International Journal of Computer and Communication Technology

Volume 3 | Issue 4 Article 12

October 2012

Blind Adaptive Watermarking Based on Wavelet Transform and HVS

T Mita Kumari
Department of Electronics & Telecomm. Engg. C.E.B Bhubaneswar, mitat2006@gmail.com

Blind Adaptive Watermarking Based on Wavelet Transform and HVS

T Mita Kumari
Department of Electronics & Telecomm. Engg.
C.E.B Bhubaneswar,
mitat2006@gmail.com

ABSTRACT :This paper proposes a novel blind image adaptive watermarking scheme in Discrete Wavelet Transform (DWT) domain for copyright protection or robust tagging applications. Watermarking scheme effectively utilizes the contrast sensitivity model of Human Visual System (HVS) to embed the watermark adaptively without degradation of the original image. Watermark can be extracted without referring to the original image. Simulation results show the robustness of the proposed algorithm against various attacks.

1. Introduction:

The availability of versatile multimedia processing software and the far-reaching coverage of the interconnected networks have facilitated flawless copying and manipulations of the digital media. The ever-advancing storage and retrieval technologies have also smoothed the way for large-scale multimedia database applications. However, abuses of these facilities and technologies pose pressing threats to multimedia security management in general, and multimedia copyright protection and content integrity verification in particular. Although cryptography has a long history of application to information and multimedia security, the undesirable characteristic of providing no protection to the media once decrypted has limited the feasibility of its widespread use. For example, an adversary can obtain the decryption key by purchasing a legal copy of the media but then redistribute the decrypted copies of the original .In response to these challenges, digital watermarking schemes have been proposed in the last decade. Digital watermarking is a technique for inserting imperceptible secret information (the watermark) into an image, which can be later extracted or detected for variety of purposes including copyright protection, authentication, content integrity verification, broadcasting, etc. Indeed, there are a number of desirable characteristics that a watermarking technique should exhibit. That is, a watermarking technique should at least respect the following requirements:

Security: A watermark should be secret and must be undetectable by an unauthorized user in general. A watermark should only be accessible by authorized parties. As information security techniques, the details of a digital watermark algorithm must be published to everyone. The owner of the intellectual property image is the only one who holds the private secret keys.

Imperceptibility: One of the main requirements for watermarking is the perceptual transparency. The digital watermark should not be noticeable to the viewer. The data-embedding process should not introduce any perceptible artifacts into the original image and not degrade the perceived quality of the image.

Robustness: The digital watermark is still present in the image after attacks and can be detected by the watermark detector, especially on the attacks from compression. Possible attacks include linear or nonlinear filtering, noise addition, cropping, re-quantization, resizing, and image compression.

Capacity: Ability to detect watermarks with a low probability of error as the number of watermarked versions of the image increases.

Many watermarking schemes were proposed in recent years; generally they are classified depending on the domain of watermark insertion, i.e. the spatial-domain and frequency-domain watermarking. The earlier watermarking techniques are almost spatial-based approach. In spatial domain the watermark is embedded into the host image by directly modifying the pixel values, i.e. simplest example is to embed the watermark in the least significant bits (LSBs) of image pixels [1]. Spatial domain watermarking is easy to implement and requires no original image for watermark detection. However, it often fails under signal processing attacks such as filtering and compression and having relative low-bit capacity. For example, a simple image cropping operation may eliminate the watermark. Besides, the fidelity of the original image data can be severely degraded since the watermark is directly applied on the pixel values. In contrast to the spatial-domain-based watermarking, frequency- domain-based techniques can embed more bits of watermark and are more robust to attack; thus, they are more attractive than the spatial-domain-based methods, because the watermark information watermark information can be spread out to the entire image. Transform domain scheme includes DFT [2], DCT [3][7][8], and DWT [4][10]. However, embedding watermark in host image by DFT is suffering from the JPEG attacks. Although embedding watermark in host image by DCT is more robust than that of by DFT, the DWT has a number of advantages over the DCT, because the DWT provides both space and frequency localization, and different resolution levels. Thus, DWT based watermarking algorithm can effectively utilize the characteristics of HVS (Human Visual System) to attain good trade-off between robustness and imperceptibility. So, DWT based watermarking algorithms have gained more interest among the watermark researchers.

In the viewpoint of frequency, the high frequency area should be avoided for robustness while the low frequency area should be avoided for imperceptibility. Recent work has focused on developing methods for embedding watermarks in the middle frequency range, because this is known to provide a good trade-off between robustness and imperceptibility.

