Volume 1, No. 2, July-August 2010

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A DFT-DWT Domain Invisible Blind Watermarking Techniques for Copyright Protection of Digital Images

Munesh Chandra*
I.M.S, Ghaziabad
Ghaziabad, India.
munesh.trivedi@gmail.com

Shikha Pandey
R.K.G.I.T,Ghaziabad.
Ghaziabad, India
shikpan@gmail.com

***Abstract*:** In this paper, we have given overview of digital watermarking and proposed a frequency based invisible blind watermarking technique that use DFT Discrete Fourier transform) and DWT (Discrete Wavelet Transform) transform for copyright protection of digital images. Using these transforms is motivated by good time frequency features and well matching with human visual system directives of wavelet transform and averagely distribution of energy of watermarking message in spatial domain after the signal is implemented in DFT. In order for a watermark to be useful, it must be perceptually invisible and robust against any possible attack.
In this paper we measured imperceptibility and robustness of the method through parameters, PSNR (Peak Signal to Noise Ratio) and AR (Accuracy Rate).

Keywords – Digital Watermarking, DFT, DWT, Copyright Protection

I. INTRODUCTION

The great success of Internet and digital multimedia technology have made the fast communication of digital data, easy editing in any part of the digital content, capability to copy a digital content without any loss in quality of the content and many other advantages.
The great explosion in this technology has also brought some problems beside its advantages. The great facility in copying a digital content rapidly, perfectly and without limitations on the number of copies has resulted the problem of copyright protection. Digital watermarking is proposed as a solution to prove the ownership of digital data. A watermark, a secret imperceptible signal, is embedded into the original data in such a way that it remains present as long as the perceptible quality of the content is at an acceptable level. The owner of the original data proves his/her ownership by extracting the watermark from the watermarked content in case of multiple ownership claims.
In general, any watermarking scheme (algorithm) consists of three parts.

- The watermark.
- The encoder (insertion algorithm).
- The decoder and comparator (verification or extraction or detection algorithm).

Each owner has a unique watermark or an owner can also put different watermarks in different objects the marking algorithm incorporates the watermark into the object. The verification algorithm authenticates the object determining both the owner and the integrity of the object [1].

A. Embedding Process

Let us denote an image by I, a signature by $S = s_1, s_2, \ldots$ and the watermarked image by I′. E is an encoder function, it takes an image I and a signature S, and it generates new image which is called watermarked image I', mathematically,

$$E(I, S) = I' \qquad (1)$$

It should be noted that the signature S may be dependent on image I. In such cases, the encoding process described by (1) still holds. The figure 1 illustrates the encoding process [1].

B. Extraction Process

A decoder function D takes an image J (J can be a watermarked or un-watermarked. image, and possibly corrupted) whose ownership is to be determined and recovers a signature S′ from the image [1].

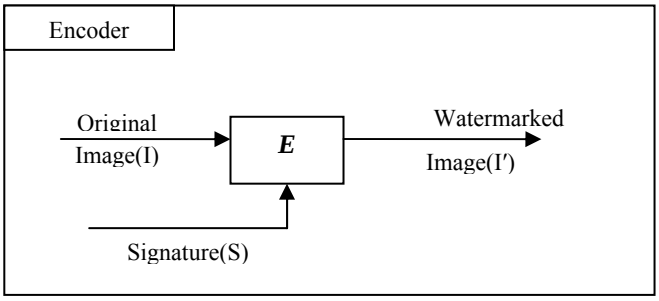

Figure 1: Encoder

In this process an additional image I can also be included which is often the original and un-watermarked version of J. This is due to the fact that some encoding schemes may make use of the original images in the watermarking process to provide extra robustness against intentional and unintentional corruption of pixels. Mathematically,

$$D(J, I) = S' \qquad (2)$$

In proposed algorithm, original image is not used while extracting watermark from watermarked image and we provide robustness by using some keys.
The extracted signature S' will then be compared with the owner signature sequence by a comparator function C_δ and a binary output decision generated. It is 1 if there is match and 0 otherwise, which can be represented as follows.

$$C_\delta(S, S') = \begin{cases} 1, & c \le \delta \\ 0, & \text{otherwise} \end{cases} \quad (3)$$

Where C is the correlator, $x = C_\delta(S, S')$. c is the correlation of two signatures and δ is certain threshold. Without loss of generality, watermarking scheme can be treated as a three-tupple (E, D, C_δ). Following figure 2 & figure 3 demonstrate the decoder and the comparator respectively.

