DIGITAL IMAGE WATERMARKING (DIW) IN WAVELET TRANSFORM DOMAIN AS PROTECTING TECHNOLOGY FOR MULTIMEDIA INTELLECTUAL PROPERTY RIGHTS

Yoiceta Vanda[*]
Achmad Choerudin[**]
Dwiyanto**

ABSTRACT

Digital image can be simply duplicated and distributed rapidly using all of the existing software. The watermarking is a method by hiding a part of information into a digital image on the purpose of protecting the intellectual property right of the image from duplication. In this research, *Digital Image Watermarking* is introduced by taking an advantage from *Wavelet Transform Domain* on purpose to hide the watermark spectrum in the circular form spread in the image. The watermark will be resistant to the existing attacks. The achievement of this research shows the resistance of this method towards the geometrical transformation, and compression of JPEG. The activities include (1) Presenting the definition of *Digital Image Watermarking, Wavelet Transform Domain*, and the ownership of Multimedia Intellectual Property Rights, (2), describing the method of *Digital Image Watermarking* that has been performed in the previous studies and then analyzing the weaknesses and strengths, *(*3) Structuring algorithm of *Digital Image Watermarking* using *Wavelet Transform Domain.* The results then show that (1). Most of societies are not aware of the protecting technology for the Multimedia Intellectual Property Rights and the way of making it. The percentage obtained was at 15.34 % (lowest percentage), (2) Society needs a technique that can be used as the evidence of the ownership of digital image

[*] Lecturer in Electronics Engineering, Department of Electronics Engineering, AUB Technology of College, Surakarta, Central Java, Indonesia.

[**] Lecturer in Mechanical Engineering, Department of Mechanical Engineering, AUB Technology of College, Surakarta, Central Java, Indonesia.

called *Digital Image Watermarking*. Here, the percentage obtained was at 19.02% (highest percentage). Based on the results, it is found that the response of the society with the highest percentage is about the knowledge of the society about the need of *Digital Image Watermarking* method as a protection for Multimedia Intellectual Property Rights. Furthermore, in the second year, DIW was made, given some attacks in the form of rotation, scaling, cropping, JPEG compression, Media Filter and Adaptive Filter.

Index Term-- digital image watermarking, wavelet transform domain, Multimedia Intellectual Property Right, geometric transformation.

INTRODUCTION

The rapid growth of internet has enabled human to unlimitedly access all types of information – particularly for the information in the form of digital data such as image, video, and MP3 that can be easily duplicated and spread as desired. However, this simplicity, in fact, can also be used for negative matters. The spread of the copied digital data, additionally, is hard to be terminated or brought to the lawsuit. This is because the result of the copy highly resembles to the original one. Certain technique, as a consequence, is deemed essential in order to keep the copyright as the intellectual property for the originality and authentication of the data file and to trace the illegal spreading.

To cope with the problem, another technique is also essential to make the originality of the data traceable. This technique is known as watermarking security technique, the aim of which is to protect the copyright by adding mark commonly used to identify the authorized owner. Mark can be in the form of registered number such as UPC: *Universal Producer Number* that can be found on CD, text message, or logo [1]. Meanwhile, the data given watermark generally is in the form of image.

Digital Image Watermarking

The fundamental idea of *Digital Image Watermarking* (DIW) [2, 3] refers to the combination of certain signal and the host image in which the signal is secured and invisible. It is only possible to obtain the signal back if and only if the secret key used in the inserting process is known. Analogically, it is similar with the paper watermark used on paper money that becomes the insight for the application of *Digital Image Watermarking* used to protect digital image. To make it efficient and effective, the watermark system must have the following characteristics [4]:

- *Invisible* – it means that the watermark cannot be identified using human sense or it must not change the characteristics of the original image.
- *Robust* – it means that the *watermark* must be difficult to be vanished even by using the simplest signal operation such as median filter and adaptive filter and by using geometrical distortion such as rotation, cutting and scaling.
- *Unambiguous* - it means that the watermark can only be identifiable by the owner.

Watermarking Systems Model In General

W refers to *watermark* inserted in *I* using special key of *k* and I_ω as the *watermarked image* containing *watermark* [5,6]. The watermarked image after getting an attack is symbolized as $\hat{I}_\omega$. This becomes the purpose of the extracting process by adding watermark into W from I_ω or $\hat{I}_\omega$. It is possible to be done to identify the existence of the watermark in analyzing the image. This can be done in detecting process as seen in Fig. 1.

