Dynamic Binary Location based Multi-watermark Embedding Algorithm in DWT

Ammar Jameel Hussein, Seda Yuksel, and Ersin Elbasi

***Abstract* – In order to achieve a good imperceptibility and robustness, using 4-level DWT algorithm based on dynamic binary host image location and embedding two watermark logos in different DWT levels are proposed for copyright protection and authenticity. In the propounded watermarking algorithm, 5-level DWT is applied to host image to obtain the fifth low frequency sub band (LL5), and examination the dynamic binary location value of selected location for embedding purpose in five different locations in host image using the same algorithm process. Our experimental results demonstrate that our algorithm scheme is imperceptible and robust against several image processing attacks, and watermarked image quality evaluating by calculation of SNR, PSNR, RMSE, and MAE.**

***Index Terms*—Copyright Protection, Discrete Wavelet Transforms, Information Security, Frequency-domain Analysis, Watermarking**

I. INTRODUCTION

THE idea of Internet of thing or Internet of everything [1] makes a digital achievement, transmission of digital media is not a simple task. Proving the ownership of digital multimedia being transmitted introduces the requirement of having a robust watermarking scheme, to satisfy this growing necessity. Mostly, an operational digital watermarking scheme should meet elementary requirements which are:

1) Imperceptibility: Watermark cannot be realized by human sense, only can be perceived over special handling [6]. In addition, watermarks should not interfere with the media being protected [2].
2) Trustworthiness [2]: Assurances that it is difficult to generate counterfeit watermarks, and they should provide trustworthy proof to keep the legal ownership.
3) Capacity [6]: This defines how many information bits that can be embedded. Additionally, statements the possibility of embedding multiple watermarks in one object.
4) Robustness [6]: The watermark should be robust against general signal processing attacks and malicious operation.

Manuscript received June 29, 2014.
Ammar Jameel Hussein is with the Department of Computer Engineering, Iraqi Board of Supreme Audit, Baghdad, Iraq (email: ammar.jameel.ict@gmail.com).
Seda Yuksel is with the Department of Computer Engineering, Çankaya University, Ankara, Turkey (e-mail: seda.yuksel.sy@gmail.com).
Ersin Elbasi is with the Department of Digital Game Design, Ipek University, Ankara, Turkey (e-mail: eelbasi@ipek.edu.tr).

Digital watermarking [3] is a relatively new study zone that attracts the attention of various researchers in academic and business world. This becomes one of the most up-to-date research topics in the multimedia signal processing community. The term of watermarking has a little different meaning, one definition gives the impression to overcome the following [4]: Watermarking is the process of imperceptibly modifying a part of data so as to embed info around the data. The above definition mentions two important features of watermarking. Initially, information embedding should not cause visible changes to the second host medium; the message should be associated to the host medium [5]. Digital watermarking can be classified regarding to several of classes which are [6]:

1) Characteristics, robustness (Robust, Fragile and Semi-fragile)
2) Attached media, host signal (Image watermarking, Video watermarking, Audio watermarking, Text watermarking and Graphic watermarking)
3) Perceptivity (Visible watermark and Invisible watermarking)
4) Purpose (Copyright protection watermarking, Tampering tip watermarking, Anti-counterfeiting watermarking and Anonymous watermarking)
5) Watermark type (Noise type and Image type)
6) Detection process (Visual watermarking, Semi blind watermarking and Blind watermarking)
7) Use of keys (Asymmetric watermarking and Symmetric watermarking)
8) Domain (Spatial domain and Frequency domain)

Reviewing a previous work, we realize that, Dugad et al. [7] offered discrete wavelet transform based structure for embedded the watermark in low - low (LL) band, coefficients in similar method by way of Cox et al. that had been previously offered by Elbasi and Eskicioglu [8] embedded a pseudorandom sequence as a watermark in two bands (LL and HH) by using DWT [9]. P. Kumhom et al. [10] applied a non-blind watermark scheme that focused on collection the high frequency variety that holds huge sum of information. While Jila Ayubi et al. [11] proposed a watermark scheme built on chaotic maps and DWT, P. Kumar et al et al. [12] used (Haar wavelet) structure designed for rebuilding filter banks, skimming data according to Least Significant Bits of the coefficient. Parthiban V. and Ganesan R. [13] enhanced the robustness of his scheme through grouping of DWT and Singular Value Decomposition (SVD) technique.