The watermarking scheme proposed in this paper is blind watermarking scheme, i.e. no original host image is required to extract the watermark in the decoder. The scheme was operated in DWT domain, which effectively utilizes the contrast sensitivity characteristic of the HVS to embed the robust watermark adaptively without degradation of the original image. The watermark is embedded in mid-frequency band to achieve good trade-off between robustness and imperceptibility. Our simulation result s shows that the proposed watermarking scheme is very robust to image compression, noise, cropping etc.

The remaining sections of this paper are organized as follows: the next section describes the proposed algorithm in detail and simulation results are provided in section 3. Discussions are concluded in section 4.

2. The Proposed Scheme

In the proposed watermarking scheme, we use $f(m,n)$ to denote the host image and $w(m,n)$ to denote the visually recognizable binary image as watermark**.**

2.1. Watermark Embedding Method

The watermark embedding technique is comprised of the 4 main stage discussed below.

2.1.1. Stage 1

The host image is transformed into the wavelet domain. We perform the one-level discrete wavelet decomposition of the original image, and we got four sub-bands, namely, LL , LH , HL , and HH . In order to avoid serious image degradation and survive lossy compression, we will embed the watermark in the mid frequency band that is LH and HL . We split LH and HL sub-band into the non-overlapping 8×8 blocks respectively, suppose that the original image is of size $M \times M$, then LH and HL will be of $\frac{M}{2} \times \frac{M}{2}$ size. After splitting there will be $\frac{M}{16} \times \frac{M}{16}$ blocks respectively in LH and HL sub-band.

The watermark image is converted into an array of bits. If the watermark is of size 32×32 , the number of bits is 1024. The number of watermark bits used should be less than total number of blocks in LH or HL sub-band.

2.1.2. Stage 2

The *salience* S (which is a numerical measure of perceptual importance) of each of these localized segments is computed using information about the contrast sensitivity characteristics of the HVS. Mathematically, contrast sensitivity is defined as the reciprocal of the contrast necessary for a given spatial frequency to be perceived. For this paper, we assume the well-known model given by Dooley [5]. We extend the model to two dimensions using the same approach as [6]. The resulting contrast sensitivity for a particular pair of spatial frequencies is given by:

$$C(u,v) = 5.05e^{-0.178(u+v)}(e^{-0.1(u+v)} - 1) \qquad (1)$$

Where $C(u,v)$ is the contrast sensitivity matrix and u and v are the spatial frequencies. The salience of each block is defined as:

$$S^{k,l} = \sum_{\forall(u,v)} C(u,v) \left| F^{k,l}(u,v) \right|^2 \qquad (2)$$

Where $1 \le k,l \le \frac{M}{16}$, $S^{k,l}$ is the salience value of the block (k,l). The $F^{k,l}(u,v)$ is the normalized discrete Fourier transform of the image block $f^{k,l}(m,n)$, where $f^{k,l}(m,n)$ is the DWT coefficient in position (m,n) in block (k,l). Thus each block generates a corresponding salience value.

2.1.3. Stage 3

In order to keep secret of watermark embedding position, we generate pseudo random number to be used as the allocation of the watermarking position of the blocks in LH and HL sub-band. In generating the pseudo random number, a 'key' is used as a seed number. To fit the random number to the number of blocks in LH and HL , it is scaled to the block numbers in LH and HL sub-band. Watermark is embedded in chosen blocks in LH and HL only. We use another different key to generate a 8×8 random sequence having distribution of $N(0,1)$ to embed a watermark bit in each chosen block [9]. The same watermark bit is embedded in the chosen blocks, which have the same location in LH and HL sub-band.

Watermark bit embedding procedure can be represented as follows:

$$\alpha_{LH}^{k,l} = \sqrt{\frac{S_{LH}^{k,l}}{\max(S_{LH}^{K,l})}}$$

(3)

$$\alpha_{HL}^{k,l} = \sqrt{\frac{S_{HL}^{k,l}}{\max(S_{HL}^{K,l})}}$$

(4)

