Robust Non-Oblivious DWT-Adaptive Invisible Digital Watermarking

Mr. K.Naga Prakash
Dept of Electronics and Computer Engineering
KL University
Vijayawada, India

Ms. Gajula Sindhuri
Dept of Electronics and Computer Engineering
KL University
Vijayawada, India

Mr. K.Akshay
Dept of Electronics and Computer Engineering
KL University
Vijayawada, India

Mr. G.Apuroop
Dept of Electronics and Computer Engineering
KL University
Vijayawada, India

Abstract: **The main idea of this paper is embedding invisible watermark into an image. The advantage of this method over previous works is that it is easy to embed and robust to attacks. Non-oblivious detection technique is used. This is implemented using matlab and is verified for the robustness and results are compared with previous. Here we introduced a factor 'k' as scaling factor for the watermark. To make the embedding more strong divide the image into different sub levels and each sub level is again divided into sub bands and watermark is embedded into each sub band except the low frequency band. To achieve this we adapted the transform domain method using the DWT. To HVS minute changes in high frequencies are imperceptible, hence based on this we perform invisible watermarking. We use DWT transform domain as it is better to embed the watermark in transform domain, selecting only perceptually significant coefficients, because those are the most likely to survive compression. We use a non-oblivious technique for detection of the watermark and extract it from the cover image**

Keywords-*watermark, non-oblivious, imperceptible, Discrete Wavelet Transform (DWT), Human Visual System (HVS).*

I. INTRODUCTION

Digital watermarking **[1,2]** is the process of embedding information into a digital signal which may be used to verify its authenticity or the identity of its owners. It came into existence in order to solve the problems related to digital media available online like images which may be subject to illegal copy. Images watermarking encoding can be classified into two classes namely the additive class known by spread spectrum(SS)[11] methods introduced by Cox et al. [2], and the substitutive class known by Quantization Index Modulation (QIM) methods introduced by Chen and Wornell [3]. After embedding the watermark, there should be no perceptual degradation. The watermark decoder is of three types oblivious (the cover work is not known at the decoder, only the secret key is used), semi-blind (using the watermarked data and the secret key) or non-oblivious (using the cover work and the secret key), comparatively non-oblivious is better as it assures robustness and also is more secure. Apart from these, there are some important features for watermarking to be considered like robustness: A digital watermark is called *robust,* if it resists a designated class of transformations (intentional or unintentional attacks like AWGN, filtering, lossy compression, scaling,).

Robust watermarks may be used in copy protection applications to carry copy and no access control information. Perceptibility: A digital watermark is called *imperceptible* if the original cover signal and the marked signal are (close to) perceptually indistinguishable, data hiding capacity (the amount of information that can be embedded into the original cover work without causing serious distortions) and computational cost and

complexity. It is today widely accepted that robust image watermarking techniques should largely exploit the characteristics of the HVS[4], for more effectively hiding a robust watermark [1], [5], [6]. Watermarking techniques can be broadly classified into two categories: such as spatial domain methods [4] [5] and transform domain methods [6] [7]. Spatial domain methods are less complex as no transform is used, but are not robust 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) has a number of advantages over other transform such as progressive and low bit-rate transmission, quality scalability and region-of-interest (ROI) coding demand more efficient and versatile image.. Cox *et al*. embeds a continuous watermarking the largest 1000 DCT coefficients of the original image, except the DC coefficient, thus spreading its energy on several bins of frequency [2].

Detection is made using the similarity between the two watermarks. Xia *et al*. [7] insert several watermarks in the DWT domain in each detail image. We propose a technique that embeds watermark redundantly into the coefficients at each level into three sub bands.

In this paper we presented the watermark embedding and detection with examples, followed by the results and finally the conclusion.

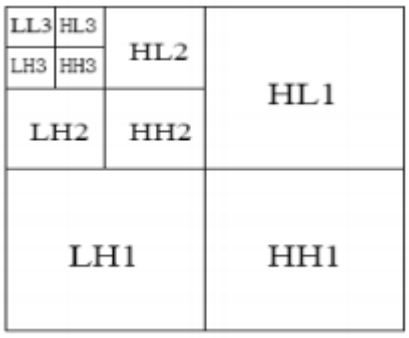
II. EMBEDDING AND DETECTION OF THE WATERMARK:

Watermark is embedded into detail sub bands of the cover image, using Discrete Wavelet Transform (DWT) through Daubechies 2pt analysis wavelet filter bank [8] the original image is decomposed into L levels and in each sublevel in each sub band the watermark is embedded. The algorithm for embedding is as follows.

-Initially the image is read and is resized into 256x256 for our convenience.

-Using DWT the image is divided into different layers and each layer to 4 sub bands namely LL(low frequency band), LH(vertical), HL(horizontal), HH(diagonal high pass bands).

