Journal of Research in Science and Engineering (JRSE)
ISSN: 1656-1996 Volume-4, Issue-4, April 2022
DOI: 10.53469/jrse.2022.04(04).20

Digital Image Watermarking Technology Based on Discrete Wavelet Transform and Discrete Cosine Transform

Bhupendra Raesam

IIMT Greater Noida, CSE Department

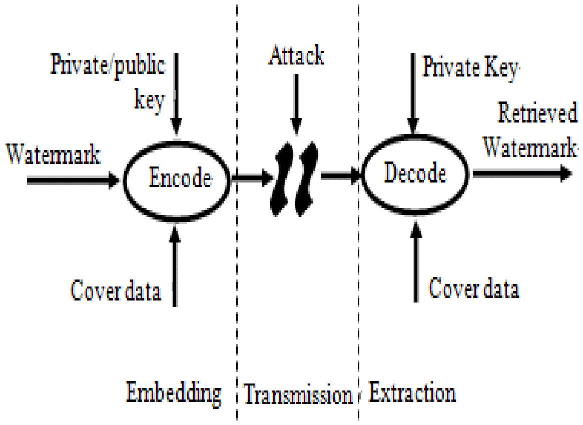
bhupendrabr@yahoo.co.in

Abstract: ***Digital watermarking has been proposed as a viable solution to the need of copyright protection and authentication of multimedia data in a networked environment, since it makes possible to identify the author, owner, distributor or authorized consumer of a document. In this paper a new watermarking technique to add a code to digital images is presented: the method operates in the frequency domain embedding a pseudo-random sequence of real numbers in a selected set of DCT coefficient and a new method for digital image watermarking which does not require the original image for watermark detection. The watermark is added in selected coefficients with significant image energy in the transform domain in order to ensure non-erasability of the watermark. Advantages of the proposed method include: improved resistance to attacks on the watermark, implicit visual masking utilizing the time-frequency localization property of wavelet transform and a robust definition for the threshold which validates the watermark. . Experimental results demonstrate that this proposed technique is robust to most of the signal processing techniques and geometric distortions.***

Keywords: Digital watermark, discrete wavelet transform, discrete cosine transform, watermarking technique, copyright protection

1. Introduction

Digital watermarking technology is an emerging field in computer science, cryptography, signal processing and communications. Digital watermarking is intended by its developers as the solution to the need to provide value added protection on top of data encryption and scrambling for content protection. In general a digital watermark is a technique which allows an individual to add hidden copyright information or other verification message to digital media. Watermarking is the process that embeds data called a watermark or digital signature or tag or label into a multimedia object such that watermark can be detected or extracted later to make an assertion about the object. Digital watermark is a sequence of information containing the owners copyright for the multimedia data. It is inserted visibly or invisibly into another image so that it can be extracted later as an evidence of authentic owner. Usage of digital image watermarking technique has grown significantly to protect the copyright ownership of digital multimedia data as it is very much prone to unlawful and unauthorized replication, reproduction and manipulation. The watermark may be a logo, label or a random sequence. A typical good watermarking scheme should aim at keeping the embedded watermark very robust under malicious attack in real and spectral domain. Incorporation of the watermark in the image could be performed in various ways.



(General processes involved in a watermarking system)

2. Previous Work

There have been many proposed novel techniques to hide watermark in digital images. These techniques can be classified into different categories according to several criteria. The first criterion is the type of domain in which the data embedding takes place. There are two major domain types, spatial and transform domains. The transform domain image is represented in terms of its frequencies; however, in spatial domain it is represented by pixels. The second criterion is according to the ability of watermark to resist attack; fragile watermarks are ready to be destroyed by random image processing methods, the change in watermark is easy to be detected, thus can provide information for image completeness, robust watermarks are robust under most image processing methods can be extracted from heavily attacked watermarked image.