A watermark must be detectable or extractable to be useful. Depending on the way the watermark is inserted and depending on the nature of the watermarking algorithm, the method used can involve very distinct approaches. In some watermarking schemes, a watermark can be extracted in its exact form, a procedure we call watermark extraction. In other cases, we can detect only whether a specific given watermarking signal is present in an image, a procedure we call watermark detection. It should be noted that watermark extraction can prove ownership whereas watermark detection can only verify ownership.

The proposed technique extract watermark to prove ownership.

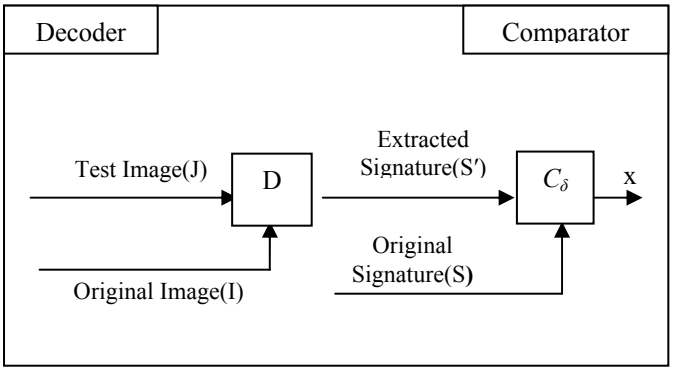

Figure 2: Decoder

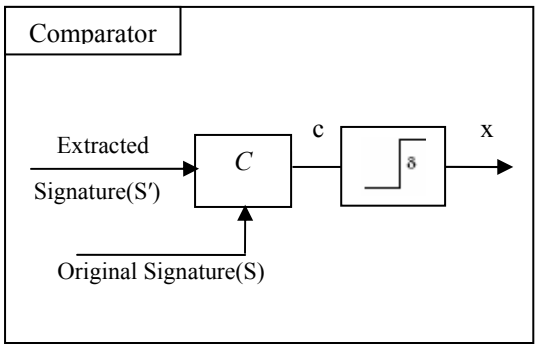

Figure 3: Comparator

The quality of extracted watermark can also be measured by: *PSNR* (Peak Signal-to-Noise Ratio) and *AR* (Accuracy rate)

PSNR is provided only to give us a rough approximation of the quality of the watermark.

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right)dB \quad (4)$$

Where *MSE* is mean square error of an image with H × W pixels is defined as:

$$MSE = \frac{1}{H \times W}\sum_{i=1}^{H}\sum_{j=1}^{W}(a_{ij} - \bar{a}_{ij})^2 \quad (5)$$

Where a_{ij} is the original pixel value and $\bar{a}_{ij}$ is the processed pixel value.

Besides, we utilized the accuracy rate *AR* to evaluate the robustness of a copyright protection scheme for a specific attack. The formula for *AR* is shown below:

$$AR = \frac{CP}{NP}, \quad (6)$$

Where *NP* is the number of pixels of the watermark image and *CP* is the number of correct pixels in the extracted watermark image.

C. Classification of Watermarking Techniques:

Watermarking techniques can be divided into four categories according to the type of document to be watermarked as follows [1]: Text Watermarking, Image Watermarking, Audio Watermarking and Video Watermarking.

In the case of images from implementation point of view, watermarks can be applied in spatial domain and in frequency domain. In Spatial domain, pixels of one and two randomly selected subsets of an image are modified based on perceptual analysis of the original image. In Frequency domain, values of certain frequencies are altered from their original.

