ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 4, July 2014

Transformed Based Secured Watermarking Of Image Signal

[1]Huma Vohra, [2]Rajiv Dahiya
[1]M-Tech Scholar, PDM College of Engineering, Bahadurgarh, Haryana
[2]Assistant Professor, PDM College of Engineering, Bahadurgarh, Haryana

Abstract: - This paper present digital watermarking techniques for image signal based on transformation. Different transformed based watermarking techniques are available such as Discrete Fourier transform, discrete sine transform, discrete cosine transform and discrete wavelet transform. Here, we are using a new type of digital watermarking based on DCT-II transform. Transform domain techniques are a frequency domain watermarking of image signal. Transform based techniques is operates in the frequency domain embedding a watermark image in a selected set of DCT-II coefficients. Watermark casting is performed by exploiting the masking characteristics of the Human Visual System, to ensure watermark invisibility. Watermarking is the direct embedding of additional information into the original content or host signal. Ideally, there should be no perceptible difference between the watermarked and original signal and the watermark should be difficult to remove or alter without damaging the host signal. A straightforward way to provide an imperceptible watermark is to embed the watermark signal into the perceptually insignificant portion of the host data. This makes the watermark vulnerable to attack because it is fairly easy to remove or alter the watermark without affecting the host signal. Results show the performance of DCT-II based watermarking of gray scale image and color image in the presence of Dithering Distortion, noise attack: Salt and pepper noise, additive white Gaussian noise, Average filtering and median filtering. Simulation results reveal that the DCT-II watermarking outperforms over existing watermarking techniques.

Keywords: **- Secured Image watermarking, Transform based techniques, Discrete Fourier transform (DFT), discrete sine transform (DST), discrete cosine transform (DCT-II) and discrete wavelet transform (DWT).**

I. INTRODUCTION

In recent times, internet is being increasingly used as the platform for distribution of digital multimedia content. The inherent flexibility of Internet facilitates users to transact with one another to create, distribute, store, peruse, subscribe, enhance, modify and trade digital content in various forms like text documents, databases, e-books, still images, audio, video, computer software and games. 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. Watermarking is used in many applications where security and robustness is the main requirement these application includes Fingerprinting, Authentication, Copy and Playback Control, and signalling [1]-[3].

The use of an open medium like Internet gives rise to concerns about protection and enforcement of intellectual property rights of the digital content involved in the transaction. In addition, unauthorized replication and manipulation of digital content is relatively trivial and can be done using inexpensive tools, unlike the traditional analog multimedia content. Digital watermarking is the imperceptible insertion of copyright information into multimedia data [4], where the information remains detectable as long the quality of the content itself is not rendered useless. It is commonly assumed that digital watermarking is the only one of several measures that has to be combined to build a good copy protection mechanism [4].

Although there are a variety of digital watermarking methods but the performance of any digital watermarking must be evaluated on merits such as: transparency, robustness, capacity, security, and rapid detection. In a good watermarking algorithm [3]-[7], the watermark that has been inserted into the host signal should be invisible by the human eye. Usually each watermarked signal may be subjected to intentional or unintentional attacks where the signal is chased and an attempt is made to alter or remove the watermark from the watermarked signal. Filtering, adding noise, and geometric distortions are among these attacks. All video watermarking methods are categorized into two domains: uncompressed domain [8]-[12] and compressed domain [13], [14]; in which the uncompressed domain can in turn be divided into spatial domain [12] and transform domain [8]-[11].

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 4, July 2014

This paper present digital watermarking techniques for image signal based on transformation. Different transformed based watermarking techniques are available such as Discrete Fourier transform, discrete sine transform, discrete cosine transform and discrete wavelet transform. Here, we are using a new type of digital watermarking based on DCT-II transform. Transform domain techniques are a frequency domain watermarking of image signal. Transform based techniques is operates in the frequency domain embedding a watermark image in a selected set of DCT-II coefficients. Watermarking is the direct embedding of additional information into the original content or host signal. This makes the watermark vulnerable to attack because it is fairly easy to remove or alter the watermark without affecting the host signal.

