp. 226–230, 1999.
- [4] S.G.Kwon, S.W.Ban, I.S.Ha, et al., "Highly reliable digital watermarking using successive sub band quantization and human visual system," Proceedings of IEEE ISIE, Pusan, pp.205–209, 2001.
- [5] H.J.Wang and C.C.J.Kuo, "High fidelity image compression with multithreshold wavelet coding (MTWC)," SPIE's Annual Meeting-Application of Digital Image Processing, San Diego, pp. 383–392, 1997.
- [6] F.Davoine, "Comparison of two wavelet based image watermarking schemes," International Conference on Image Processing, Vancouver, pp.682–685, 2000.
- [7] M.Hsieh, D.Tseng, and Y.Huang, "Hiding digital watermarks using multiresolution wavelet transform," IEEE Transactions on Industrial Electronics, Vol.48, No.5, pp.875–882, 2001.
- [8] C.Temi, S.Choomchuay, and A.Lasakul, "A robust image watermarking using multiresolution analysis of wavelet," Proceedings of the IEEE ISCIT, pp.623–626, 2005.
- [9] W.H.Lin, Y.R.Wang, S.J.Horng, T.W.Kao and Y.Pan, "A blind watermarking method using maximum wavelet coefficient quantization," Expert Systems with Applications, Vol.36, No.9, pp.11509-11516, Nov 2009.
- [10] S.H.Wang and Y.P.Lin, "Wavelet tree quantization for copyright protection watermarking," IEEE Trans. Image Processing, Vol.13, No.2, pp.154–165, 2004.
- [11] E.Li, H.Liang and X.Niu, "An integer wavelet based multiple logo-watermarking scheme," Proceedings of the IEEE WCICA, pp.10256–10260, 2006.
- [12] B.K.Lien and W.H.Lin, "A watermarking method based on maximum distance wavelet tree quantization," 19th Conf. Computer Vision, Graphics and Image Processing, pp.269–276, 2006.
- [13] JH.Holland, "Adaptation in natural and artificial systems: an introductory analysis with applications to biology, control and artificial intelligence," Cambridge, MA: MIT Press; 1992.
- [14] K.Ramanjaneyulu and K.Rajarajeswari, "Wavelet Based Oblivious Image Watermarking Scheme Using Genetic Algorithm," The Institution of Engineering and Technology (IET) Image Processing Journal, International Journal, Vol.6, No.4, pp.364-373, June 2012.
- [15] VeyselAslantas, "A singular-value decomposition-based image watermarking using genetic algorithm," International Journal of Electronics and Communications, (AEÜ), 62, pp.386-394, 2008.

- [16] Ali Al-Haj and Aymen Abu-Errub, "Performance Optimization of Discrete Wavelets Transform Based Image Watermarking Using Genetic Algorithms,"

Journal of Computer Science, Vol.4, No.10, pp.834-841, ISSN 1549-3636, 2008.