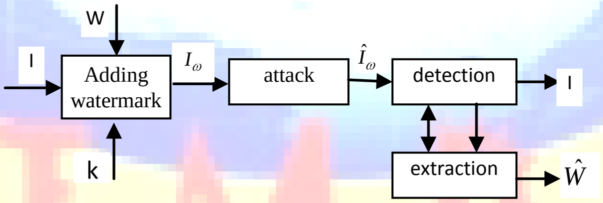

Fig.1: Model Watermarking System in general

Inserting Process

The process of inserting the watermarking [7, 8] is illustrated in Fig. 2. As previously presented, watermark can be inserted through the spatial domain or frequency domain of an image. In addition, it is possible to insert the watermark into the significant components form the image in order to add the strength for the watermark. Fig. 2 shows the uncut lines indicating the process of watermark insertion. Those lines show the selected operation in which the models can commonly be inserted with watermark both in frequency domain or spatial domain. Then, the perceptual analysis is chosen and the method used to insert the watermark commonly is simple. A research is conducted purposely to cover any imperfection from human sight.

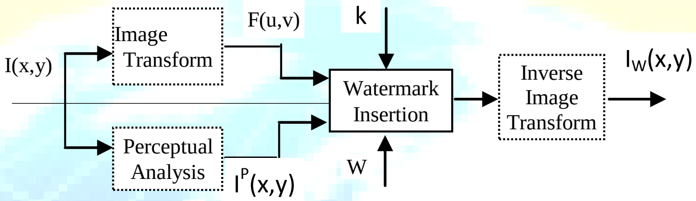

Fig. 2: Watermark Insertion Process

Wavelet transformation

Wavelet refers to small wave that is capable of grouping the energy of image concentrated in a small group of coefficients. Meanwhile, the other group of coefficients only contains less energy that can be vanished without a need to reduce the value of its information [9].

$$\Psi_{a,b}(x) = \frac{1}{\sqrt{a}} \Psi\left(\frac{x-b}{a}\right) \qquad (1)$$

where a = dilated parameter

b = translated parameter

$\frac{1}{\sqrt{a}}$ = normalization of energy equal to the host energy.

The dilated (scaled) and translated (shifted) host *Wavelet* through the separation in accordance with the frequency comes to be subs. To re-obtain the signal, wavelet construction is performed. An image, to illustrate this, is divided into low and high frequency component using *Daubecchies* filter (Fig. 3).

For *G* .G = lower filter (low)

H, H = upper filter (high)

Sub-band = dissimilation and interpolation

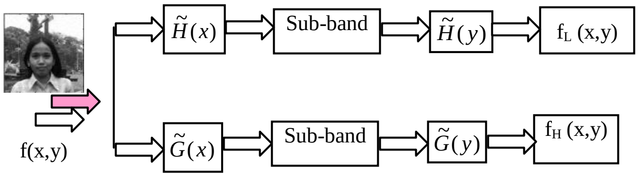

Fig. 3: Block diagram of the frequency splitting

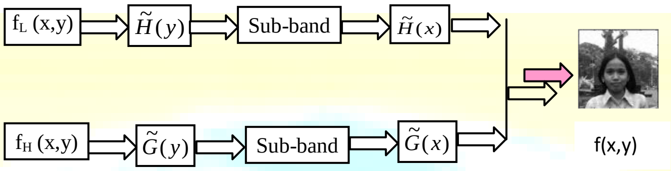

Fig. 4: Block diagram of frequency reconstruction

Attacks in Watermarking

Attack or disturbance in watermarking technique [10, 11] refers to all attempts to depart the mark data. After the mark data can be disappeared, it then is possible to copy and to distribute the image. The common attack in watermarking technique is geometrical transformation (scaling, rotating, cutting and compressing).

Scaling

An axis scaling in a spatial domain can result in a conversion of scaling in wavelet domain, in this case for two scalars of *a* and *b* as stated below:

$$I(ax,by) \leftrightarrow \frac{1}{|ab|}F\left(\frac{u}{a},\frac{v}{b}\right) \qquad (2)$$

In Matlab for scaling, the function of *imresize* is used to change the size of the image using interpolation method.