In our paper, we focus on domain based watermarking techniques (i.e. spatial domain and Frequency domain). Spatial domain watermark indicates fewer confrontations in contradiction of several image processing operations [14], henceforth, termed as a fragile watermarking. Despite the fact that frequency domain techniques like discrete wavelet transform (DWT) [15], discrete Fourier transforms (DFT) [16], and discrete cosine transform (DCT) [17] offer more robustness.

II. DISCRETE WAVELET TRANSFORMS

Wavelets are discovered by Daubechies (1988, 1992) which have been proved to be as successful as the FBI's chosen method of compression for fingerprint data (Brislawn, 1995) [18].

Wavelet transform in two dimensional can be stated as a two dimensional scaling function $\phi(x,y)$ and three two dimensional wavelets $\psi^H(x,y), \psi^V(x,y), \psi^D(x,y)$

Wavelet transform of an image $A(x,y)$ of size is $M \times N$ defined by:

$$W_\phi(j_0,m,n) = \frac{1}{\sqrt{MN}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} A(x,y)\phi_{j0.m.n}(x,y) \quad (1)$$

$$W_\psi^i(j\ ,m,n) = \frac{1}{\sqrt{MN}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} A(x,y)\psi^i{}_{j.m.n}(x,y) \quad (2)$$

Where $i = [H,V,D]$ and j_0 is a random scale.

$W_\phi(j_0,m,n)$ Defines low frequency coefficients of $A(x,y)$, At scale, j_0 and $W_\psi^i(j\ ,m,n)$ define the horizontal, vertical and diagonal details for scale $j \geq j_0$ [19].

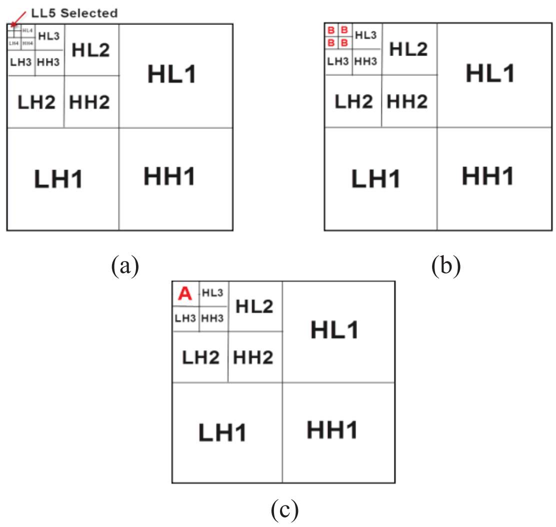


Fig. 1. (a) DWT fifth level of decomposition (b) DWT third level of decomposition and position of first watermark logo (c) DWT fourth level decomposition and position of second watermark

The purpose of DWT idea is to decompose a signal into different resolutions. The lowest frequency sub band includes the almost significant information about the image. While high frequency subs bands include the image details [20]. Fig. 1(a) shows the selection criteria of fifth level DWT decomposition, Fig. 1(b) presents embedding criteria. The first watermark is embedded in the third level of DWT decomposition in (LL3) sub band, while Fig. 1(c) shows the second four watermarks was embedded in the fourth level of DWT decomposition in (LL4, HL4, LH4, HH4) sub bands. They are distributed in different locations inside the image space, and this will improve the robustness and the security of the system.

III. THE PROPOSED SCHEME

In this section of the paper, 5-level DWT based watermarking scheme which uses scaling and translation characteristics of wavelet domain in different levels. Examination of the LL5 sub band acquires a low frequency gray value, then it is transferred it to binary (0, 1) values for the host image. The embedded first watermark logo in LL3 sub band and embedded second watermark logo in all (LL4, HL4, LH4, and HH4) sub bands. Embedding the watermark is shown in the proposed watermarking algorithm Fig. 2(a). The host image is a 512x512 and watermark is a 512x512, and it is applied with 4-level DWT decomposition for first and second watermark logos.

