ISSN: 2277-9655
Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Prosperous Digital Image Watermarking Approach by using DCT-DWT

Mr.Prabhakar C. Dhavale[*1], Mrs.Meenakshi M. Pawar[2]
[*1,2] Department of Electronics and Communication Engineering, Sveri, Coe-Pandharpur, Solapur, Maharashtra, India
prabhakar1599@gmail.com

Abstract

In this paper, Everyday tons of data is embedded on digital media or distributed over the internet. The data so Distributed can easily be replicated without error, putting the rights of their owners at risk. Even when encrypted for distribution, data can easily be decrypted and copied. One way to discourage illegal duplication is to insert information known as watermark, into potentially valuable data in such a way that it is impossible to separate the watermark from the data. These challenges motivated researchers to carry out intense research in the field of watermarking.

A watermark is a form, image or text that is impressed onto paper, which provides evidence of its Authenticity. Digital watermarking is an extension of the same concept. There are two types of watermarks visible watermark and invisible watermark. In this project we have concentrated on implementing watermark in image. The main consideration for any watermarking scheme is its robustness to various attacks

Keywords: Digital image, Copyright protection, Watermarking, Wavelet transform.

Introduction

Information hiding can be mainly divided into three processes -cryptography, stenography and watermarks. Cryptography is the process of converting information to an unintelligible form so that only the authorized person with the key can decipher it. As many advances were made in the field of communication it became rather simple to decrypt a cipher text. Hence more sophisticated methods were designed to offer better security than what cryptography could offer. This led to the discovery of stenography and watermarking. Stenography is the process of hiding information over a cover object such that the hidden information cannot be perceived by the user. Thus even the existence of secret information is not known to the attacker. Watermarking is closely related to stenography, but in watermarking the hidden information is usually related to the cover object. Hence it is mainly used for copyright protection and owner authentication.

Overviews on watermarking techniques can be found in (Langelaar et al., 2000) [3].

Watermarking techniques can be broadly classified into two categories: such as spatial domain methods [10][11] and transform domain methods [12][13]. Spatial domain methods are less complex as no transform is used, but are not robust against attacks. Transform domain watermarking techniques are more robust in comparison to spatial domain methods. This is due to the fact when image is inverse wavelet transformed watermark is distributed irregularly over the image, making the attacker difficult to read or modify. Among the transform domain watermarking techniques discrete wavelet transform (DWT) based watermarking techniques are gaining more popularity because DWT has a number of advantages over other transform. As many advances are made in the field of communication it became rather simple to decrypt a cipher text. Hence more sophisticated methods are designed to offer better security than what cryptography can offer. This led to the discovery of stenography and watermarking. Stenography is the process of hiding information over a cover object such that the hidden information cannot be perceived by the user. Watermarking is closely related to steganography, but in watermarking the hidden information is usually related to the cover object. Hence it is mainly used for copyright protection and owner authentication. Figure 1 explains how watermarking is derived from steganography.

ISSN: 2277-9655
Impact Factor: 1.852

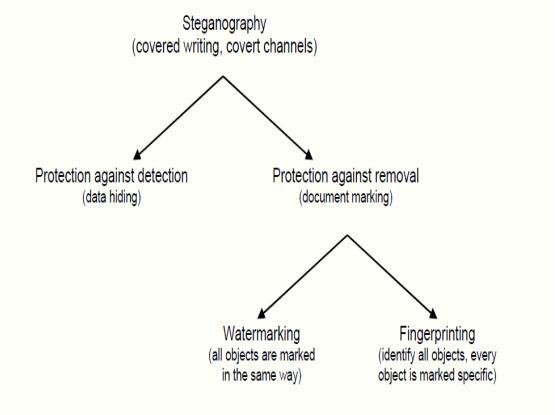

Fig.1 Types of Steganography [14]