Rotation

If the pair of SWT and ISWT is presented in the polar coordinate [Licks, 1999] as

$$\begin{aligned} x &= r\cos\theta, \; y = r\sin\theta \\ u &= w\cos\phi, \; v = w\sin\phi \end{aligned} \qquad (3)$$

The form of notation I (x,y) and F(u,v) comes to be I(r,θ) and F(W,ϕ). The rotation of the image with the angle of θ_0 can lead the watermarking to rotate with a similar angle as follows:

$$I(r, \theta + \theta_0) \leftrightarrow F(w, \phi + \theta_0) \qquad (4)$$

Matlab uses the function of *imrotate* to turn the image using the method of *nearest neighbor interpolation*.

Cropping

If F(u,v) and I(x,y) are the periodic function with N period, there will be a relation as follows:

$$F(u,v) = F(u+N,v+N) \qquad (5.a)$$

$$I(x,y) = I(x+N,y+N) \qquad (5.b)$$

Furthermore, in the conjugation symmetry, it is found that lF (u, v)l = lF(-u,-v)l, thus in the cropping, there will be a relation as follows:

$$I(x-N, y-N) \leftrightarrow F(u-N, v-N) \qquad (6)$$

Matlab uses the function of *imcrop* to extract the part of the box of an image. The determination of the box can be conducted through the input or by selecting using mouse.

Compression

Compression [12, 13] in JPEG image is performed by dividing the image into the blocks sized at 8X8 or 16x16. Subsequently, two-dimensional DCT (*discrete cosine transforms*) is used to calculate each of the blocks. The obtained coefficient of DCT will be then quantified, coded and transmitted. At JPEG, *receiver* or *file* of JPEG *reader*, it is done by coding the coefficient of DCT quantization, calculating the invers of DCT in each block and placing the blocks in order to create a new image. For the image with the value approaching zero, its values can be disappear. From this fact, the compression can be analogized using the scaling process. For the wavelet transformation, a relation will take place as follows:

$$I(a_m x_i, b_n y_j) \leftrightarrow \frac{1}{|a_m b_n|} F\left(\frac{u_i}{a_m}, \frac{v_j}{b_n}\right) \qquad (7)$$

RESEARCH METHOD

Research Materials

The research materials used are the original images including kiddy2.jpeg, ary71.jpeg, kid3.jpeg, kidir2.jpeg, kidin3.jpeg, kidjem2.jpeg. Those images were obtained from capturing the image using the digital camera in which it was cut into the 256 x 256 pixels.

Research Devices

The devices used in this research included the computer hardware with the specification of *Processor Intel Celeron* 233 MHz, RAM 128 MB, *Hardisk* 40 GB, and the adapter of VGA with the 24-bit color resolution. Meanwhile, the software used included *Malab 6.5* and *Adobe Photoshop 6.0.*

Research Method

Quantitative and qualitative assessments (subjective) were given for the image as a result of watermarking process. Here, the quantitative assessment was based on the statistic of the image and the qualitative one was based on the perception of the human sight on the image. The results of both two assessments were then supported with the comparative method.

Research Process

The values of the map of some images coming from the editing process of using *Adobe Photoshop* were changed from color images to grayscale ones using the Matlab program that is by giving the following value of RGB: R(*red*)=0,2290, G(*green*)=0,5870, and B(*blue*)=0,1140.

The *grayscale* in Matlab was in the form of matrix values. The image sized at 256 x 256 pixels was in the form of matrix with the size of 256 rows x 256 columns. Meanwhile, the data text was in the form of a group of letters from *a* to z, 0 – 9 and some of commonly used punctuations and spaces. The selected characters were then changed into the binary letters 0 and 1 with the code of one character replaced by 6 bits.

The original image was decomposed using *wavelet transform* that resulted in the approximate values and 3 details (vertical, horizontal and diagonal). Furthermore, the mark data and security data were inserted into the wavelet transform. This is what actually is called the *watermarking* process as seen in Fig. 5(a).