The rest of the paper is organized as follows: In Section II, basic steps of digital watermarking is explained with visible and invisible watermarking. Section III presents the DCT-II based watermarking. Different steps used with digital watermarking are presented. Section IV, simulation results will be explained with the help of graphical representation in the presence of Dithering Distortion, noise attack: Salt and pepper noise, additive white Gaussian noise, Average filtering and median filtering. Section V, conclusions will be made.

II. DIGITAL WATERMARKING

Digital watermarking is the process of embedding information into a digital signal. In visible watermarking, the information is visible in the picture or video. Typically, the information is text or a logo which identifies the owner of the media [7]. In invisible watermarking, information is added as digital data to audio, picture or video, but it cannot be perceived as such. An important application of invisible watermarking is to copyright protection systems, which are intended to prevent or deter unauthorized copying of digital media [5].

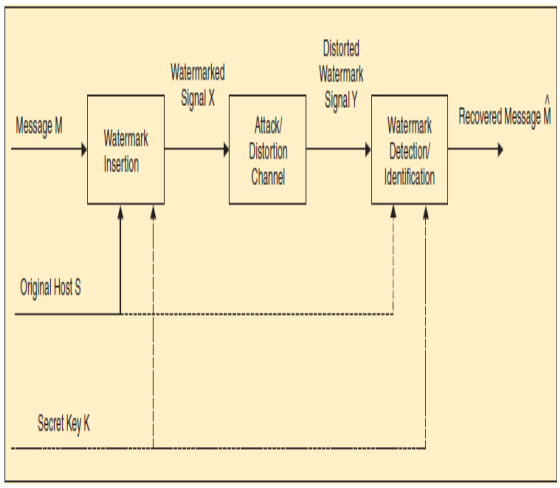


Fig. 1 digital watermarking System

All digital watermarking schemes could possibly partake in the same generic principal of the watermarking implementation which are the two watermarking systems and known as embedding and extracting systems. The scheme's input is the watermark itself and it can be such an image or a secret key. The digital watermark can be formed in many different forms such as a text, a number or even an image. The real use of the key the scheme has is to compel the security which then can prevent those unauthorized parties from manipulating either from recovering the watermark. The watermark scheme will have an output which is the watermarked data. Fig. 1 shows the generic scheme for digital watermarking technique.

III. DCT-II BASED WATERMARKING

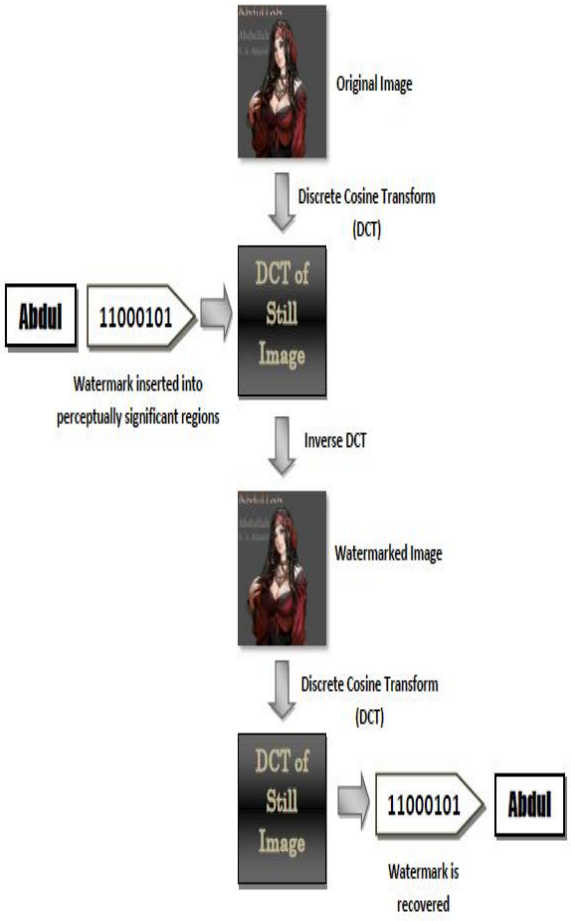
In this section, we are presenting the watermarking algorithm based on DCT-II with both colour and B/W image.