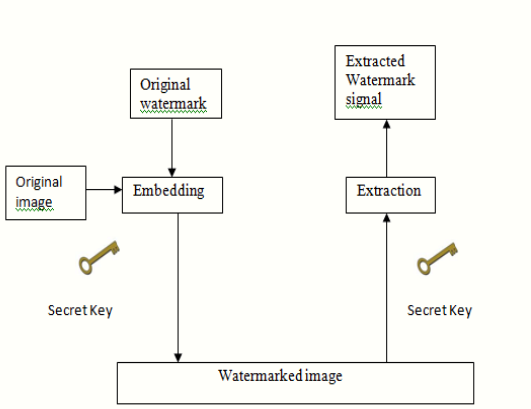

Figure 2. basic block diagram of watermarking process.

Principle of Watermarking

This section gives an overview of the numerous wavelet based digital watermarking techniques that have been developed to help protect the copyright of digital images and to verify multimedia data integrity. Most watermarking techniques transform the host image into a domain that facilitates embedding of the watermark information in a robust and imperceptible way.

The following principal embedding strategies that can be used to embed a watermark in a host image. A watermarking system is usually divided into three distinct steps, embedding, attack and detection. In embedding, an algorithm accepts the host and the data to be embedded and produces a watermarked signal. The watermarked signal is then transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called an attack. There are many possible attacks. Detection is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was not modified during transmission, then the watermark is still present and it can be extracted. If the signal is copied, then the information is also carried in the copy. The embedding takes place by manipulating the content of the digital data, which means the information is not embedded in the frame around the data, it is carried with the signal itself. Figure 2 shows the basic block diagram of watermarking process.

The original image and the desired watermark are embedded using one of the various schemes that are currently available. The obtained watermarked image is passed through a decoder in which usually a reverse process to that employed during the embedding stage is applied to retrieve the watermark. The different techniques differ in the way in which it embeds the watermark on to the cover object. A secret key is used during the embedding and the extraction process in order to prevent illegal access to the watermark. These techniques are used in application like

A. Copyright Protection.
B. Authentication.
C. Broadcast Monitoring.
D. Content Labelling.

Techniques or Schemes of Watermarking.

Spatial Domain Techniques:-

In Spatial domain watermarking slightly modifies the pixels of one or two randomly selected subsets of an image. Modifications might include flipping the low-order bit of each pixel. However, this technique is not reliable when subjected to normal media operations such as filtering or lossy compression [10].

Least Significant Bit Coding (LSB) :-

LSB coding is one of the earliest methods. It can be applied to any form of watermarking. In this method the LSB of the carrier signal is substituted with the watermark. The bits are embedded in a sequence which acts as the key. In order to retrieve it back this sequence should be known. The watermark encoder first selects a subset of pixel values on which the watermark has to be embedded. It then embeds the information on the LSBs of the pixels from this subset. LSB coding is a very simple technique but the robustness of the

ISSN: 2277-9655
Impact Factor: 1.852

watermark will be too low. With LSB coding almost always the watermark cannot be retrieved.

Predictive Coding Schemes :-

Predictive coding scheme was proposed by Matsui and Tanaka in [8] for gray scale images. In this method the correlation between adjacent pixels are exploited. A set of pixels where the watermark has to be embedded is chosen and alternate pixels are replaced by the difference between the adjacent pixels. This can be further improved by adding a constant to all the differences. A cipher key is created which enables the retrieval of the embedded watermark at the receiver. This is much more robust when compared to LSB coding.