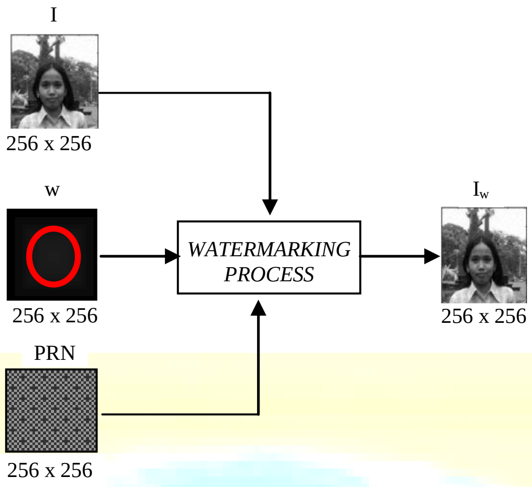

Figure 5. Watermarking process

After combining into one, the data would be stored and used as the final result of *watermarking*. The correlation value between the original image and the watermarking image subsequently was measured. If the change occurred was not significant for its appearance, it was then said that the watermarking process was successfully performed. When this combination was completely done, the inverting process was performed by decomposing the images inserted into the watermarking images in order to obtain the inserted mark data as seen in Fig. 6.

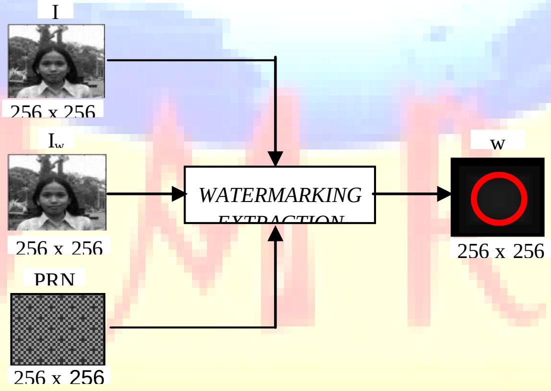

Figure 6. Watermarking extraction

RESULT AND DISCUSSION

To determine the form of the mark data that would be made, we must determine the value of R that is the radian value that must be sought in order to make the mark data suitable as expected. Subsequently, the value of Alpha as the supporting value was sought in order to improve the display of mark data and the maximum number of characters that can be written. Of the experiments performed, it was found that the suitable value of R was around the values of 100, the suitable value of alpha was 12000 and the number of characters that could be written was 32. Following this, the mark data that had been made was inserted into the original image (Fig. 7 (a) and Fig. 7 (b)).

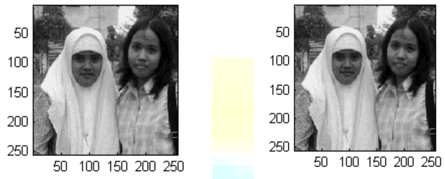

Figure 7 (a). Original Image, (b). Watermarking Image

Attack in watermarking

Watermarking image that has been created in the process of decomposing SWT would be given a number of attacking treatments. This was aimed to test the resistance of the created watermarking technique from the external effects. The attack in watermarking technique included geometrical transform such as scaling, rotating and cutting. Other attacks could also include adaptive filter and median filter.

Image scaling

Scaling refers to the size transform of the watermarking image (bmp) created from the original image and watermark in the size of 256 x 256. The size of image is transformed into 400 x 400. Thus, it could be seen whether the text data inserted into the original image is still intact or not.

Image rotation

Rotation is the change of the form due to the rotation of the watermarking image (bmp) resulted from the original image in the size of 256 x 256. The image was rotated clockwise (negative angle) and counterclockwise (positive angle). In this experiment, the image was rotated with the angles of–30º, 30º, 60º, 180º, 270º, and 300º.

Cropping Image

Cropping in the image was performed in watermarking image. It was to test the text data inserted into the original image. The watermarking image in the size of 256 x 256 was cropped into 100 x 100

Median filter

Filtering in digital image refers to the modification technique to improve the image quality. In common, filtering an image is used to remove certain features. It is also used to remove the noise. Filtering in watermarking technique frequently is used by the attackers to weaken or remove the mark data inside.

Table 1: Correlation value of the original image with the image watermarking in determining the degree of decomposition of SWT