A. DCT-II TRANSFORM BASED EMBEDDING SYSTEM

Let's X is referred to the original image (cover image), and its size N_1 X N_2. Moreover, let us suppose Y as a notation for the watermark image and its size noted as M_1 X M_2. The size of the watermark image that we

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 4, July 2014

donated as *Y* is supposed to be smaller than the size of the cover image *X*. Fig. 2 shows the essential procedure that could insert the desired watermark into the DCT transform of the cover image. As well that the watermark can be extracted once again due to the procedure of executing the DCT transform on the watermarked image.



Step 1: Both the cover image *X* and the watermark *Y* must be divided into block.

Step 2: For the purpose of enhancing the perceptual invisibility, we need to take within consideration the understanding of the original image characteristics. Thus, those divided blocks from the watermark which contain such more details or more complex contents should be in fact embedded into those blocks of the original image which also consist of more information.

Step 3: After breaking the original image *X* into blocks, the DCT transform[15] is then applied and performed for each block of the image *X* so that each single block can be DCT transformed independently[16].

Step 4: Since we have got the image *X* and the watermark *Y* converted into the frequency domain as in the new resultant image *A*, all we need to do next is extracting out the middle-frequency coefficients (*FM*) from the computed image *A*. In fact, there is a significant cause for the reason of choosing the middle-frequency coefficients of *A* and it is due to two significant folded as follow:

1. The first basis is that the human eye indeed is more sensitive to whatever noise existing within the frequency components of the low region (*FL*), so it's more sensitive to the noise in those lower

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 4, July 2014

frequency components than to the components of the higher frequencies. Therefore, we should not replace the watermark into those components where the low frequency region is placed.

2. The second basis however is the fact that since the components of the higher frequencies are being affected by means of the quantization operation for the JPEG lossy compression, replacing the watermark into this frequency band of the high region (*FH*) may discard the watermark while performing the lossy compression.

Step 5: for any DCT transformed image that has been divided into the size of 8x8 block out of 64 coefficients there will be only two-middle coefficients chosen.

Step 6: Afterwards, we will attain the reduced image as well as obtaining the modified digital watermark which both have the size *M1 x M2*.

Step 7: The final procedure can be performed by mapping the middle-frequency coefficients we achieved into the resulted image in the frequency domain *A* which leads us to come by the *À*. The associated result we have got *À* would then require the inverse function of the DCT for the purpose of accomplishing the watermarked image *X`*.

B. DCT TRANSFORM BASED EXTRACTION SYSTEM

The proper technique for extracting back the invisible watermark from the watermarked image and analyzing this scheme by such following up stages

Step 1: The extracting system requires all of the original image *X* as well as the resultant watermarked image *X`* and either the digital watermark.

Step 2: The discrete cosine transform function should be applied to both of the watermarked image and the reference image through the decoding process, so that the images can be DCT transformed after being computed and converted into the frequency domain in consequence of the functionality of the DCT [16].

Step 3: Now since we have already applied the DCT for the purpose of decoding the reference image as well as the watermarked image in virtue of the property thereafter is to generate the reduced image which will help us to get rid of the low frequency and high frequency DCT components as long as that reduced image contains only of the middle frequency coefficients.

Step 4: That generated image (reduced image) which is composed of the middle-band frequencies (FM) will then give us the chance for cultivating the polarity pattern. So then we are almost in the last stage to retrieve back the embedded watermark signature.

IV. SIMULATION RESULTS

In this section, simulation results are presented for watermarking of gray scale image and color image in the presence of Dithering Distortion, noise attack: Salt and pepper noise, additive white Gaussian noise, Average filtering and median filtering.