Patchwork Techniques:-

In patchwork watermarking, the image is divided into two subsets. One feature or an operation is chosen and it is applied to these two subsets in the opposite direction. For instance if one subset is increased by a factor k, the other subset will be decreased by the same amount. If a[i] is the value of the sample at I in subset 'A' which is increased and b*i+ is the value of the sample in the subset 'B' whose value is decreased, then the difference between the two subsets would intuitively result in

$\sum(a[i]-b[i]) = 2N$ for watermarked images
$= 0$ otherwise

Discrete cosine transform (DCT) based technique:-

Discrete cosine transform (DCT): It is a process which converts a sequence of data points in the spatial domain to a sum of sine and cosine waveforms with different amplitudes in the frequency domain. The DCT is a linear transform, which maps an n-dimensional vector to set of n coefficients. A linear combination of n known basis vectors weighted with the n coefficients will result in the original vector. The known basis vectors of transforms from this class are "sinusoidal", which means that they can be represented by sinus shaped waves or, in other words, they are strongly localized in the frequency spectrum. Therefore one speaks about transformation to the frequency domain. The most popular member of this class is the Discrete Fourier Transformation (DFT).The difference between DCT and DFT is that DFT applies to complex numbers, while DCT uses just real numbers. For real input data with even symmetry DCT and DFT are equivalent. There are eight different variants of DCT. There is a very slight modification between these eight variants. [12] [13] .

There are some DCT levels are explained in this paper

DCT –I :-

In JPEG compression the input data are two-dimensional, presented in 8x8 blocks. There's a need of using two-dimensional DCT. Since each dimension can be handled separately, the two-dimensional DCT follows straightforward form the one-dimensional DCT. A one-dimensional DCT is performed along the rows and then along the columns, or vice versa.

DCT –II :-

$$F(u,v)=C(u)C(v)\sum_{x=0}^{N-1}\sum_{y=0}^{M-1} f(x,y)\cos\left|\frac{\pi(2x+1)u}{2N}\right|\cos\left|\frac{\pi(2y+1)v}{2N}\right|$$

$$where\ u=0,1,\ldots N-1 \quad v=0,1,\ldots M-1$$

$$C(u),C(v)=\sqrt{\frac{1}{N}}\ when\ u,v=0 \quad C(u),C(v)=\sqrt{\frac{2}{N}}\ when\ u,v\neq 0$$

Eq. 1 and 2

Applying these formulas directly requires much computational resources therefore an implementation in hardware can be very efficient.

The figure 3, shows example of 8x8 block before DCT.

75	76	75	75	69	66	77	71
73	74	73	74	63	64	68	69
69	68	71	72	67	58	48	41
59	55	56	52	47	40	24	9
51	50	45	41	33	22	7	-5
43	37	32	24	15	5	-6	-25
29	21	9	-2	-10	-21	-44	-69
9	-4	-17	-35	-52	-61	-57	-35

Fig 3. 8x8 block before DCT.

After Discrete Cosine Transform the block has following values

251	118	-13	6	-2	6	-1	0
279	-68	-8	-7	-1	4	-4	-1
-51	-14	34	-14	5	0	-1	0
27	5	-10	8	-7	4	-5	1
-22	-7	14	-9	4	-2	1	1
-3	15	-18	15	-6	2	-1	2
7	-9	6	-6	4	0	0	2
3	7	-9	3	0	-2	-1	0

Fig 4.8x8 block after DCT of fig 3.[10]

As it can be seen higher values of transform coefficients are concentrated on the top left corner. In the frequency domain it looks like low frequency has advantage over high frequency. It is shown on the figure 4

ISSN: 2277-9655
Impact Factor: 1.852

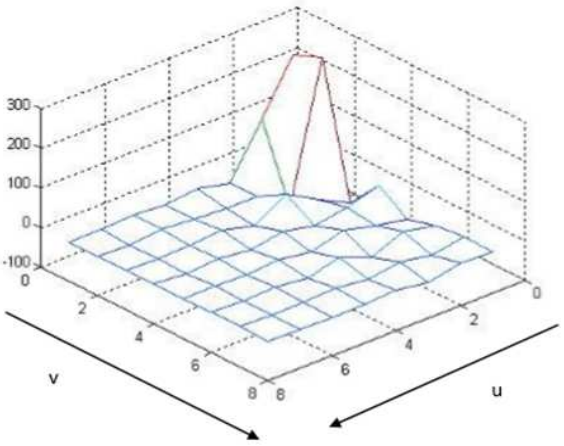

Fig 5.Frequency Map

As you can see only small amount of low frequency elements dominates over the rest of the coefficients. It allows reducing data during next stages of JPEG compression.