Dekomp.	Rekons.	Corr W	Corr M	SNR W	PSNR W	SNR M	PSNR M
1	1	0.9418	0.7324	8.8493	57.0141	-3.2011	44.5698
3	3	0.9903	0.6726	18.3205	66.4865	-3.1590	45.0035
5	5	0.9961	0.9778	22.7305	70.1236	-3.3561	45.6321
7	7	0.9982	0.9766	25.6346	73.1458	-3.1256	44.5689
9	9	0.9989	0.9751	27.8085	75.1236	-3.1478	44.4561
11	11	0.9992	0.9737	29.2356	77.1235	-3.5698	44.9652
13	13	0.9994	0.9701	30.2589	79.1041	-3.1234	45.1236
15	15	0.9996	0.9691	32.0147	80.2369	-3.2345	44.4789
17	17	0.9997	0.9648	33.2156	81.2356	-3.5694	44.4569
19	19	0.9998	0.9632	67.0258	82.0145	-3.1258	44.9400
20	20	0.9998	0.9588	34.1236	82.0148	-3.4569	45.6321
21	21	0.9998	0.9581	34.0189	83.1258	-3.1245	44.7890
23	23	0.9998	0.9853	36.1258	84.1270	-3.2258	44.1258
24	24	0.9999	0.9507	36.9986	84.6952	-3.1698	44.7769
26	26	0.9998	0.9497	37.5556	86.2356	-3.1478	44.9631
27	27	0.9999	0.9504	37.1546	86.1245	-3.5894	44.6821
29	29	0.9999	0.9467	38.3692	86.1478	-3.6698	77.1456
30	30	0.9998	0.9417	38.1254	86.1124	-2.7895	45.1236
35	35	0.9999	0.9349	36.1112	86.1254	-2.5681	45.7891
40	40	0.9999	0.9188	16.4729	87.1258	-3.1479	45.3125

Table 2: Correlation value, SNR, and PSNR in the Scaling Process

skala	corr W	corr M	SNR	PSNR	SNR	PSNR
300	0.9999	0.9393	12,105	61,647	2,921	52,468
400	0.9999	0.9378	12,101	64,123	2,889	54,930
500	0.9999	0.9387	12,102	66,081	2,886	56,864
600	0.9999	0.9393	12,103	67,664	2,891	58,453
700	0.9999	0.9384	12,104	69,006	2,913	59,815
800	0.9999	0.9389	12,102	70,154	2,892	60,954
900	0.9999	0.9383	12,103	71,187	2,901	61,986
1000	0.9999	0.9387	12,103	72,103	2,903	62,903

Table 3: Correlation value, SNR, and PSNR in Cropping Process

Crop	Corr W	Corr	SNR	PSNR	SNR	PSNR
800	0.9998	0.9405	12,104	70,166	0,7630	58,842
700	0.9998	0.9409	12,129	69,301	0,9401	57,841
600	0.9997	0.9399	12,143	67,706	1,739	57,302
500	0.9996	0.9396	12,097	66,076	0,066	53,913
400	0.9996	0.9301	12,387	64,428	8,729	60,770
300	0.9997	0.9036	12,421	61,963	9,928	59,525
256	0.9992	0.9083	12,211	60,384	3,392	51,557
200	0.9996	0.9092	12,393	58,414	9,219	55,240
100	0.9999	0.3677	12,386	52,381	9,095	49,095

CONCLUSION

1. *Digital Image Watermarking* (DIW) by means of the advantage of wavelet transformation can result in the best watermarking technique with the value of correlation approaching 1 (0.9999) when the value of the decomposition 26 uses SWT2 (*Stationary Wavelet Transform* 2).
2. In the scaling process, the quality of the watermarking image can decrease that is when the image is transformed into the larger or smaller size. Though not significant, it is still considered that wavelet transformation is resistant to the scaling attack.
3. In common, the rotation process cannot cause the change on the watermarking image quality. Conversely, the quality change of the watermark with the angle limit of 180^0 took place. It can be said then that the watermarking technique in the wavelet transformation is resistant to the rotation attack.

4. The quality decrease of the watermarking image occurs in the cropping process. In this process, the mark data inserted is cropped in which the results of the mark extraction remain a few of characters depending upon the size of the cropping. This, however, can be coped with by inserting the watermark that has few characters. It can be said that the watermarking technique made in the wavelet domain is resistant to the cropping attack.
5. *Watermarking* image given with the median filter experienced the decrease of quality when using block [5 5] and so on along with the increase of the block size. The characters of the inserted watermark would vanish one by one. However, it can be handled by giving the length of the characters not more than 13 characters.
6. The compressing process can cause the decrease of watermark quality but for the watermarking image quality, it is not so significant up to the value of quality 10. It can be said then that the watermarking technique made in this wavelet domain is resistant to the compressing attack.

ACKNOWLEDGMENT

Authors thank to Directorate General Higher Education for financially supporting this research during 2 years in the program of *Hibah Bersaing*.

REFERENCES

[1] Anderson, R.J. and F.A.P. Petitcolas, Information Hiding – An Annotated Bibliography, at http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography.