According to human perception, digital watermarks can be divided into three categories as follows [2]: Visible, Invisible-robust and Invisible-Fragile. Visible watermark is where the secondary translucent overlaid into the primary content and appears visible on a careful inspection. Invisible-Robust watermark is embedded is such a way changes made to the pixel value are perceptually unnoticed. Invisible –Fragile watermark is embedded in such a way that any manipulation of the content would alter or destroy the watermark. Sometimes another watermarking called dual watermarking is used. Dual watermark is a combination of a visible and an invisible watermark [1]. In this type of watermark an invisible watermark is used as a back up for the visible watermark as clear from the following diagram.

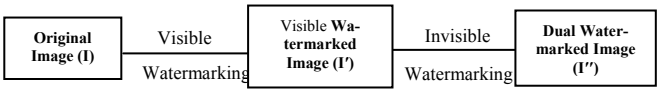

Figure 4: Schematic representation of dual watermarking

From application point of view, digital watermarking could also be [2]: source based and destination based. In source based a unique watermark identifying the owner is introduced to all the copies of particular content being distributed. Destination based is where each distributed copy gets a unique watermark identifying the particular buyer. Different types of watermarks are shown in the figure. 5:

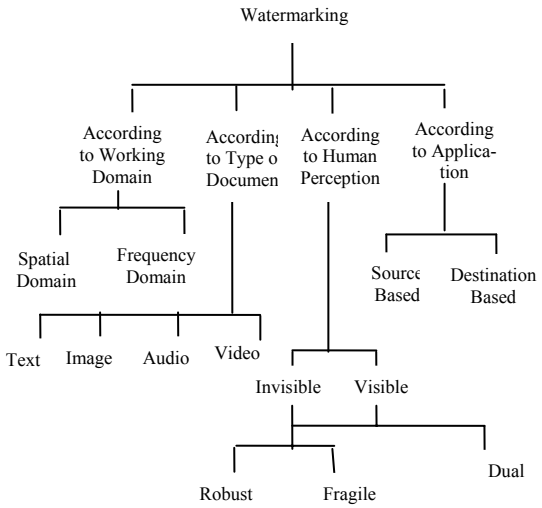

Figure 5. Types of watermarking techniques

Current digital image watermarking techniques can be grouped into two major classes: spatial-domain and frequency-domain watermarking techniques [3]. Compared to spatial domain techniques [4], frequency-domain watermarking techniques proved to be more effective with respect to achieving the imperceptibility and robustness requirements of digital watermarking algorithms [5].

Commonly used frequency-domain transforms include the Discrete Wavelet Transform (DWT), the Discrete Cosine Transform (DCT) and Discrete Fourier Transform (DFT). The host signal is transformed into a different domain and the watermark is embedded in selective coefficients. Here we have described DFT and DWT domain techniques.

1) Discrete Fourier transform:

The Discrete Fourier Transformation (DFT) controls the frequency of the host signal. Energy of watermarking message can be distributed averagly in space domain after the signal is implemented DFT. It enables the schemes further to embed the watermark with the magnitude of its coefficients.

Given a two-dimensional signal *f(x, y)*, the DFT is defined

$$F(u,v)=\frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y)\, e^{-j2\pi(ux/M+vy/N)} \quad (7)$$

For $u = 0, 1, 2..., M-1$, $v = 0, 1, 2,., N-1$ and $j=\sqrt{-1}$

The inverse DFT (IDFT) is given by:

$$f(x,y) = \sum_{u=0}^{M-1}\sum_{v=0}^{N-1} F(u,v)\, e^{j2\pi(ux/M+vy/N)} \quad (8)$$

where, (M, N) are the dimensions of the image.

The DFT is useful for watermarking purposes because it helps in selecting the adequate parts of the image for embedding, in order to achieve the highest invisibility and robustness.

2) The wavelets transform:

Wavelet transform decomposes an image into a set of band limited components which can be reassembled to reconstruct the original image without error. The DWT (Discrete Wavelet Transform) divide the input image into four non-overlapping multi-resolution sub-bands LL1, LH1, HL1 and HH1. The process can then be repeated to computes multiple "scale" wavelet decomposition, as in the 2 scale wavelet transform shown in Fig. 6.

One of the many advantages over the wavelet transform is that it is believed to more accurately model aspects of the HVS as compared to the FFT or DCT. This allows us to use higher energy watermarks in regions that the HVS is known to be less sensitive, such as the middle frequency bands (LH, HL) and high resolution band (HH). But watermark embedded in high resolution band can be easily be distorted by geometric transformation, compression and various signal processing operations.