A. Spatial Domain

Additive Watermarking

The most straightforward method for embedding the watermark in spatial domain is to add pseudo random noise pattern to the intensity of image pixels. The noise signal is usually integers like (-1, 0, 1) or sometimes floating point numbers.

Least Significant Bit Modification

A digital image version of this analogue image contains sampled values of the function at discrete locations or pixels. These values are said to be the representation of the image in the spatial domain or often referred to as the pixel domain. Spatial embedding inserts message into image pixels.

B. Transform Domain

Transform domain embeds a message by modifying the transform coefficients of the cover message as opposed to the pixel values. Ideally, transform domain has the effect in the spatial domain of apportioning the hidden information through different order bits in a manner that is robust. There are a number of transforms that can be applied to digital images, but there are notably three most commonly used in image watermarking. They are Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT).

Discrete Fourier Transform

Fourier Transform (FT) is an operation that transforms a continuous function into its frequency components. The equivalent transform for discrete valued function requires the Discrete Fourier Transform (DFT). In digital image processing, the even functions that are not periodic can be expressed as the integral of sine and/or cosine multiplied by a weighing function. This weighing function makes up the coefficients of the Fourier Transform of the signal. Fourier Transform allows analysis and processing of the signal in its frequency domain by means of analyzing and modifying these coefficients.

Discrete Cosine Transform

Discrete Cosine Transform is related to DFT in a sense that it transforms a time domain signal into its frequency components. The DCT however only uses the real parts of the DFT coefficients. In terms of property, the DCT has a strong energy compaction property and most of the signal information tends to be concentrated in a few low-frequency components of the DCT. The JPEG compression technique utilizes this property to separate and remove insignificant high frequency components in images.

Discrete Wavelet Transform

Wavelet Transform is a modern technique frequently used in digital image processing, compression, watermarking etc. The transforms are based on small waves, called wavelet, of varying frequency and limited duration. A wavelet series is a representation of a square-integrable function by a certain ortho-normal series generated by a wavelet. Furthermore, the properties of wavelet could decompose original signal into wavelet transform coefficients which contains the position information. The original signal can be completely reconstructed by performing Inverse Wavelet Transformation on these coefficients. Watermarking in the wavelet transform domain is generally a problem of embedding watermark in the sub bands of the cover image.

Advantages and Disadvantages

Watermarking also called tamper-proofing or content verification hides a secret and personal message to protect a products copyright or to demonstrate its data integrity, secure and fast digital data encryption and decryption, n content verification (authentication) of the received data by the recipient, and n robust and trustworthy marks indicating copyright and legal ownership. The loss of the private key can enable a pirate to remove the watermarks from all the images that belong to that particular owner. This would make the system dangerously unstable. Detection of false positives. A pirate can apply a sequence of various uncommon image-processing operations to confuse the monitoring software or to desynchronize the detector. (For example, the pirate might use the mosaic attack, which is essentially a cropping attack.13) Unfortunately, once the data are out in the distribution network, there is always the risk of watermark removal by new techniques.

Applications

In this section we discuss some of the scenarios where watermarking is being already used as well as other potential applications. The list given here is by no means complete and intends to give a perspective of the broad range of business possibilities that digital watermarking opens.

Authentication

This is a variant of the previous application, in an area where cryptographic techniques have already made their way. However, there are two significant benefits that arise from using watermarking: first, as in the previous case, the signature becomes embedded in the message, second, it is possible to create soft authentication algorithms that offer a multi-valued perceptual closeness measure that accounts for different unintentional transformations that the data may have suffered (an example is image compression with different levels), instead of the classical yes/no answer given by cryptography-based authentication.

Copy and Playback Control

The message carried by the watermark may also contain information regarding copy and display permissions. Then, a secure module can be added in copy or playback equipment to automatically extract this permission information and block further processing if required.