The main advantage of DCT which makes it attractive for watermarking is its energy compaction property. This property divides the image into distinct frequency bands which makes it easy to embed the watermark in the desired area of the image. Most of the energy in the DCT domain is concentrated in the low frequencies. As is known low frequencies are perceived very well by human eye, hence the chances of the watermark being perceptible is high where as high frequencies are prone to attacks such as compression and scaling. So, a trade-off has to be made.

Wavelet Based Watermarking Techniques

This section gives an overview of the numerous wavelet based digital watermarking techniques that have been developed to help protect the copyright of digital images and to verify multimedia data integrity. Most watermarking techniques transform the host image into a domain that facilitates embedding of the watermark information in a robust and imperceptible way. The following principal embedding strategies that can be used to embed a watermark in a host image:

1. Linear additive embedding
   i. Gaussian sequence
   ii. Image fusion
2. Non-linear quantization embedding, via
   i. Scalar quantization
   ii. Vector quantization
3. Miscellaneous embedding techniques

Additive embedding strategies are characterized by the linear modification of the host image and the correlative processing in the detection stage. The quantization schemes on the other hand perform non-linear modifications and detect the embedded message by quantizing the received samples to map them to the nearest reconstruction point [13].

Implemented Techniques

We studied in detail and implemented two wavelet domain techniques proposed in [14][15], in order to compare which technique is more robust for copyright protection of intellectual property.

A . *A New Robust Watermark Embedding into Wavelet DC Components [1].*

Embedding: Joo's [1] watermarking technique embed watermarks into the DC area while preserving good quality fidelity. The gray image is decomposed into several bands by wavelet transform. To embed watermark i.e. a pseudo-random binary sequence {-1,1}, a reference DC′ is prepared by taking low pass filtering to the original DC. The DC values are changed to values smaller or larger than the DC′ values in accordance with the corresponding watermark bits. To reduce image degradation, the watermark bits are embedded into locations with smaller differences between the DC and DC′. This is depicted in the Fig. 1.

Extraction: In extraction Joo [1] used the original image as required in extracting watermarks. Such an extraction is classified as non-blind watermarking. The same wavelet decomposition is applied to both the original and embedded images. The watermark-embedding locations are obtained from the original image. Since LLn and LLn' are obtained from the watermark embedded image, the watermarks are extracted by comparing the two values, LLn and LLn'. Then the extracted watermarks are compared with the original watermarks generated by the user key. In this comparison, Joo [1] used the similarity measure given in (2), where '.' denotes the inner product.

$$Sim(w, w^*) = \frac{w \cdot w^*}{\sqrt{w^* . w}} \quad (3)$$

B. A Robust watermarking method for copyright Protection of Digital Images using Wavelet domain [2]

Embedding: Dote's [2] presented a multilevel wavelet transformation technique. The host image and watermark are transformed into wavelet domain. Dote [2] selected 5th level transformation for host image and 1st level for watermark. The transformed watermark coefficients were embedded into those of host image at each resolution level with a secret key. The Dote's [2] technique is depicted in the Fig. 6.