-Here in this paper we divide the image in to three sub layers and three sub bands each. Hence we embed the water mark into each sub band in each layer ie., total of 9 sub bands.



SUB BANDS IN EACH SUB LAYER

-In the above figure we can see that the image is divided into 3 sub layers in each layer all are high frequency bands, as low frequency band distortions are perceptible to human eye we do not embed watermark into LL band.

ORIGINAL IMAGE DIVIDED IN TO SUB BANDS

-Let us call S the sub band resolution level l={0,1,2,3} and with orientation ϴϵ{0,1,2,3}

-The watermark, consisting of a pseudorandom binary sequence, is inserted by modifying the wavelet coefficients belonging to the three detail bands at level 0

i.e., s_0^0, s_0^1, $and\ s_0^2$

-The choice of embedding the watermark only into the three largest detail sub bands was motivated by experimental tests, as the one offering the best compromise between robustness and invisibility where 2Mx2N are the dimensions of the host image and sub bands coefficients are then modified according to the rule

The choice of embedding the watermark only into the three largest detail sub bands was motivated by experimental tests, as the one offering the best compromise between robustness and invisibility where2Mx2N are the dimensions of the host image and sub bands coefficients are then modified according to the rule

$s_0^{\emptyset}$ (i,j) = $s_0^{\emptyset}$ (i,j)+$\alpha w^{\emptyset}$(i,j)$x^{\emptyset}$(i,j)

where α is a global parameter accounting for watermark strength, and$w^{\emptyset}$ is a weighing function considering the local sensitivity of the image to noise. It is this weighing function that allows to exploit the masking characteristics of the HVS.

- We also introduce a scaling factor k with which the watermark is embedded.

-The watermark which is embedded in the received image is detected using non-oblivious technique.

-Hence both the cover image and the secret key are required for the detection process.

$$\tilde{b}(m,n) = \mathrm{sgn}\left\lfloor \frac{c'_{s,l}(m,n) - c_{s,l}(m,n)}{c_{s,l}(m,n)} \right\rfloor$$

Where b(m,n) is the recovered watermark bit. By this way the watermarks are extracted from all 9 sub bands. C(m,n) is the cover image where l is the no of levels E{h,vd}i.e., horizontal, vertical and diagonal components. The final watermark is computed from these sub bands watermarks by making a comparison using the majority rule defined as follows: the most common bit values from the recovered sub bands are assigned to the final watermark. We use the inverse dwt for extraction of the embedded watermark, the most common bit values from the recovered sub bands are assigned to the final watermark.

RESULTS:

The proposed method is tested over various images. The Daubechies 2pt (db2) wavelet [8] is used to produce the wavelet coefficients. In this paper, we consider the images with number of rows and columns are of equal size since the embedded watermark is a square matrix. The proposed method is tested using MATLAB. After embedding the watermark, there was no visual difference between the original and watermarked images as seen below.

Original image

watermark to embed

Watermarked image

extracted watermark

-The distortion caused by the watermark can be measured by the peak signal-to-noise ratio (PSNR), SSIM respectively [9]. The security value for data hiding can be measured using Kulback Leibler distance [10].

PSNR=$10log10(255^2/MSE)$

where MSE is Mean Squared Error between original and distorted images, which is defined as

MSE=$\sum_{i=0,j=0}^{m-1,n-1}$ $[OI(i,j) - DI(i,j)]^2/MxN$

-where OI is original image and DI is the distorted image. A comparison between extracted and original watermark can be done by computing Similarity Ratio (SR) between these two patterns as defined in equation(6), which is the metric used for identifying robustness of the watermarking process.

SR=S/S+D

-where ‘S’ denotes number of matching pixel values and ‘D’ denotes number of different pixel values.

-Graphs for both MSE and PSNR are shown below.