Signaling

The imperceptibility constraint is helpful when transmitting signaling information in the hidden channel. The advantage of using this channel is that no bandwidth increase is required. An interesting application in broadcasting consists in watermarking commercials with signaling information that permits an automatic counting device to assess the number of times that the commercial has been broadcast during a certain period.

Labeling

The hidden message could also contain labels that allow for example to annotate images or audio. Of course, the annotation may also been included in a separate file, but with watermarking it results more difficult to destroy or lose this label, since it becomes closely tied to the object.

Fingerprinting

This is similar to the previous application and allows acquisition devices (such as video cameras, audio recorders, etc) to insert information about the specific device (e. g., an ID number) and date of creation.

Common Distortions and Attacks on Watermark Object

In practice, a watermarked object may be altered either on purpose or accidentally, so the watermarking system should still be able to detect and extract the watermark. Obviously, the distortions are limited to those that do not produce excessive degradations, since otherwise the transformed object would be unusable, depending on the application:

Additive Noise

This may stem in certain applications from the use of D/A and A/D converters or from transmission errors. However, an attacker may introduce perceptually shaped noise (thus, imperceptible) with the maximum unnoticeable power. This will typically force to increase the threshold at which the correlation detector works.

Filtering

Low-pass filtering, for instance, does not introduce considerable degradation in watermarked images or audio, but can dramatically affect the performance, since spread-spectrum-like watermarks have a non negligible high-frequency spectral contents.

Cropping

This is a very common attack since in many cases the attacker is interested in a small portion of the watermarked object, such as parts of a certain picture or frames of a video sequence. With this in mind, in order to survive, the watermark needs to be spread over the dimensions where this attack takes place.

Compression

This is generally an unintentional attack which appears very often in multimedia applications. Practically all the audio, video and images that are currently being distributed via Internet have been compressed.

Rotation and Scaling

This has been the true battle horse of digital watermarking, especially because of its success with still images. Correlation based detection and extraction fail when rotation or scaling is performed on the watermarked image because the embedded watermark and the locally generated version do not share the same spatial pattern anymore.

Statistical Averaging

An attacker may try to estimate the watermark and then unwatermark the object by subtracting the estimate. This is dangerous if the watermark does not depend substantially on the data. Note that with different watermarked objects it would be possible to improve the estimate by simple averaging. This is a good reason for using perceptual masks to create the watermark.

Discrete Wavelet Transform

Wavelet transform is time domains localized analysis method with the windows size fixed and form convertible. There is quite good time differentiated rate in high frequency part of signals DWT transformed. Also there is quite good frequency differentiated rate in its low frequency part. It can distill the information from signal effectively. The basic idea of discrete wavelet transform (DWT) in image process is to multi-differentiated decompose the image into sub-image of different spatial domain and independent frequency district. Then transform the coefficient of sub-image. After the original image has been DWT transformed, it is decomposed into 4 frequency districts which is one low-frequency district (LL) and three high-frequency districts (LH, HL, HH).

Advantages of DWT

1) No need to divide the input coding into non-overlapping 2-D blocks, it has higher compression ratios avoid blocking artifacts
2) Allows good localization both in time and spatial frequency domain
3) Transformation of the whole image introduces inherent scaling
4) Better identification of which data is relevant to human perception higher compression ratio
5) Higher flexibility: Wavelet function can be freely chosen.

Disadvantages of DWT

1) The cost of computing DWT as compared to DCT may be higher.
2) The use of larger DWT basis functions or wavelet filters produces blurring and ringing noise near edge regions in images or video frames
3) Longer compression time

Discrete Cosine Transform

Digital watermarking has been proposed as a viable solution to the need of copyright protection and authentication of multimedia data in a networked environment, since it makes possible to identify the author, owner, distributor or authorized consumer of a document. In this paper a new watermarking technique to add a code to digital images is presented: the method operates in the frequency domain embedding a pseudo-random sequence of real numbers in a selected set of DCT coefficients. Watermark casting is performed by exploiting the masking characteristics of the Human Visual System, to ensure watermark invisibilily. The embedded sequence is extracted without resorting to the original image, so that the proposed technique represents a major improvement to methods relying on the comparison between the watermarked and original images.