Embedding watermarks in middle frequency regions allow us to increase the robustness of our watermark, at little to no additional impact on image quality [6].

D. Watermarking Applications:

Although the main motivation behind the digital watermarking is the copyright protection, its applications are not that restricted. There is a wide application area of digital watermarking, including broadcast monitoring, fingerprinting, authentication and covet communication [7, 8, 9, 10].

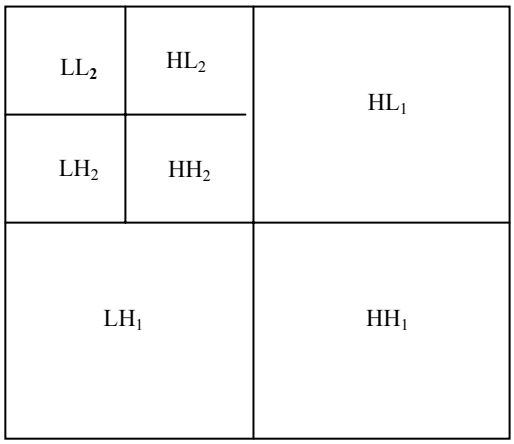

Figure 6: Scale 2 Dimensional DWT

By embedding watermarks into commercial advertisements, the advertisements can be monitored whether the advertisements are broadcasted at the correct instants by means of an automated system [7, 8]. The system receives the broadcast and searches these watermarks identifying where and when the advertisement is broadcasted. The same process can also be used for video and sound clips. Musicians and actors may request to ensure that they receive accurate royalties for broadcasts of their performances.

Fingerprinting is a novel approach to trace the source of illegal copies [7, 8]. The owner of the digital data may embed different watermarks in the copies of digital content customized for each recipient. In this manner, the owner can identify the customer by extracting the watermark in the case the data is supplied to third parties. The digital watermarking can also be used for authentication [7, 8]. The authentication is the detection of whether the content of the digital content has changed. As a solution, a fragile watermark embedded to the digital content indicates whether the data has been altered. If any tampering has occurred in the content, the same change will also occur on the watermark. It can also provide information about the part of the content that has been altered.

Covert communication is another possible application of digital watermarking [7,8]. The watermark, secret message, can be embedded imperceptibly to the digital image or video to communicate information from the sender to the intended receiver while maintaining low probability of intercept by other unintended receivers.

There are also non-secure applications of digital watermarking. It can be used for indexing of videos, movies and news items where markers and comments can be inserted by search engines [8]. Another non-secure application of watermarking is detection and concealment of image/video transmission errors [11]. For block based coded images, a summarizing data of every block is extracted and hidden to another block by data hiding. At the decoder side, this data is used to detect and conceal the block errors.

E. Watermarking Requirements

The efficiency of a digital watermarking process is evaluated according to the properties of perceptual transparency, robustness, computational cost, bit rate of data embedding process, false positive rate, recovery of data with or without access to the original signal, the speed of embedding and retrieval process, the ability of the embedding and retrieval module to integrate into standard encoding and decoding process etc. 7, 8, 9, 12, 13].

Depending on the application, the properties, which are used mainly in the evaluation process, vary.

The main requirements for copyright protection are imperceptibility and robustness to intended or non-intended any signal operations and capacity.

The owner of the original data wants to prove his/her ownership in case the original data is copied, edited and used without permission of the owner. In the watermarking research world, this problem has been analyzed in a more detailed manner [13, 14, 15, 16, 17, 18].

The imperceptibility refers to the perceptual similarity between the original and watermarked data. The owner of the original data mostly does not tolerate any kind of degradations in his/her original data. Therefore, the original and watermarked data should be perceptually the same.

Robustness to a signal processing operation refers to the ability to detect the watermark, after the watermarked data has passed through that signal processing operation.