A. Algorithm: Watermark Embedding

1) Preparing the cover image with the size of (512x512), read the two watermark logos each with the size of (512x512).
2) Performing fifth level DWT using Haar wavelets and selecting LL5 sub band, converting it to gray image; then converting it to a binary image to get value position in forms of (0,1).
3) Performing fourth level DWT, for first and second watermark logos.
4) Examination of LL5 position value; if LL5 (i, j) == 0, embedding first watermark logo in the host image to (LL3) sub band position.
5) Examination of LL5 position value; if LL5 (i, j) == 1, then embedding second watermark logo in the host image to (LL4, HL4, LH4, HH4) sub bands position.
6) Performing third level IDWT, to reconstruct first watermarked image, and fourth level IDWT to reconstitute second watermarked image.

Let $f(i,j)$ be the original cover images, $w(i,j)$ is the first watermark image, and $w'(i,j)$ is the second watermark image. Then, $v(i,j)$ is the first watermarked image, and $v'(i,j)$ is the second watermarked image. Therefore,

$f'(i, j)$ is the watermarked image, the embedding is done, according to the following equations:

$$v(i, j) = f(i, j) + w(i, j) \quad (3)$$

$$v'(i, j) = f(i, j) + w'(i, j) \quad (4)$$

$$f'(i, j) = (v(i, j) + v'(i, j)) / 2 \quad (5)$$

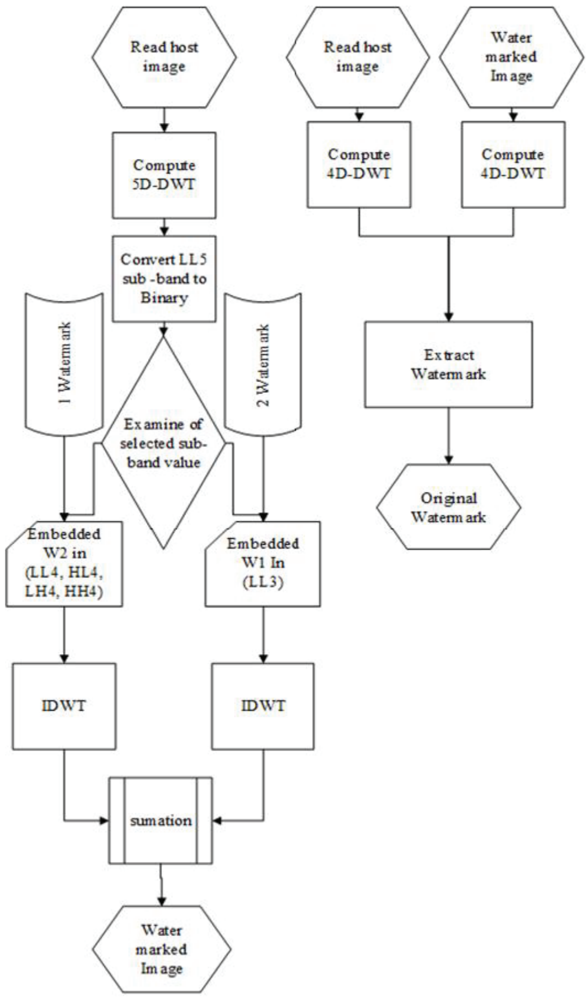
B. Watermark Extraction

1) Prepare the original host image and the watermarked image.
2) Decompose both, host image cover and the watermarked cover with using the fourth level of DWT decomposition. Afterwards, subtract the bands to get the first watermark and four second watermark, the extraction equations are:

$$w(i, j) = f'(i, j) - f(i, j) \quad (6)$$

$$w'(i, j) = f'(i, j) - f(i, j) \quad (7)$$

Fig. 2 (b) shows the extraction process.



(a) (b)

Fig. 2. (a) Embedding scheme (b) Extraction process

IV. EXPERIMENTAL RESULTS

A number of experiments are performed to evaluate the performance of the proposed watermarking algorithm on different gray scale images of size 512x512 like mandrill, boxer, Boat, Goldhill, Lena and Barbara, using MATLAB platform. The results of two gray scale host images, mandrill and boxer along with used watermarked logo shown in Fig. 3, Fig. 4 and Fig. 5 respectively. Fig. 3 (a) - (b) show comparison between first host image and watermarked image, Fig. 5 (a) - (b) demonstrate comparison between second host image and watermarked image and Fig. 5 (a) - (b) demonstrate comparison between third host image and watermarked image, while Fig. 6 (a) and (b) present first watermark logo and second watermark logo.