Advantages of DCT

1) Semantically meaningful watermark pattern
2) Good perceptual invisibility
3) Acceptable robustness
4) Various user-selected options
5) Reasonable complexity/execution time
6) Fast and Suitable for robustness against JPEG compression.
7) Its a real transform with better computational efficiency than DFT which by definition is a complex transform.

Disadvantages of DCT

1) Block effect
2) Effect of picture cropping
3) One of the main problems and the criticism of the DCT is the blocking effect. In DCT images are broken into blocks 8x8 or 16x16 or bigger. The problem with these blocks is that when the image is reduced to higher compression ratios, these blocks become visible. This has been termed as the blocking effect.

3. Proposed Discrete Wavelet Transform Based Watermarking Scheme

Since DWT has the excellent spatio-frequency localization property, it has been extensively utilized to identify the image areas where a disturbance can be more easily hidden. A new method for digital image watermarking which does not require the original image for watermark detection.

Watermark Embedding:

The algorithm to embed a watermark in the original image is summarized as follows:

1) Decompose the original image into four levels (thirteen subbands).
2) Any binary image with approximately equal number of 0s and 1s is utilized as a watermark image.
3) Map 0– 1 and 1– +1 to generate a pseudo-random binary sequence containing either 1 or +1.
4) The subband pairs (LH3, LH2), (HL3, HL2), and (HH3, HH2) at level 3 and level 2 are selected to calculate the changes made in these middle frequency subbands.
5) The pseudo-random binary sequence generated from the binary image is rearranged in three different ways to be embedded in the LH3, HL3, HH3, LH2, HL2, and HH2 using the pixel-wise computation.
6) Apply the IDWT (Inverse Discrete Wavelet Transform) using the newly updated sub-band values at the level 3 and level 2 to obtain the watermarked image.

Watermark Extraction:

Watermark detection is accomplished without referring to the original image. The correlations Z between the DWT coefficients and the watermarking sequence to be tested at level 2 and computed by using the watermark embedding algorithm. This correlation is compared to the thresholds T saved in the watermark embedding procedure. The watermark is present if and only if one of the following conditions is true:

$Z >= T$

Then watermarking revealed it means watermarked image

$Z < T$

Then watermarking not revealed it means non watermarked image.

4. Proposed Discrete Cosine Transform Based Watermarking Technique

In this watermarking technique to add a code to digital images is presented: the method operates in the frequency domain embedding a pseudo-random sequence of real numbers in a selected set of DCT coefficients. Watermark casting is performed by exploiting the masking characteristics of the Human Visual System, to ensure watermark invisibilily. The embedded sequence is extracted without resorting to the original image.

Watermark Embedding:

The algorithm consists of the following steps:

1) The first step is the conversion of the scaled input image from the RGB color model to the grayscale color model.

2) An original gray-level image of size (NxN) is divided into n = (NxN) / (8x8) non-overlapped blocks (8x8) which are transformed to frequency domain by the DCT. The watermark bit stream is embedded into eight coefficients in lower band of each block.
3) For the purpose of scattering watermark into the host image and prompting security, we use pseudo random system to generate a random position in watermarking algorithm. Obtain a random number, generated by pseudo random system, which points to one of n blocks of host image.
4) Embed extracted the 8-bit watermarking data into the 8 lower-band coefficients in the block pointed by previous step.
5) Apply inverse DCT (IDCT) into the 8 lower-band coefficients in the block to obtain the watermarked image.

Watermark Extraction:

Watermark detection is accomplished without referring to the original image. The correlations Z between the DCT coefficients and the watermarking sequence to be tested at each block and computed by using the watermark embedding algorithm. This computated correlations are compared to the thresholds T saved in the watermark embedding procedure. The watermark is present if and only if one of the following conditions is true:

Z >= T

Then watermarking revealed it means watermarked image

Z < T

Then watermarking not revealed it means non watermarked image.