A. WATERMARKING WITH DITHERING DISTORTION

Fig. 3 shows the Dithered distorted image. Fig. 4 shows the Watermark Detector response to dithered image.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 4, July 2014

Fig. 3 Dithered image

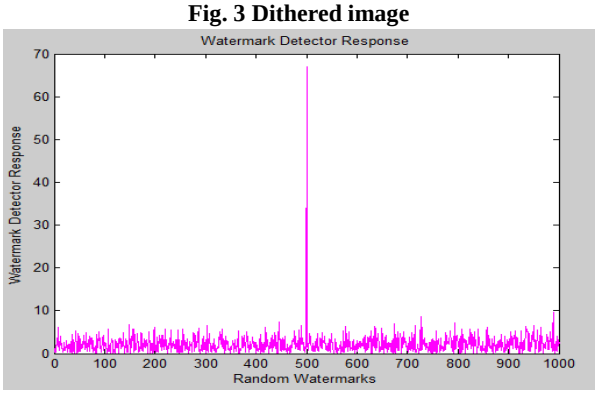


Fig. 4 Watermark Detector response to dithered image

B. WATERMARKING WITH NOISE ATTACK: SALT AND PEPPER NOISE

Fig. 5 shows the Salt and pepper noise distorted image. Fig. 6 shows the Watermark Detector response to Salt and pepper noise distorted image.

Fig. 5 Salt and pepper noise distorted image

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 4, July 2014

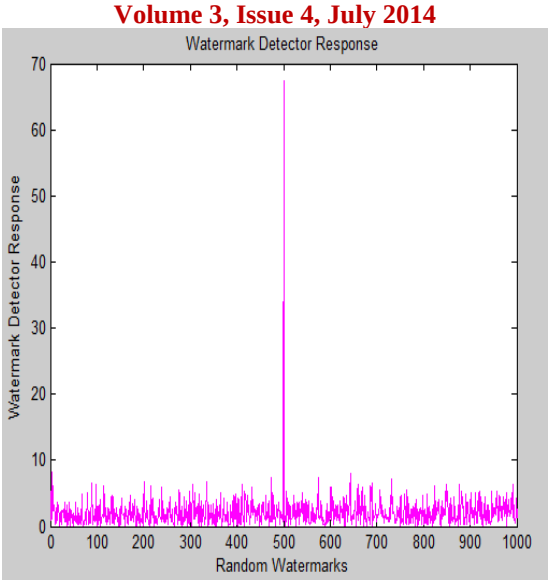


Fig. 6 Watermark Detector response to Salt and pepper noise distorted image

C. WATERMARKING WITH NOISE ATTACK: ADDITIVE WHITE GAUSSIAN NOISE

Fig. 7 shows the additive white Gaussian noise distorted image. Fig. 8 shows the Watermark Detector response to additive white Gaussian noise distorted image.