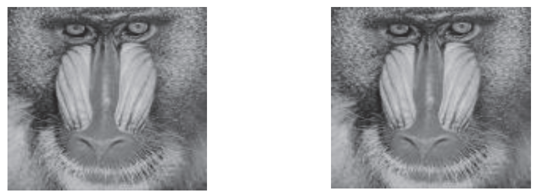


Fig. 3 (a) Host Image (b) Watermarked Image

Fig. 4. (a) Second host Image (b) Watermarked Image

Fig. 5. (a) Third host Image (b) Watermarked Image

Fig. 6. (a) First watermark logo (b) Second watermark logo

A. Attacks

In our experiment, we apply ten types of attacks, which generate a comparison to prove the superiority of recommended scheme. MATLAB is used for all attacks. The chosen attacks are JPEG compression, resizing, adding Gaussian noise, low pass filtering, rotation, histogram equalization, contrast adjustment, gamma correction, and cropping. The attacked images and the attack parameters for mandrill host image by using MATLAB are shown in Table - 1.

TABLE I
ATTACKED IMAGES, AND ATTACKED PARAMETERS

No.	Attacks	Parameters	Result Image
1.	Gaussian noise	(mean = 0, variance = 0.001)	
2.	Low pass filtering	(window size=3x3)	
3.	Cropping	on both sides	
4.	Scaling	512x256	
5.	Rotation	(20^0)	
6.	Equalization	automatic	
7.	Adjustment	([l=0 h=0.8],[b=0 t=1])	
8.	Gamma	(1.5)	
9.	Jpeg compression	(Q = 50)	
10.	Noise	(0.02)	

B. Evaluation

The evaluation of watermarked image quality is measured by SNR, PSNR, RMSE, and MAE. In our experiment, we use image J's plugin to evaluate the quality of images [21]. This program calculates the SNR, PSNR, RMSE, and MAE of images or sequences of images depend on the definitions of Gonzalez [22]. The plugin matches a reference image r(x, y) with a test t(x, y). The two images should have the same size [nx, ny], SNR, PSNR, RMSE, and MAE calculated by the given equations:

1) Signal-to-noise ratio (SNR) defined by the equation:

$$SNR = 10.\log 10\left[\frac{\sum_{0}^{Nx-1}\sum_{0}^{Ny-1}[r(x,y)]^2}{\sum_{0}^{Nx-1}\sum_{0}^{Ny-1}[r(x,y)-t(x,y)]^2}\right] \quad (8)$$

2) Peak signal-to-noise ratio (PSNR) defined by the equation:

$$PSNR = 10.\log 10\left[\frac{Max(r(x,y))^2}{\frac{1}{Nx.Ny}\bullet\sum_{0}^{Nx-1}\sum_{0}^{Ny-1}[r(x,y)-t(x,y)]^2}\right] \quad (9)$$

3) Root mean square error (RMSE) defined by the equation:

$$RMSE = \sqrt{\frac{1}{Nx.Ny}.\sum_{0}^{Nx-1}\sum_{0}^{Ny-1}[r(x,y)-t(x,y)]^2} \quad (10)$$

4) Mean absolute error (MAE) defined by the equation:

$$MAE = \frac{1}{Nx.Ny}.\sum_{0}^{Nx-1}\sum_{0}^{Ny-1}[r(x,y)-t(x,y)] \quad (11)$$

In our experiment, we take many standard host images like mandrill, boxer, boat, Barbara, Lena, and Goldhill to test our watermarked schema along with applying ten type of attacks. After watermarking process, we calculate the SNR, PSNR, RMSE, and MAE shown in Table – 2 (a) (b), Table – 3 (a) (b), and Table – 4 (a) and (b).