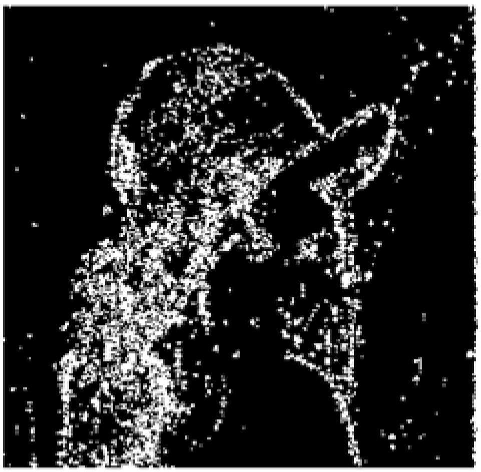
5. Results and Discussion for DWT

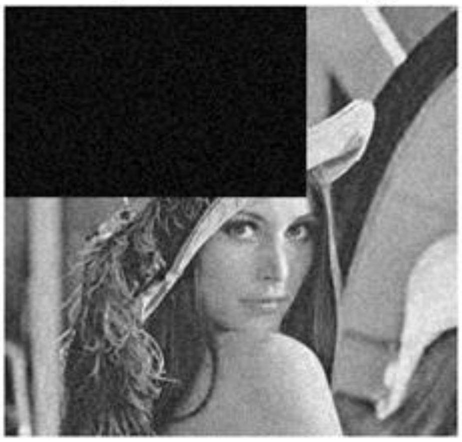
A number of experiments are performed on the watermarked image to test the resilience of the proposed scheme towards common image processing attacks.512x512 gray scale Lena and baboon images are used as cover image and watermark image respectively. These images are shown following.

Input image

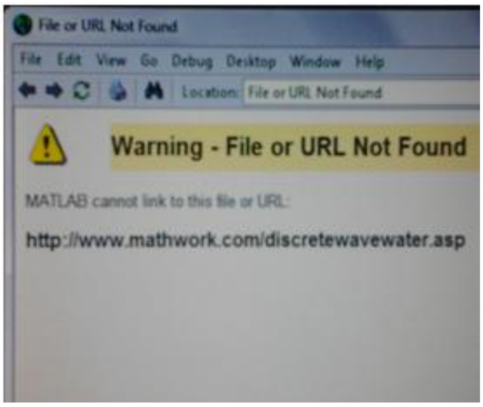
Watermarked image

Differences





Corrupted, watermarked image

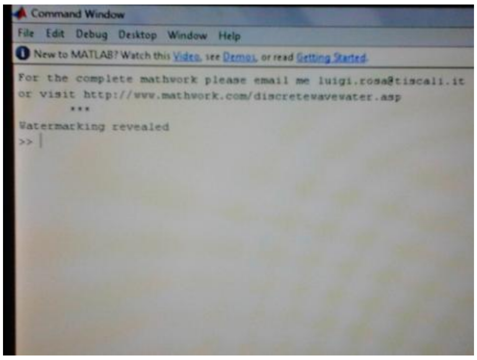

File or URL Not Found
File Edit View Go Debug Desktop Window Help
Location: File or URL Not Found

Warning - File or URL Not Found

MATLAB cannot link to this file or URL:

http://www.mathwork.com/discretewavewater.asp

Web Browser


Command Window
File Edit Debug Desktop Window Help
New to MATLAB? Watch this Video, see Demos, or read Getting Started.

```
For the complete mathwork please email me luigi.rosa@tiscali.it
or visit http://www.mathwork.com/discretewavewater.asp
     ***
Watermarking revealed
>> |
```