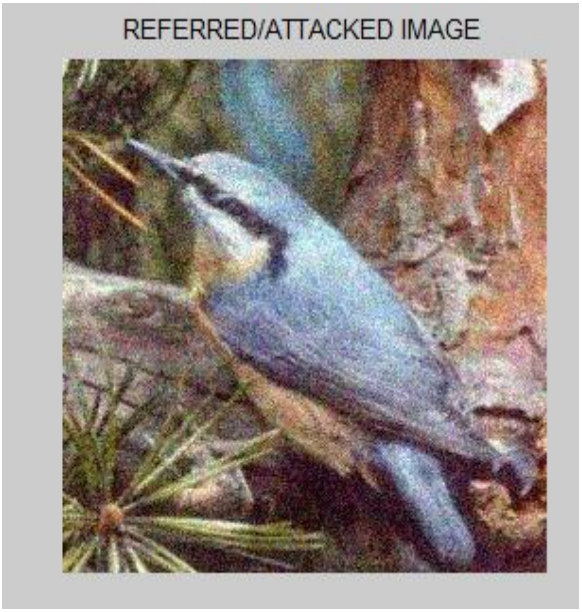


Fig. 7 additive white Gaussian noise distorted image

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 4, July 2014

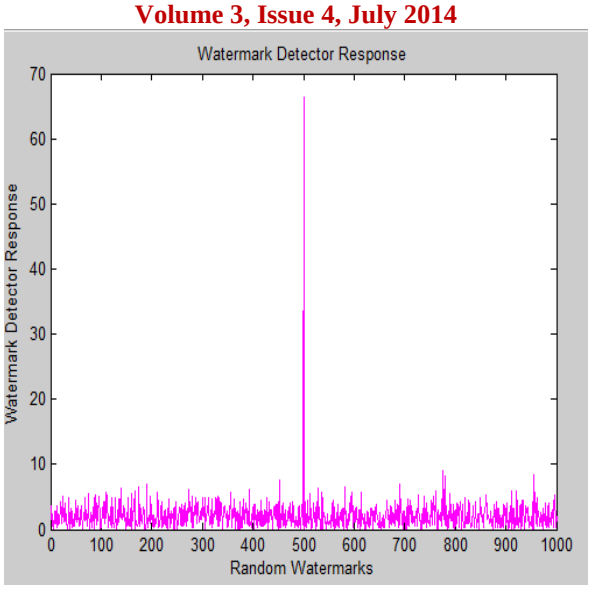


Fig. 8 Watermark Detector response to additive white Gaussian noise distorted image

D. WATERMARKING WITH LINEAR FILTERING ATTACK: AVERAGE FILTERING

Fig. 10 shows the Average filtering attacked image. Fig. 11 shows the Watermark Detector response to Average filtering attacked image.

Fig. 11 Average filtering attacked image

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 4, July 2014

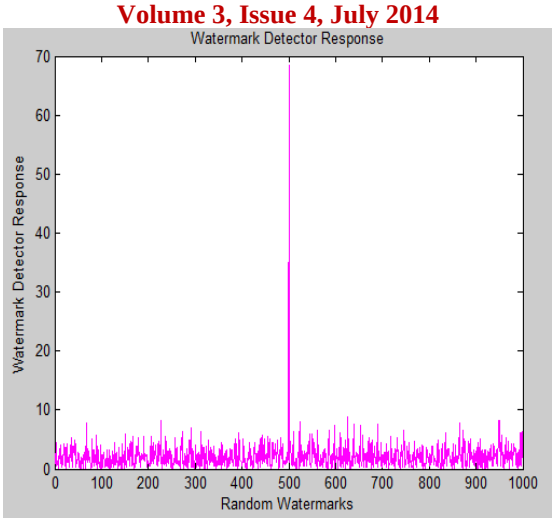


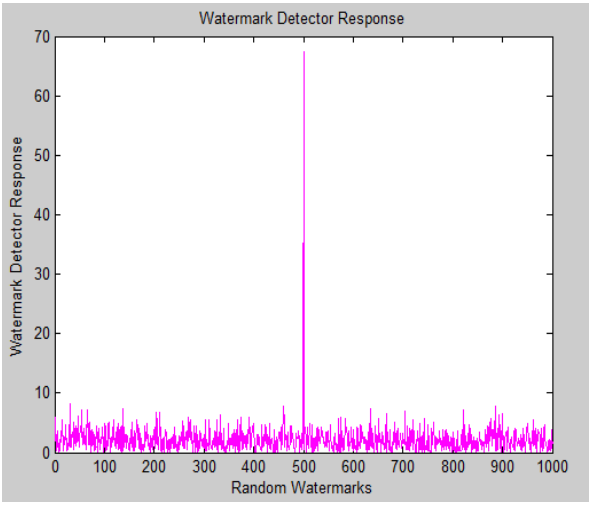
Fig. 12 Watermark Detector response to Average filtering attacked image

A.

E. WATERMARKING WITH LINEAR FILTERING ATTACK: MEDIAN FILTERING

Fig. 13 shows the median filtering attacked image. Fig. 14 shows the Watermark Detector response to median filtering attacked image.