[2] Boland, F.M, J.J.K. Ó.Ruanaidh and W.J. Dowling, 1996, Watermarking digital images for copyright protection", IEE Proceedings on Vision, Signal and Image Processing, 143(4), pp. 250-256.

[3] Bruyndonckx, O, J.J. Quisquater, and B. Macq, 1995, Spatial method for copyright labeling of digital images", In Proc. IEEE Workshop Nonlinear Signal and Image Processing, Halkidiki, Greece.

[4] Cox, I, J. Kilian, T. Leighton and T. Shamoon, Secure Spread Spectrum Watermarking for Multimedia, Technical Report 95-10, NEC Research Institute.

[5] Hartono, 2000, Cap Air Digital Sebagai Tanda Pengenal Citra Digital, Final Task of Electrical Engineering of UGM.

[6] Hartung, F. and M. Kutter, 1999, Multimedia Watermarking Techniques, In Proc. IEEE, 97(7), pp. 1079-1107.

[7] Heileman, G.L, C.E. Pizano and C.T. Abdallah, 1999, Image Watermarking for Copyright Protection", In Lecture Notes in Computer Science 1619, Algorithm Engineering and Experimentation: International Workshop ALENEX'99, Springer-Verlag, Berlin, pp. 226-245.

[8] Koch, E. and J. Zhao, 1995, Toward robust and hidden image copyright labeling", in Proc. Workshop Nonlinear Signal and Image Processing, Greece.

[9] Kusban, Muhammad, 2002, Digital Watermarking Dalam Kawasan Alihragam Wavelet, Thesis for the Program Study of Electro UGM.

[10] Kutter, M. and F.A.P. Petitcolas, 1999, A fair benchmark for image watermarking systems", Electronic Imaging '99 – Security and Watermarking of Multimedia Contents, 3657, San Jose, United States.

[11] Kutter, M. Watermarking resisting to translation, rotation and scaling, in http://ltssg3.epfl.ch:1248/kutter/watermarking/#publications.

[12] Licks, Vinicius, 1999. On Digital watermarking robust to geometric transformations, Thesis, B.S., Control Enginnering, Pontificia Universdade Catoloic, Brasil.

[13] Meerwald, Peter, 2001. Digital Image watermarking in the wavelet transform domain', diplomarbeit, zur Erlangung des Diplomgrades an der Naturwissenschaftlichen Faculty of Salzburg.

[14] Pereira, S, J.J.K.O. Ruanaidh, T. Pun, Secure Robust Digital Watermarking Using the Lapped Orthogonal Transform.

[15] Petitcolas, F.A.P, R.J. Anderson and M.G. Kuhn, 1999, Information Hiding – A Survey, in Proc. IEEE, 87(7), pp. 1062-1078.

[16] Pickholtz, R.L, D.L. Schilling and L.B. Milstein, Theory of Spread-Spectrum Communications – A Tutorial, In IEEE Trans. Comm., COM-30(5).

[17] Ruanaidh, J.J.K.O. and T. Pun, 1998, Rotation, scale and translation invariant spread spectrum digital image watermarking, Signal Processing, 66(3), pp. 303-318.

[18] Ruanaidh, J.J.K.O. and T. Pun, 1997, Rotation, Scale and Translation Invariant Digital Image Watermarking, IEEE International Conference on Image Processing, pp. 536-539, Santa Barbara.

[19] Ruanaidh, J. œ, W.J. Dowling and F.M. Boland, 1996, Phase watermarking of digital images, In Proceedings of ICIP’96, III, pp. 239-242, Lausanne, Switzerland.

[20] Smith, J. and B. Comiskey, 1996, Modulation and information hiding in images, in Proc. First International Workshop on Information Hiding, Lecture Notes on Computer Science, Cambridge, UK, pp. 207-226.

[21] Solachidis, V. and I. Pitas, 1999, Circularly symmetric watermark embedding in 2-D DFT domain”, IEEE Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP’99), Phoenix, 6, pp. 3469 -3472.

[31] Tirkel, A, G. Rankin, R. van Schyndel, W. Ho, N. Mee, and C. Osborne, 1993, Electronic water mark, in Proc. DICTA 1993, pp. 666-672.

[32] Voyatzis, G. and I. Pitas, 1999, The Use of Watermarks in the Protection of Digital Multimedia Products, in Proc. IEEE, 87(7), pp. 1197-1207.

IJMRA