Command Window

Table for MSE, PSNR and NC Values of Different Watermarking Attack on DWT Images

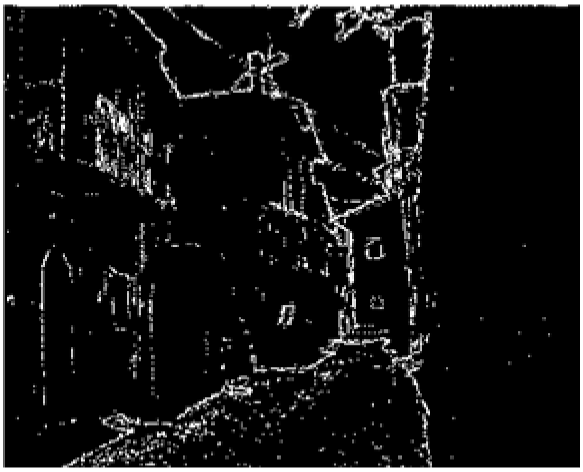
Kind of attack	*MSE*	*PSNR*	*NC VALUE*
Watermarked Image	21.1607	34.8755	0.7211
Extracted Image	5.0729e+003	11.0782	-----
Decorrupted Image	219.1801	24.7228	0.7198
Gaussian Noise	265.4543	23.8909	0.7283
HE	1.6040e+003	16.0786	0.7473
Blur-SA	449.1617	21.6068	0.7186
Detect Edge-Sobel	4.4784e+004	1.6196	0.1746
Sharpen-Laplacian	413.0848	21.6068	0.7320
Resize	1.5100e+004	1.5100e+004	-----

6. Results and Discussion for DCT

A number of experiments are performed on the watermarked image to test the resilience of the proposed scheme towards common image processing attacks.512x512 input gray scale image are used as cover image and watermark image respectively. These images are shown in figure following.

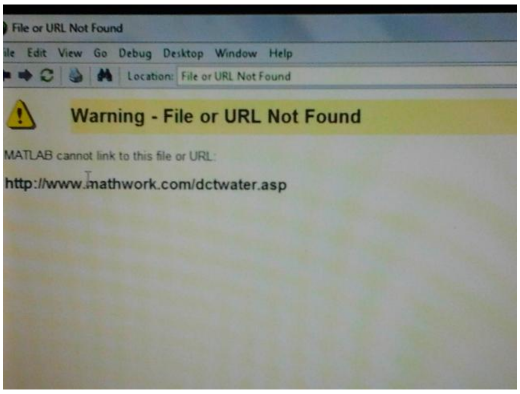
Input Image

Watermarked Image



Extracted Image

Corrupted Image



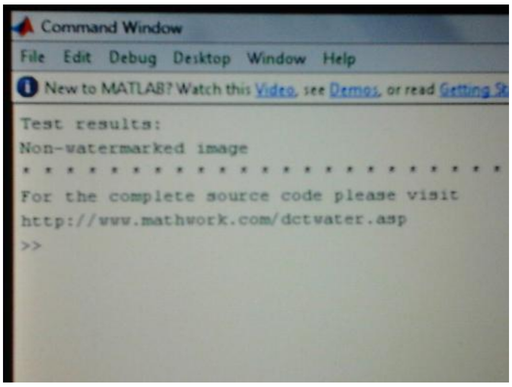
File or URL Not Found
ile Edit View Go Debug Desktop Window Help
Location: File or URL Not Found

Warning - File or URL Not Found

MATLAB cannot link to this file or URL:

http://www.mathwork.com/dctwater.asp

Web Browser



Command Window
File Edit Debug Desktop Window Help
New to MATLAB? Watch this Video, see Demos, or read Getting St

```
Test results:
Non-watermarked image
* * * * * * * * * * * * * * * * * * * * * * * * *
For the complete source code please visit
http://www.mathwork.com/dctwater.asp
>>
```