The robustness of a watermarking scheme can vary from one operation to another. Although it is possible for a watermarking scheme to be robust to any signal compression operations, it may not be robust to geometric distortions such as cropping, rotation, translation etc. The signal processing operations, for which the watermarking scheme should be robust, changes from application to application as well. While, for the broadcast monitoring application, only the robustness to the transmission of the data in a channel is sufficient, this is not the case for copyright protection application of digital watermarking. For such a case, it is totally unknown through which signal processing operations the watermarked data will pass. Hence, the watermarking scheme should be robust to any possible signal processing operations, as long as the quality of the watermarked data preserved.

The capacity requirement of the watermarking scheme refers to be able to verify and distinguish between different watermarks with a low probability of error as the number of differently watermarked versions of an image increases [17]. While the robustness of the watermarking method increases, the capacity also increases where the imperceptibility decreases. There is a trade off between these requirements and this trade off should be taken into account while the watermarking method is being proposed.

II. PROPOSED TECHNIQUES

We have proposed a blind invisible watermarking technique for copyright protection of the colored images.

In blind techniques, during the extraction process original image is not required. Watermarking systems which involve marking imperceptible alteration on the cover data to convey the hidden information, is called invisible watermarking.

Here 512*512 grayscale image of 'peppers' is taken as host image and 32*32 binary image is taken as watermark image. Then implement second level wavelet transform on host image using wavelet function 'haar' and extracted middle level components (HL_2, LH_2) for embedding watermark.

Middle level components are selected for embedding watermark as much of the signal energy lies at low-frequencies sub-band which contains the most important visual parts of the image and high frequency components of the image are usually removed through compression and noise attacks.

We have divided the HL_2 and LH_2 bands in to 4x4 blocks and applied DFT in these blocks and used to two highly uncorrelated pseudo random sequences (treated as key: key1) to embed watermarking message according to template matrix. We reshaped watermark image of 32x32 into a row vector of size 1024, called watermark message.

A template matrix is such a matrix whose size is 4x4 and elements are 0 and 1. Watermarking message is embedded into image blocks only in the position where the template matrix's element is 1. Through amounts of experiments, we found when the template matrix is set to $[1,1,1,1;1,0,0,1;0,0,0,1;0,0,0,1]^T$, imperceptibility and robustness of the algorithm can get better balance. Here template matrix is used as a key2.

We have embedded watermark according to the (9) given below.

$$I_w(x, y) = I(x, y) + k^* W(x, y) \qquad (9)$$

In (9), k denotes a gain factor, and I_W the resulting watermarked image, I the cover image and W the watermark to be embedded. Increasing k increases the robustness of the watermark at the expense of the quality of the watermarked image.

The algorithm for the proposed method is given below:

The watermark embedding steps are as follows:

- Implement second level wavelet transform on host Image H using wavelet function 'Haar' and Extract middle frequency components (LH_2, HL_2).
- Divide the HL_2, LH_2 components in several blocks of size 4x4 and DFT is applied to these blocks.
- Perform search to find highly uncorrelated pseudo random (PN) sequences (seq_zero and seq_one) and use these as a key1.
- Defines the template matrix of an 4x4.
- Set gain factor K and embed the watermark to the cover image under the following rule:
- If wa(i,j) ==0 then
  If template(m,n)==1 then
  I(m,n)=I(m,n) + K*seq_zero(m,n)
  End
  Else
  if template(m,n)==1 then
  I(m,n)=I(m,n)+K*seq_one(m,n)

End
End
Where $1 \le i \le M$, $1 \le j \le N$, and $1 \le m,n \le 4$
Here I denotes to 4x4 DFT blocks.

- Apply IFFT to each image block and use the result as the middle frequency component of DWT to recover the component which has been embedded watermarking messages.
- Replace the component of the host image by the watermarked component.
- Display watermarked image.

The watermark extraction steps of this technique are as follows:

- Implement Wavelet transform on Host image using wavelet function 'Haar' and Extract middle frequency components (LH_2, HL_2).
- Divide the HL_2, LH_2 components in several blocks of size 4x4 and DFT is applied to these blocks.
- Use same highly uncorrelated PN sequences (key1) and the template matrix of 4x4 (key2) to select elements that are embedded watermarking message to make up sequence.
- Calculate the correlation separately between sequence and seq_zero and between sequence and seq_one. The result is stored in corr_zero and corr_one respectively.
- Detect the watermark according the following rule:
  If corr_zero(i) > corr_one(i) then
  watermark_detected(i)=0;
  Else
  watermark_detected(i)=1
  End
  - Reshape the recovered message.
  - Display recovered message.
  - Calculate the quality of recovered image by using PSNR function according to the (4).
  - Calculate the Accuracy rate of recovered image by using AR function as per the (6).