Fig. 13 median filtering attacked image



ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 4, July 2014

Fig. 14 Watermark Detector response to median filtering attacked image

V. CONCLUSIONS

In this paper, we present digital watermarking techniques for image signal based on transformation. Different transformed based watermarking techniques are available such as Discrete Fourier transform, discrete sine transform, discrete cosine transform and discrete wavelet transform. Here, we are using a new type of digital watermarking based on DCT-II transform. Transform domain techniques are a frequency domain watermarking of image signal. Transform based techniques is operates in the frequency domain embedding a watermark image in a selected set of DCT-II coefficients. Watermark casting is performed by exploiting the masking characteristics of the Human Visual System, to ensure watermark invisibility. Watermarking is the direct embedding of additional information into the original content or host signal. Ideally, there should be no perceptible difference between the watermarked and original signal and the watermark should be difficult to remove or alter without damaging the host signal. A straightforward way to provide an imperceptible watermark is to embed the watermark signal into the perceptually insignificant portion of the host data. This makes the watermark vulnerable to attack because it is fairly easy to remove or alter the watermark without affecting the host signal. Results show the performance of DCT-II based watermarking of gray scale image and color image in the presence of Dithering Distortion, noise attack: Salt and pepper noise, additive white Gaussian noise, Average filtering and median filtering.

REFERENCES

[1]. Furon T. and P. Duhamel. Copy Protection of Distributed Contents: An Application of Watermarking Technique. in Workshop COST 254: Friendly Exchange through the net. 2000. Bordeaux, France.

[2]. P. Meerwald, A. Uhl, “Watermark Security Via Wavelet Filter Parameterization”, International Conference on Image Processing, Thessaloniki, Greece, 2001.

[3]. P. Meerwald, A. Uhl, “A Survey of Wavelet-Domain Watermarking Algorithms” EI San Jose, CA, USA, 2001.

[4]. H. Inoue, A. Miyazaki, T. Katsura “An Image Watermarking Method Based on the Wavelet Transform”, Kyushu Multimedia System Research Laboratory.

[5]. F.A.P. Petitcolas, , “Watermarking Schemes Evaluation” ”, in IEEE Signal Processing Magazine, Vol 17, pp 58-64, September 2000.

[6]. F.A.P. Petitcolas, “Introduction to information hiding” in Information Techniques for Steganography and Digital Watermarking, S.C. Katzenbeisser et al., Eds. Northwood, MA: Artec House, Dec. 1999, pp 1-11.

[7]. A.H. Tewfik, “Digital Watermarking”, in IEEE Signal Processing Magazine, vol 17, pp 17-88, September 2000.

[8]. Yan Liu, Jiying Zhao, "A new video watermarking algorithm based on ID DFT and Radon transform," Signal Processing 90 (2010) 626-639.

[9]. Radu O. Preda and Dragos N. Vizireanu, "A robust digital watermarking scheme for video copyright protection in the wavelet domain," Measurement 43 (2010) 1720-1726.

[10]. Dooseop Chio, Hoseok Do, Hyuk Choi and Taejeong Kim, "A blind Mpeg-2 video watermarking robust to camcorder recording," Signal Processing 90 (2010) 1327-1332.

[11]. Alper Koz and A. Aydin Alatan, "Oblivious Spatio-Temporal Watermarking of Digital Video by Exploiting the Human Visual System," IEEE Transactions on circuits and systems for video technology, vol. 18, no. 3, March 2008.

[12]. B. Mobasseri, M. Sieffert and R. Simard, "Content authentication and tamper detection in digital video,” Proceeding of IEEE International Conference on Image Processing, vol. 1, 2000, pp. 458-461.

[13]. Dengpan Ye, Changfu Zou, Yuewei Dai and Zhiquan Wang, "A new adaptive watermarking for real-time MPEG videos,” Applied Mathematics and Computation 185 (2007) 907-918.

[14]. J. Zhang, A. Ho, G. Qju and P. Marziliano, "Robust video watermarking of H.64/AVC," IEEE Transactions on Circuits and System-II: Express Briefs 54 (February) (2007) 205-209.

[15]. Barni Mauro, et al., A DCT-domain system for robust image watermarking. Signal Processing, 1998. **66**(3): p.357-372.

[16]. Yang Cheng-Han, Hui-Yu Huang, and Wen-Hsing Hsu. An adaptive video watermarking technique based on DCT domain. in 8th IEEE International conference on computer and information technology. 2008. Sydney. p. 589-594.