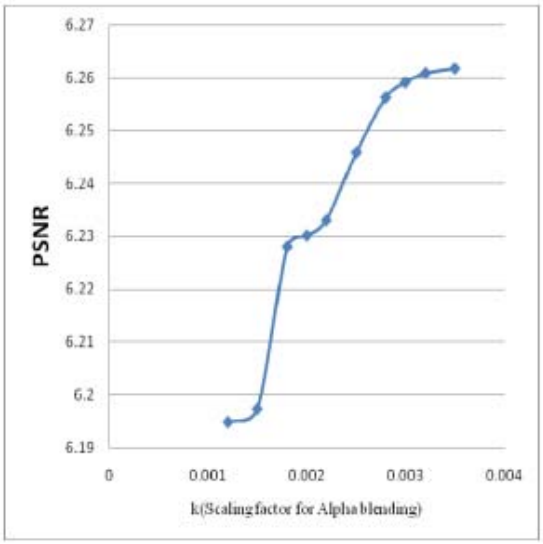


Fig. : 2 PSNR for recovered image

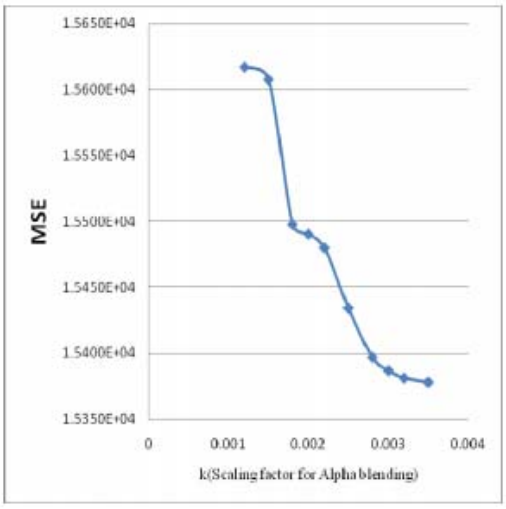


Fig. : 3 MSE for recovered image

This technique is also tested on some standard pictures as mentioned below.

Image	PSNR (dB)	SSIM
Lena	36.74	0.9827
Fishing Boat	36.68	0.9879
Peppers	39.11	0.9850
Baboon	37.68	0.9943
USAir Force	34.31	0.9798

ROBUST TO ATTACKS COMPARITIVELY

Attack	Our method	Variance based Mask	Constant Mask
JPEG	50:1	30:1	25:1
SPIHT	100:1	70:1	50:1
Despeckle + JPEG	25:1	20:1	10:1
Cropping	32 × 32	48 × 48	48 × 48

We compare our results with the previous methods and the proposed method shows more robustness comparatively to different attacks.

CONCLUSION:

Digital watermarking can be defined as a way of digital communication with high security in the digital media. In this paper we presented a robust and easy way for embedding and extracting the watermark in a single matlab file.It is also advantageous over the previous methods comparitively. This system is practically feasible for real world applications, encoding or decoding images with great speed. Future work can include applying this method for other digital information like audio, video.

Acknowledgment:

We thank Mr. K. Naga Prakash who guided us all the time.

REFERENCES:

[1] J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure Spread spectrum watermarking for multimedia," *IEEE Transaction on Image Processing*, volume 6, pages 1673-1687, 1997.
[2] B. Chen and G.W. Wornell, "Quantization index modulation: a class of provably good methods for digital watermarking and information embedding," Information Theory, IEEE Transactions on, vol. 47, no. 4, pp. 1423–1443,May 2001.
[3] I.J. Cox, J. Kilian, F.T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," Image Processing, IEEE Transactions on, vol. 6, no. 12, pp. 1673–1687, Dec 1997.
[4] N. J. Jayant, J. Johnston, and R. Safranek, "Signal compression based on models of the human perception," Proc. IEEE, vol. 81, pp. 1385–1422,1993.

[5] H. Tewfik and M. Swanson, "Data hiding for multimedia personalization, interaction, and protection," IEEE Signal Processing Mag., vol. 14, pp. 41–44, July 1997.
[6] R. B. Wolfgang, C. I. Podilchuk, and E. J. Delp, "Perceptual watermarks for digital images and video," Proc. IEEE, vol. 87, pp. 1108–1126, July 1999.
[7] X. G. Xia, C.G. Boncelet, G.R. Arce, "Wavelet transform based watermark for digital images," *Optics Express*, Vol. 3, No. 12, pp. 497-511.
[8] Daubechis, "Orthogonal bases for Compactly Supported Wavelets," Comm., Pure Appl. Math, Vol. 41, pp 909-996, 1988.
[9] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: From error measurement to structural similarity," IEEE Transaction on Image Processing,Volume 13, pages 1-14, January 2004.
[10] Cachin, "An information theoretic model for steganography," In Proc. of 2nd Workshop on Information
[11] *Hiding*. Portland, May 1998.
[12] [Cox97b] Ingemar J. Cox, Joe Kilian, Tom Leighton, and Talal G. Shamoon.
[13] "Secure spread spectrum watermarking for multimedia," In *Proceedings of the IEEE International Conference on Image Processing, ICIP '97*, volume 6, pages 1673 - 1687, Santa Barbara, California, USA, 1997.

Authors Profile:

K. Naga Prakash is presently working as Associate Professor in KL University and his area of interest is Image Processing. He is a member of CSI.

Gajula Sindhuri presently studying B.Tech final year in KL University Vijayawada. She was placed in TCS. Her area of interest is Image Processing. She is a member of ISTE and CSI.

Konijeti Akshay presently studying B.Tech final year in KL University Vijayawada. He was placed in TCS. His area of interest is Image Processing. He is a member of ISTE and CSI.

G. Apuroop presently studying B.Tech final year in KL University Vijayawada. His area of interest is Image Processing. He is a member of ISTE and CSI.