If watermark bit=1

$$f_{LH1}^{ck,cl}(m,n) = f_{LH}^{ck,cl}(m,n) + \beta_{LH}^{ck,cl}\alpha_{LH}^{ck,cl}PN(m,n)$$
$$f_{HL1}^{ck,cl}(m,n) = f_{HL}^{ck,cl}(m,n) + \beta_{HL}^{ck,cl}\alpha_{HL}^{ck,cl}PN(m,n)$$

else

$$f_{LH1}^{ck,cl}(m,n) = f_{LH}^{ck,cl}(m,n) - \beta_{LH}^{ck,cl}\alpha_{LH}^{ck,cl}PN(m,n)$$
$$f_{HL1}^{ck,cl}(m,n) = f_{HL}^{ck,cl}(m,n) - \beta_{HL}^{ck,cl}\alpha_{HL}^{ck,cl}PN(m,n)$$

Where $1 \le m,n \le 8$, $f_{LH1}^{ck,cl}$, $f_{HL1}^{ck,cl}$ and $f_{LH}^{ck,cl}$, $f_{HL}^{ck,cl}$ are watermarked and original DWT coefficients of chosen block in LH and HL sub-band respectively. $\alpha_{LH}^{ck,cl}$, $\alpha_{HL}^{ck,cl}$ are a relative measure that gives greater weight judiciously to the embedded watermark in more salient blocks in LH and HL sub-band. $\beta^{ck,cl}$ are positive real numbers that determine a tradeoff between the imperceptibility and robustness against signal distortion. The $\beta^{ck,cl}$ range between 50% to 95% of the mean value of the sub-band blocks. PN is random sequence.

2.1.4. Stage 4

Perform one-level IDWT to obtain watermarked image.

2.2. Watermark Extracting Method

The extraction process of watermark is rather similar to the embedding process, first we compute DWT of the watermarked image and spilt LH and HL sub-band into non-overlapping 8×8 blocks and then use the same key to generate the same random number by which to find the watermark embedding position, and also use the same key to generate random sequence which have the distribution of $N(0,1)$. Then we compute the correlation between PN and the coefficients of selected block that embed the same watermark bit both in LH and HL sub-band and calculate the average correlation. Watermark bit value can be decided as follows:

If correlation >0
 watermark bit =1
else
 watermark bit =0

Watermark extraction is blind technique, and thus is more practical than non-blind one. We use correlation coefficient R and bit error rate BER to measure the robustness of the extracted watermark against different attacks.

The correlation coefficient R is defined as

$$R = \frac{\sum_{m=1}^{p}\sum_{n=1}^{q} w(m,n)w^{'}(m,n)}{\sqrt{\sum_{m=1}^{p}\sum_{n=1}^{q} w^{2}(m,n)}\sqrt{\sum_{m=1}^{p}\sum_{n=1}^{q} w^{'2}(m,n)}} \qquad (5)$$

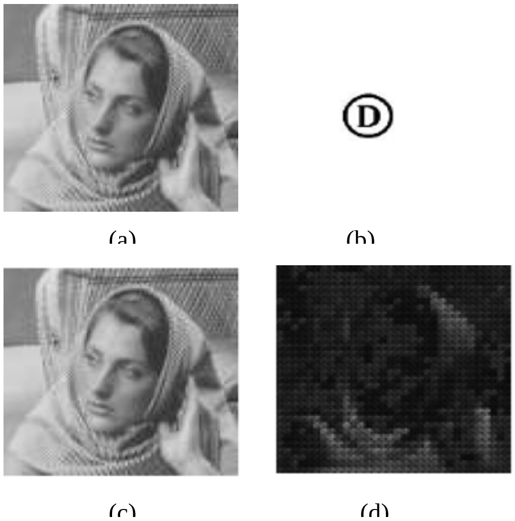
and bit error rate (BER) is defined as

$$BER = \frac{\sum_{m=1}^{p}\sum_{n=1}^{q} w(m,n)\oplus w'(m,n)}{p\times q}\times 100 \qquad (6)$$

Where $w(m,n)$ and $w'(m,n)$ are the elements of the original watermark and extracted watermark respectively, and $p\times q$ is the size of watermark $w(m,n)$.