ISSN: 2277-9655
Impact Factor: 1.852

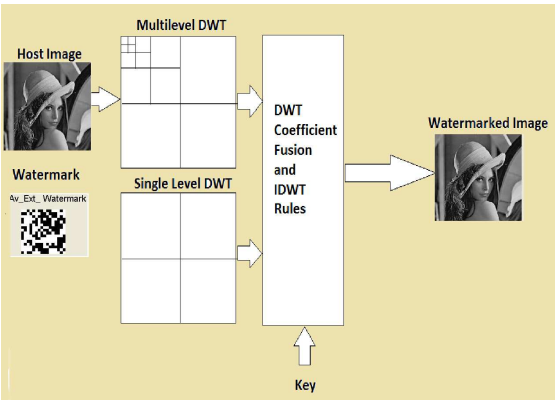

Fig. 6 proposed method by Dote's

Extraction: Dote [2] extracted the watermark by applying inverse procedure at each resolution level using the same secret key. Estimated the watermark by averaging the extracted watermarks and normalize it for binary values. In order to find out similarity between embedded and extracted watermarks first Dote [1] observed the host and the marked images perceptually. The correlation coefficients between them at different signal to noise ratios (SNR) values were calculated.

The correlation coefficient, , used for similarity measurement, and SNR are defined in (4) and (5).

$$\rho(w,\hat{w}) = \frac{\sum_{i=1}^{N} w_i \hat{w}_i}{\sqrt{\sum_{i=1}^{N} w_i^2}\sqrt{\sum_{i=1}^{N} \hat{w}_i^2}} \qquad (4)$$

$$SNR(W,\hat{W}) = 10\log_{10}\frac{\sum_{i=1}^{N} w_i^2}{\sum_{i=1}^{N}(W_i - \hat{W}_i)^2} \qquad (5)$$

Where N is the number of pixels in watermark, w and are the original and extracted watermarks, respectively. The related measure of PSNR (in db) between host and marked image is computed using

PSNR = 20log10 [255/RMSE]

Where

$$RMSE = \sqrt{\frac{1}{M*N}\sum_{i=1}^{M}\sum_{j=1}^{N}[\tilde{f}(m,n) - f(m,n)]^2}$$

Eq (6) for the 8-bit (0-255)image.

Experimental Results

In our experiments for Joo [1] and Dote [2] techniques, we performed fidelity tests to analyze the unobtrusiveness of the watermarks after watermark embedding, whether perceptual distortion occurred to the host images or not. Also we tested the robustness against standard noise attacks i. e. Gaussian, salt and pepper, Speckle and JPEG compression to the marked images. For our results we supposed that the correlation coefficient of about 0.75 or above is assumed as an acceptable value for the extracted watermarks from noisy images.

For Joo's [1] technique a pseudo-random binary sequence is used as a watermark. Sequence is generated from seed no. 500 of length 1000. The watermarks are embedded in the 512*512 gray-level Lena image. A three level DWT is employed and thus the size of the DC area to be embedded is 64*64. We set K to 28, the resulting PSNR was 43.08db. The host image, watermarked image, watermark, and extracted watermark are shown in Fig. 7.

Fig. 7 Fidelity test on Joo's technique

There is no perceptual distortion in the original and watermarked image, which means that scheme has satisfied the criteria that an efficient watermark should be unobtrusive, discreet and easily extracted.

For robustness, the obtained PSNRs between host image and watermarked images under standard noise degradations, between original watermark and extracted watermarks and the correlation coefficients were calculated, respectively as shown in Table I.

ISSN: 2277-9655
Impact Factor: 1.852

TABLE I
EFFECT OF NOISE ATTACKS ON JOO'S TECHNIQUE

Attacks	Images PSNRs	Watermarks PSNRs	Correlation Coefficients
Gaussian	25.59	10.14	0.89
Salt & pepper	34.99	14.44	0.99
Speckle	36.33	15.83	0.99
JPEG	35.86	17.75	0.98

The watermarked images and extracted watermarks after Gaussian, salt and pepper, Speckle and JPEG noise distortion are shown in the Fig. 8.

Fig. 8 Noise distortion attacks on Joo's Technique

For Dote's [2] technique we choose 256*256 gray intensity image and 16*16 binary watermark which is randomly generated. We set key to 500, the resulting PSNR was 47.27db. The original image, watermarked image, watermark, extracted watermark are shown in Fig. 9.