Command Window

Table for MSE, PSNR and NC Values of Different Watermarking Attack on DCT Images

Kind of attack	MSE	PSNR	NC VALUE
Watermarked Image	5.1520	41.0110	0.6609
Extracted Image	5.9240e+003	10.4047	-----
Decorrupted Image	2.0078e+003	15.1035	0.6608
Gaussian Noise	325.7615	23.0018	0.6679
HE	470.8554	21.4019	0.6876
Blur-SA	214.5226	24.8161	0.6601
Detect Edge-Sobel	3.1059e+004	7.6948	0.3721
Sharpen-Laplacian	157.5431	26.1568	0.6622
Resize	1.1056e+004	7.6948	-----

7. Conclusion and Future Scope

In this dissertation, a digital image watermarking technique based on discrete wavelet transform and discrete cosine transform has been presented, where the method operates in the frequency domain embedding a pseudo-random sequence of real numbers in a selected set of DCT coefficients. And the watermark is added in select coefficients with significant image energy in the discrete wavelet transform domain in order to ensure non-erasability of the watermark. Experimental results demonstrate that the watermark is robust to most of the signal processing techniques and geometric distortions. Result suggest that the proposed scheme can be used to extract a good quality watermark for various image processing attacks like JPEG compression, average filtering, median filtering and cropping.

There is a scope of future work in this dissertation, as is observed from the qualitative results that the proposed scheme shows comparable results with that of the scheme proposed by earlier. These results can be improved to increase the utility of the proposed scheme for varying levels of compression.

References

[1] C. I. Podilchuk and E. J. Delp, Digital watermarking: algorithm and application, IEEE Signal Processing Magazine, vol.18, no.4, pp.346, 2001.

[2] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, Secure spread spectrum watermarking for multimedia, IEEE Transactions on Image processing, vol.6, no.12, pp, 16731687, 1997.

[3] H. J. M. Wang, P. C. Su, and C. C. J Kuo, Wavelet-base digital image watermarking, Opt. Express, Vol.3, No.12, pp.491496, Dec.1998.

[4] F. Y. Shih and S. Y. T. Wu, Combinational image watermarking in the spatial and frequency domains, Pattern Recognition, vol.36, no.4, pp.969975, 2002.

[5] C.-S. Shieh, H.-C. Huang, F.-H. Wang, and J.-S. Pan, Genetic watermarking based on transform-domain techniques, Pattern Recognition, vol.37, no.3, pp.555565, 2004.

[6] P. Tao and A. M. Eskicioglu, A robust multiple watermarking scheme in the discrete wavelet transform domain, in Internet Multimedia Management Systems V, Proceedings of SPIE, pp.133144, Philadelphia, Pa, USA, October 2004.

[7] A. Bors and I. Pitas, Image watermarking using DCT domain constraints in Proc. IEEE. Int. Conf. Image Processing, Lausanne, Switzerland, Sept.1996, pp.231-234.

[8] Yusnita Yusof and Othman O. Khalifa, (2007), Digital Watermarking For Digital Images Using Wavelet Transform, IEEE.

[9] Hiroyuki Kii, Junji Onishi, Shinji Ozawa, (1999) The Digital Watermarking Method by Using Patchwork and DCT, IEEE.

[10] A. Piva, M. Barni, F. Berbolini and V. Cappellini, DCT based watermark recovery without resorting to the uncorrupted original image, Proc. IEEE Intern.

Conf. on Image Processing, ICIP97, Santa Barbara, California USA, Vol.1, October 1997.

[11] A. S. Lewis and G. Knowles, Image compression using the 2-D wavelet transform, IEEE Transactions of Image Processing, vol.1, no.2, pp.244250, 1992.27

[12] M. Barni, F. Bartolini, V. Cappellini, A. Lippi and A. Piva, A DWT based technique for spatio-frequence masking of digital signature, Proc. of the 11th SPIE Annual Symposium, Electronic Imaging 99, Security and Watermarking of Multimedia Contents, vol.3657, San Jose, CA, USA, January 1999.