III. EXPERIMENTAL RESULTS

In this section, we show some experimental results to demonstrate the effectiveness and success of our digital watermarking techniques. The standard 512 × 512 grayscale image "pepper" is used as host image, as shown in Fig. 7. The 32 × 32-pixels binary image is used as the watermark image, as shown in Fig. 8.

We applied the peak-signal to noise rate (PSNR) given in (4) to measure the image quality of an attacked image and accuracy rate AR given in (5) to evaluate the robustness of a copyright protection scheme for a specific attack.

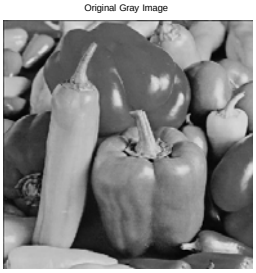

Figure 7: Original image of pepper

Figure8: Watermark image

A. Experimental Result and Analysis

The experimental results are represented in the following, respectively for watermarked image and extracted watermark image as shown in Fig. 9 (i), and Fig. 9 (ii), while taking the different values of gain factor *K*. And various observations for experiment are depicted in Table I.

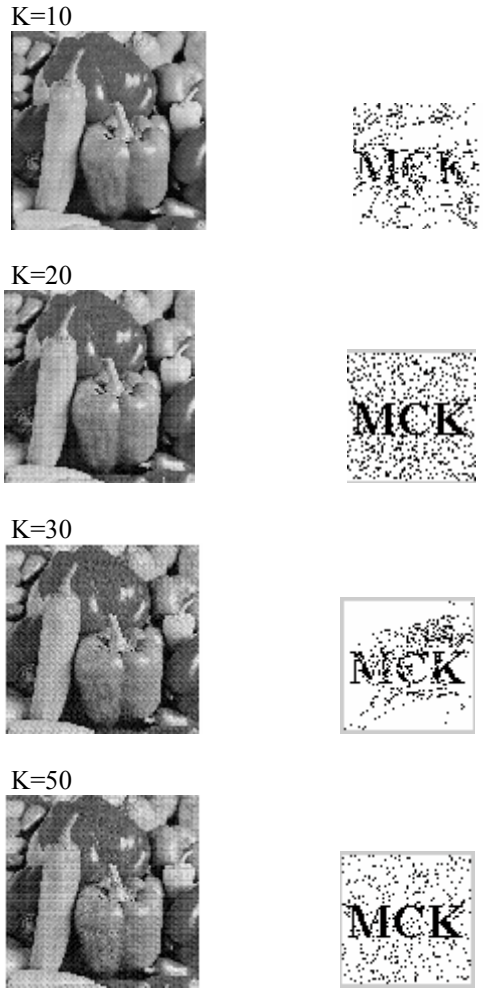

Figure 9: (i) Watermarked image, (ii) Extracted watermark image

Exhaustive testing against signal processing operation, Geometric distortion , collusion still has to be performed.

TABLE I

Gain Fator(K)	*Execution Time*	*AR*	*PSNR*
K=10	176.6796	89.4532	60.3456
K=20	175.6307	93.0640	55.2389
K=30	173.3867	91.3765	54.7829
K=40	175.3912	93.5621	54.6047

VI. CONCLUSION

The need for digital watermarking on electronic distribution of copyright material is becoming more prevalent. In this paper an overview of the digital watermarking techniques

are given and a blind invisible watermarking technique for grayscale images based on DWT and DFT is presented. The algorithm use 512*512 gray image as a host image and 32*32 binary image as watermarked image.

Firstly, two level wavelet decomposition is implemented on the host image. Then, the middle frequency components are extracted and divided in to several blocks of size 4*4 and DFT is implemented on them. Finally, two pseudo random sequences are created and embedded to blocks which have implemented DFT according to whether the corresponding position is 0 or 1 in the watermark matrix which has been implemented.