TABLE II (A)
MANDRILL HOST IMAGE USED AS REFERENCE IMAGE

Test Image	SNR	PSNR	RMSE	MAE
Wimage.png	47.5	51.76	0.5678	0.285
Gaussia.png	24.4	28.69	8.0891	6.450
Filter.png	26.7	30.94	6.2383	3.733
crop.png	6.11	10.34	66.892	32.88
Resize.png	26.0	30.24	6.7622	4.571
Rotate.png	6.49	10.71	64.060	46.91
Equal.png	10.9	15.18	38.279	34.19
Intensit.png	11.9	16.16	34.201	32.85
Gamma.png	11.9	16.18	34.129	33.85
hostr50.jpg	31.8	36.08	3.4527	2.594
Noise.png	17.1	21.40	18.704	2.808

TABLE II (B)
MANDRILL WATERMARKED IMAGE USED AS A REFERENCE IMAGE

Test Image	SNR	PSNR	RMSE	MAE
Gaussia.png	24.5	28.71	8.068	6.432
Filter.png	26.7	30.97	6.217	3.683
crop.png	6.13	10.33	66.89	32.60
Resize.png	26.0	30.28	6.735	4.521
Rotate.png	6.50	10.71	64.08	46.92
Equal.png	10.9	15.20	38.22	34.14
Intensit.png	12.0	16.24	33.90	32.56
Gamma.png	11.9	16.11	34.39	34.14
hostr50.jpg	31.9	36.20	3.406	2.547
Noise.png	17.2	21.41	18.69	2.528

TABLE III (A)
BOXER HOST IMAGE USED AS REFERENCE IMAGE

Test Image	SNR	PSNR		RMSE
Wimage.png	49.36	52.98		0.55
Gaussian.png	26.05	29.67		8.07
Filter.png	28.50	32.12		6.09
crop.png	5.47	9.09		86.37
Resize.png	34.27	37.89		3.13
Rotate.png	4.53	8.15		96.25
Equal.png	14.27	17.89		31.35
Intensity.png	12.78	16.40		37.22
Gamma.png	15.80	19.41		26.30
hostr50.png	37.67	41.29		2.11
Noise.png	17.90	21.52		20.63

TABLE III (B)
BOXER WATERMARKED IMAGE USED AS A REFERENCE IMAGE

Test Image	SNR	PSNR	RMSE	MAE
Gaussia.png	26.09	29.73	8.05	6.41
Filter.png	28.54	32.18	6.07	1.51
crop.png	5.48	9.12	86.37	39.85
Resize.png	34.43	38.07	3.08	1.41
Rotate.png	4.54	8.18	96.26	65.99
Equal.png	14.23	17.87	31.55	26.85
Intensit.png	12.85	16.49	36.97	33.87
Gamma.png	15.72	19.36	26.56	25.36
hostr50.png	38.01	41.65	2.04	1.38
Noise.png	17.92	21.56	20.63	2.55

TABLE IV (A)
BOAT HOST IMAGE USED AS REFERENCE IMAGE

Test Image	SNR	PSNR	RMSE	MAE
Wimage.png	49.02	54.3	0.487	0.186
Gaussian.png	24.64	29.9	8.071	6.441
Filter.png	23.50	28.8	9.201	5.521
crop.png	6.154	11.49	67.87	32.33
Resize.png	23.57	28.91	9.136	5.668
Rotate.png	5.815	11.15	70.57	50.57
Equal.png	11.58	16.93	36.30	32.52
Intensity.png	12.14	17.48	34.05	32.16
Gamma.png	12.49	17.84	32.69	32.09
hostr50.png	28.11	33.46	5.414	4.045
Noise.png	17.24	22.58	18.93	2.688

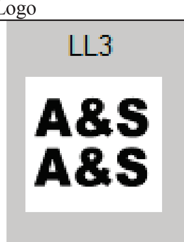
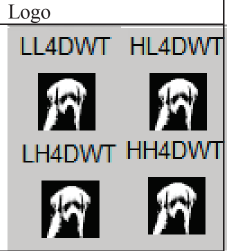
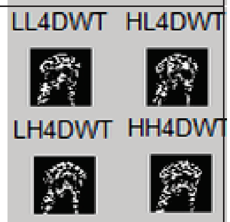
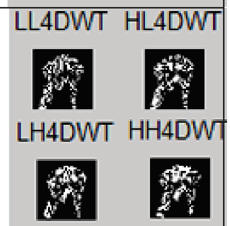
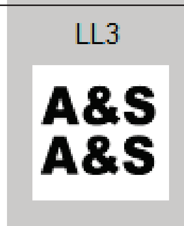
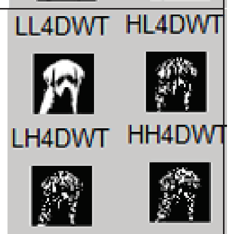
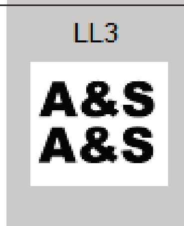
TABLE IV (B)
BOAT WATERMARKED IMAGE USED AS A REFERENCE IMAGE