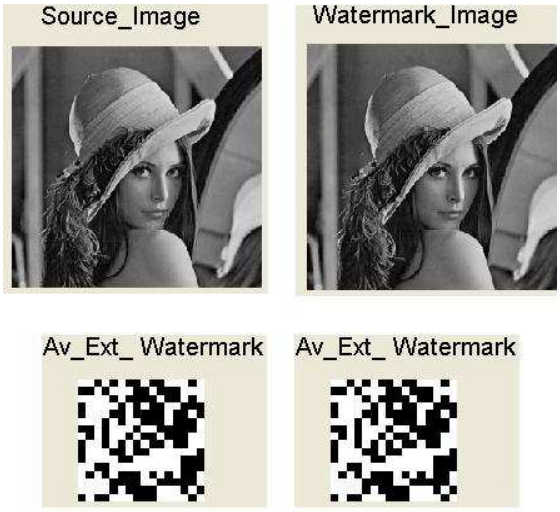

Fig. 9 Fidelity test on Dote's technique

There is no perceptual distortion in the original and watermarked image, which means that scheme has satisfied the criteria that an efficient watermark should be unobtrusive, discreet and easily extracted.

For robustness, the obtained PSNRs between host image and watermarked images under standard noise degradations, between original watermark and extracted watermarks and the correlation coefficients were calculated, respectively as shown in Table II.

TABLE II
EFFECT OF NOISE ATTACKS ON DOTE'S TECHNIQUE

Attacks	Images PSNRs	Watermarks PSNRs	Correlation Coefficients
Gaussian	25.83	4.54	0.38
Salt and pepper	34.46	6.52	0.57
Speckle	31.28	4.78	0.33
JPEG	34.35	6.22	0.56

The watermarked images and extracted watermarks after Gaussian, salt and pepper, Speckle and JPEG noise distortion are shown in the Fig. 10.

ISSN: 2277-9655
Impact Factor: 1.852

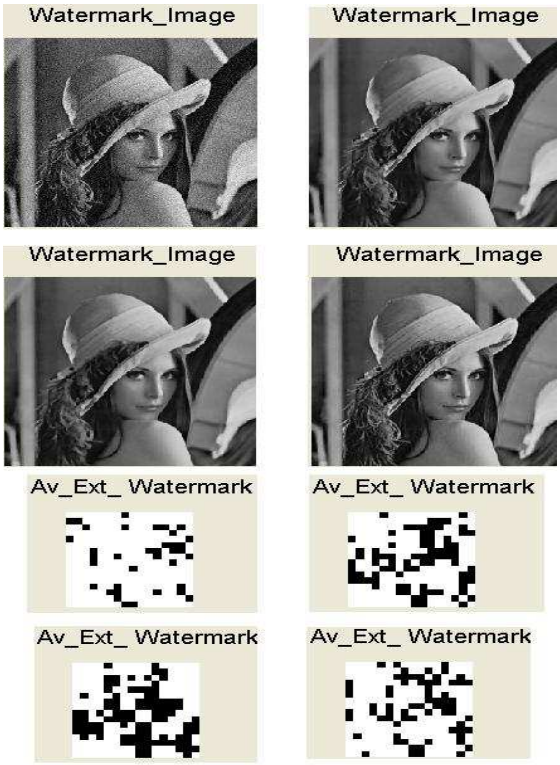

Fig. 10. Noise distortion attacks on Dote's Technique.

Through experimental results, for fidelity test, we were able to strongly embed watermarks while preserving good fidelity in both Joo [1] and Dote's [2] techniques. While for robustness, we found Joo's [1] technique more robust than Dote's [2] technique under standard noise degradation i. e. Gaussian, salt and pepper, Speckle and JPEG, by comparing correlation coefficients values of Table I with Table II.