The original image is not required while extracting the watermark Instead, correlations among each block and two sequences are respectively calculated. Watermark is recovered on foundation of the relative magnitude of correlation between the corresponding block and one sequence or the other. The idea of applying two transform is based on the fact that combined transforms could compensate for the drawbacks of each other, resulting in effective watermarking.

V. REFERENCES

[1] S.P. Mohanty, et al., "A Dual Watermarking Technique for Images", Proc.7th ACM International Multimedia Conference, ACM-MM'99, Part 2, pp 49-51, Orlando, USA, Oct. 1999

[2] Yusnita Yusof and Othman O. Khalifa , "Digital Watermarking For Digital Images Using Wavelet Transform", Proc 2007 IEEE conference, pp 665-669

[3] Potdar, V., S. Han and E. Chang, 2005. "A Survey of Digital Image Watermarking Techniques", in Proc. of the IEEE International Conference on Industrial Informatics, pp: 709-716, Perth, Australia.

[4] Chan, C. and L. Cheng, 2004. "Hiding Data in Images by Simple LSB Substitution", Pattern Recognition, 37(3):469-474.

[5] Wang, R., C. Lin and J. Lin, " Copyright protection of digital images by means of frequency domain watermarking," Proc. of the SPIE Conference On Mathematics of Data/Image Coding, Compression, and Encryption, USA.

[6] G. Langelaar, I. Setyawan, R.L. Lagendijk, "Watermarking Digital Image and Video Data", in IEEE Signal Processing Magazine, Vol 17, pp 20-43, September 2000.

[7] Ingemar J.Cox, Matt L. Miller and Jeffrey A. Bloom, "Watermarking Applications and their properties", Int. Conf. On Information Technology'2000, Las Vegas, 2000.

[8] Gerhard C. Langelaar, Iwan Setyawan, and Reginald L. Lagendijk, "Watermarking Digital Image and Video Data", IEEE Signal Processing Magazine, September 2000.

[9] Maurice Mass, Ton Kalker, Jean-Paul M.G Linnartz, Joop Talstra, Geert F. G. Depovere, and Jaap Haitsma, " Digital Watermarking for DVD Video Copy Protection", IEEE Signal Processing Magazine, September 2000.

[10] Fabien A.P. Petitcolas, " Watermarking Schemes Evaulation", IEEE Signal Processing Magazine, September 2000

[11] Technical Report, submitted to The Scientific and Technical Research Council of Turkey (Tübitak) under project EEEAG 101E007, April 2002

[12] Jean François Delaigle, " Protection of Intellectual Property of Images by perceptual Watermarking", Ph.D Thesis submitted for the degree of Doctor of Applied Sciences, Universite Catholique de Louvain, Belgique.

[13] Ingemar J. Cox, Joe Kilian, Tom Leighton, and Talal Shamoon, "Secure Spread Spectrum Watermarking for Multimedia", IEEE Trans. on Image Processing, 6, 12, 1673-1687, (1997).

[14] Mitchell D. Swanson, Mei Kobayashi, and Ahmed H. Tewfik, "Multimedia Data- Embedding and Watermarking Technologies", Proceedings of the IEEE., Vol. 86, No. 6, June 1998.

[15] Mitchell D. Swanson, Bin Zhu, and Ahmed H. Tewfik, "Transparent Robust Image Watermarking", 1996 SPIE Conf. on Visual Communications and Image Proc.

[16] Christine I. Podilchuk and Wenjun Zeng, " Image-Adaptive Watermarking Using Visual Models", IEEE Journal of Selected Areas in Communications, Vol.16, No.4, May 1998.

[17] Raymond B. Wolfgang, Christine I. Podilchuk and Edward J. Delp, "Perceptual Watermarks for Image and Video", Proceedings of the IEEE, Vol. 87, No. 7, July 1998.

[18] Sergio D. Servetto, Christine I. Podilchuk, Kannan Ramchandran, "Capacity Issues in Digital Image Watermarking", In the Proceedings of the IEEE International Conference on Image Processing (ICIP), Chicago, IL, October 1998.