Test Image	SNR	PSNR	RMSE	MAE
Gaussia.png	24.67	30.00	8.062	6.429
Filter.png	23.52	28.85	9.197	5.505
crop.png	6.165	11.49	67.87	32.15
Resize.png	23.59	28.92	9.121	5.648
Rotate.png	5.824	11.15	70.59	50.59
Equal.png	11.60	16.93	36.28	32.52
Intensit.png	12.20	17.53	33.86	31.98
Gamma.png	12.46	17.79	32.87	32.27
hostr50.png	28.16	33.49	5.391	4.025
Noise.png	17.25	22.58	18.93	2.505

C. Extraction after Attacks

In our experiment, we also extract the all embedded (LL3, LL4, HL4, LH4, and HH4) sub bands from watermarked image after and before applying ten types of attacks. MATLAB is used for all extraction process and the visual results for original watermarked image, Gaussian, filter, Gamma, and cropping shown in Table-5.

TABLE V
VISUAL RESULTS AFTER ATTACKS

Test Image	First Watermark Logo	Second Watermark Logo
Original Watermarked Image		
Gaussian (mean = 0, variance = 0.001)		
Filter (0.02)		
Gamma(1.5)		
Crop on both sides		

V. Conclusion

In this paper, we propose a robust multi-watermark embedding algorithm in DWT based on dynamic binary location by selecting a low frequency sub band from fifth level decomposition using two watermark logos to improve the robustness. We tested with the offered schema by applying ten types of attacks. Experimental results with high PSNR value measure the image quality, optimal SNR values estimate the quality of reconstructed image compared to the original one. We demonstrate that our scheme is robust against set of attacks, and also the extracted watermark logo improves to have good visual feature and image quality. Additionally, this can provide copyright protection for legal ownership. Our experimental results show that working with high level decompositions will lead the embedded watermarking logo to be in smaller part of host image. Thus, this will affect the robustness of proposed algorithm schema in face of the other set of attacks. Future work may focus on this area of study and trying to add extra parameter like "Arnold scrambling algorithm" [23] to improve the security and get better results.

ACKNOWLEDGMENT

A. J. Author thanks Iraqi board of supreme audit Iraq/Baghdad (Government Body) which contributed effectively to give me this opportunity for publishing. We would like to extend our sincere appreciation to Dr. Ersin Elbasi for his support in conducting the survey.