Conclusion

We review the various watermarking techniques in the wavelet transform domain. We simulated two of the techniques in detail to analyze the robustness for copyright scenario. Both the techniques were found non-obtrusive in gray level images. For robustness, Joo's [1] technique shows better results when compared with Dote's [2] technique. We extracted the watermarks from the noisy images to an acceptable degree of correlation in Joo's [1] technique. Therefore, we say that Joo's [1] technique has coped the added noise degradation and is more robust for such standard attacks.

Acknowledgments

We thank to Sveri COE, Pahandharpur for providing very conducive research environment support

References

[1] Sanghyun Joo, Youngho Suh, Jaeho Shin, and Hisakazu Kikuchi, A New Robust Watermarking Embedding into Wavelet DC Components, ETRI Journal, Volume 24, No. 5, October 2002.

[2] Yasuhiko Dote, and Muhammad Shafique Shaikh A Robust Watermarking Method for Copyright Prot. of Digital Images using Wavelet Trans. Trans. of the Institute of electrical Engineering of Japan, vol. 122, No.2, Jan. 2003.

[3] Langelaar, G.C., Setyawan, I., Lagendijik, R.I., 2000. Watermarking digital image and video data. IEEE signal Process. Magazine (September), 20-46

[4] A. G. Bors and I. Pitas., Image watermarking using DCT domain constraints, Proc. of IEEE Int. Conf. on Image Processing, vol. 3, pp. 231-234 (1996).

[5] R.G. van Schyndel, A. Z. Tirkel, and C. F. Osborne, A digital watermark, Proc. of Int. Conf. in Image Processing, vol. 2, pp. 86-90, (1994).

[6] J. Ohnishi and K. Matsui, Embedding a seal into a picture under orthogonal wavelet transformation, Proc. of Int. Conf. on Multimedia Comp. and Systems, pp.514-521(1996-6)

[7] D. Kunder and D. Hatzinakos, A robust digital image watermarking method using wavelet-based fusion, Proc. of IEEE Int. Conf. on Acoustics, Speech and Sig. Proc., vol. 5, pp. 544-547 Seattle, Washington (1997-5).

[8] Meerwald, P., Uhl, A., 2001. A survey of wavelet-domain watermarking algorithms. In Proc. of SPIE, Electronics Imaging, Security and Watermarking of Multimedia Contents III, CA, USA 4314 (January), pp. 505-516.

[9] D. Kunder and D. Hatzinakos. Digital watermarking using multi-resolution wavelet decomposition . In Proceedings of IEEE ICAPSSP '98, volume 5, pages 2969 - 2972, Seattle, WA, USA, May 1998. –

[10] J. Dugelay and S. Roche, "A Survey of Current Watermarking Techniques" in Information Techniques for Steganography and Digital Watermarking, S.C. Katzenbeisser et al, Eds. Northwood, MA: Artec House, pp. 121-145, Dec. 1999.

[11] I. J. Cox, et al, "Digital watermarking and steganography" (Second Edition), Morgan Kaufmann, 2008.

[12] K. R. Rao and P. Yip, "Discrete Cosine Transform: Properties, Algorithms, Advantages,

ISSN: 2277-9655
Impact Factor: 1.852

Applications", Academic Press, Massachusetts, 1990.

[13] A. Khan and A.M. Mirza, "Genetic perceptual shaping: utilizing cover image and conceivable attack information during watermark embedding". Inf. Fusion, Vol. 8, pp. 354-365, Oct. 2007.

[14] G. K. Wallace, "The JPEG still picture compression standard", IEEE Trans. on Consumer Electronics, Vol. 38, pp.18-34, Feb. 1992.

[15] R. Popa, "An analysis of steganographic techniques", The Politehnica University of Timisoara, Faculty of Automatics and Computers, Department of Computer Science and Software Engineering, Website: http://ad.informatik.uni-freiburg.de/mitarbeiter/will/dlib_bookmarks/digital- watermarking/popa/popa.pdf, 1998.