REFERENCES

[1] C. Pfister, "Getting Started with the Internet of Things: Connecting Sensors and Microcontrollers to the Cloud," O'Reilly Media Inc., 2011.
[2] P. Ramesh, Dr. V. U. Shree, and Dr. K. Padmapriya "Novel Hybrid Inaudible Audio Watermarking with Binary Image as Watermark using DWT," *International Journal Data & Network Security (IJDNS),* vol.4, pp. 169-173, 2013.
[3] G. Langelaar, I. Setyan, and R. Lagendijk, "Watermarking Digital Image And Video Data: A State Of Art Overview," *IEEE Transactions on Signal Processing Magazine,* 2000, pp. 19-47.
[4] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, "Digital Watermarking and Steganography," 2nd ed., *Morgan Kaufmann Publishers, Burlington, MA*, 2007.
[5] A. Bovik, *The Essential Guide to Image Processing*. Academic Press, 2009.
[6] P. Singh and R. S. Chadha, "A Survey of Digital Watermarking Techniques, Applications and Attacks," *International Journal of Engineering and Innovative Technology (IJEIT),* vol. 2, pp. 164-168, 2013.
[7] R. Dugad, K. Ratakonda, and N. Ahuja, "A New Wavelet-Based Scheme for Watermarking Images," *Proc. 1998 International Conference on Image Processing*, vol. 2, pp. 419-423, 1998.
[8] I. J. Cox, J. Kilian, F.T. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," *IEEE Transactions on Image Processing,* vol. 6, pp. 1672-1688, 1997.
[9] E. Elbasi and A. M. Eskicioglu, "A DWT-Based Robust Semi-Blind Image Watermarking Algorithm Using Two Bands," *Proc. SPIE 18th Annual Symposium on Electronic Image Security, Steganography and Watermarking of Multimedia Contents VIII,* vol. 6072, pp. 1-10, 2006.
[10] P. Kumhom and K. Chamnongthai, "Image Watermarking Based on Wavelet Packet Transform With Best Tree," *ECTI Transactions on Electrical Eng., Electronics, and Communications*, vol. 2, 2004.
[11] J. Ayubi et. al., "A Chaos Based Blind Digital Image Watermarking in The Wavelet Transform Domain," *International Journal of Computer Science Issues,* vol. 8, pp. 191-198, 2011.
[12] P. Kumar et al., "Digital Image Watermarking Using Wavelet Technique," *World Journal of Science And Technology,* 2012, pp. 6-9.
[13] V. Parthiban and R. Ganesan, "Hybrid Watermarking Scheme for Digital Images," *Journal of Computer Applications, 2012*, pp. 85-95.
[14] H. C. Andrews and C. L. Patterson, "Singular Value Decomposition and Digital Image Processing," *IEEE Trans. On Acoustics, Speech and Signal Processing*, no. 1, pp. 25-53, 1976.
[15] X. Y. Wang and H. Zhao, "A Novel Synchronization Invariant Audio Watermarking Scheme Based on DWT and DCT," *IEEE Trans. On Signal Processing,* vol. 12, no. 54, pp. 4834-4841, 2006.
[16] X. Y. Wang, P. P. Niu, and H. Y. Yang, *A Robust Content Based Image Watermarking Using Local Invariant Histogram*. New York: Springer, 2011, pp. 341-363.
[17] B.Y. Lei, I. Y. Soon and Zhen Li, "Blind and Robust Audio Watermarking Scheme Based on SVD-DCT," *Signal Processing*, vol. 91, pp. 1972-1985, 2011.
[18] S. G. Hoggar, "Mathematics of Digital Images Creation, Compression, Restoration, Recognition," Cambridge University Press, 2006.
[19] R. Mehta and N. Rajpal "A Hybrid Semi-Blind Gray Scale Image Watermarking Algorithm Based on DWT-SVD using Human Visual System Model," *Contemporary Computing (IC3), IEEE Sixth International Conference*, 2013.
[20] B. Furht, "Signal Processing for Image Enhancement and Multimedia Processing," Multimedia Systems And Applications Series Consulting Editor, 2008.
[21] Image plugin to assess the quality of images - Written by Daniel Sage at the Biomedical Image Group, EPFL, Switzerland. Available: http://bigwww.epfl.ch/
[22] R. C. Gonzalez and R.E. Woods, "Digital Image Processing," 3nd ed., Prentice Hall, 2008.
[23] M. Li, T. Liang, and Y. J. He, "Arnold Transform Based Image Scrambling Method", *3rd International Conference on Multimedia Technology (ICMT 2013),* pp. 1309-1316.

Ammar Jameel. He is a MS student in the Computer Engineering Department at Çankaya University/Ankara/Turkey. His research areas are the manner, methods, applications and issues in a cloud of virtual sensors. He is also working as a network administrator in Iraqi Board of Supreme Audit. He received B.Sc. and PGD in Computer Engineering at University of Technology/Baghdad/Iraq. He is a member of the Federation of Arab engineers.

Seda Yuksel. She received her B.Sc. degree in Computer Engineering from Çankaya University/Ankara/Turkey in 2011. She is a M.Sc. student in the Department of Computer Engineering at Çankaya University. She is also externally working as a software engineer for Unify since 2012. Her research interests are in the following areas: database management systems, information security, and security vulnerabilities in software testing.

Ersin Elbasi. Associate Prof. Dr. Ersin Elbasi is currently working for the Department of Digital Game Design at İPEK University. He received MS degree in Computer Science at Syracuse University; MPhil and PhD degrees in Computer Science at Graduate Center, The City University of New York. His research interests include multimedia security, event mining in video sequences and biomedical data mining and analysis.