3. Simulation Results

In order to evaluate the performance of proposed watermarking scheme, we take Barbara gray scale image with size of 512×512 as the test image, and the watermark is visually recognizable binary image of size 32×32. By using harr wavelets, we decompose Barbara image into four sub-bands and watermark are embedded in LH and HL sub-bands. We chose $\beta = 90\%$ in our simulation. Fig. 1 shows the results without any attacks using the proposed method**.**


(a) (b)

(c) (d)

Fig.1. Results for proposed watermarking method without any attack: (a) original image, (b) binary watermark image, (c) watermarked image with PSNR=35.4255, and (d) amplified

3.1. Robustness against JPEG Lossy Compression

Table 1 lists the Peak Signal to Noise Ratio (PSNR) of watermarked image, and bit error rate and Correlation values between original watermark and extracted watermark in the case that the watermarked images are attacked by JPEG compression for different quality factor. Fig 2 (a) shows the degraded watermarked image by JPEG compression of QF=50 and 2 (b) shows the corresponding extracted watermark**.**

Quality Factor	PSNR(dB)	BER (%)	Correlation (R)
90	34.7906	0	1
80	34.5648	0. 68	0.9953
70	34.3754	1.95	0.9864
60	33.9730	3.13	0.9782
50	33.5736	5.18	0.9638
40	33.0103	9.08	0.9357
30	32.1126	15.23	0.8910
20	30.7760	26.86	0.8015

Table 1. JPEG Lossy Compression

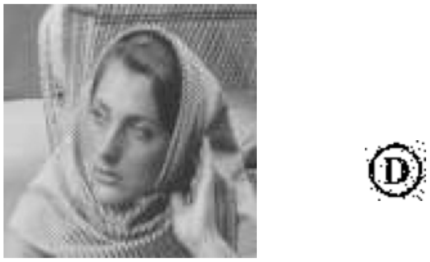

(a) (b)

Fig. 2 Result for JPEG Compression: (a) degraded watermarked image for QF=50, and (b) Extracted Watermark.

3.2. Robustness against Noise

The method was tested its robustness for both additive white Gaussian noise (AWGN) and salt & pepper noise. Table 2 shows the result for Gaussian noise for different SNR values. Table 3 shows the result for salt & pepper noise for different intensity values. Fig. 3 (a) shows the degraded watermarked image by Gaussian noise for SNR of 10 dB, and 3 (b) shows corresponding extracted watermark. Fig. 4 (a) shows the degraded watermarked image by salt & pepper noise of intensity value 0.15, and 4 (b) shows corresponding extracted watermark

Table 1. JPEG Lossy

Fig. 2 Result for JPEG

Table 2. AWGN Noise

SNR (dB)	PSNR(dB)	BER (%)	Correlation (R)
30	31.9139	0	1
25	28.4925	0	1
20	24.1408	0.097	0.9993
15	19.3679	3.03	.09789
10	14.4423	12.70	0.9092
5	9.4662	25.20	0.8144
0	4.4738	34.77	0.7366

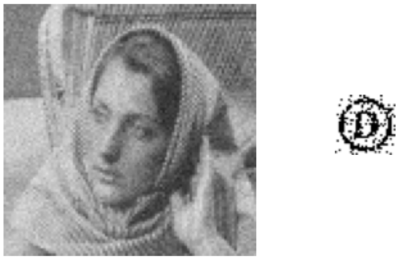


Fig. 3 Result for AWGN: (a) degraded watermarked image for SNR=10 dB, and (b) Extracted Watermark

Table 3. Salt & Pepper Noise

Noise Intensity	PSNR(dB)	BER (%)	Correlation (R)
0.05	18.4201	4.59	0.9679
0.1	15.4217	13.48	0.9038
0.15	13.6820	20.02	0.8545
0.2	12.4533	23.83	0.8270
0.25	11.4875	26.56	0.8053
0.3	10.6934	28.03	0.7913
0.35	10.0131	30.37	0.7746

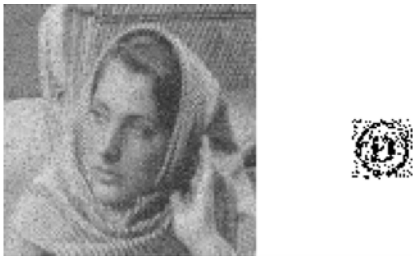


Fig. 4 Result for salt & pepper noise: (a) degraded watermarked image for intensity=0.15, and (b) Extracted Watermark

3.3. Robustness against Median Filtering

The proposed method was tested its robustness against median filtering of different order. The result was shown in table 4 for median filtering of different order and fig. 5 (a) shows the degraded watermarked image by median filtering of order $5*5$, and 5 (b) shows corresponding extracted watermark.

Table 4. Median Filtering

Order	PSNR(dB)	BER (%)	Correlation (R)
3*3	31.9710	1.76	0.9878
5*5	27.1233	19.34	0.8607
7*7	23.4634	28.22	.7906

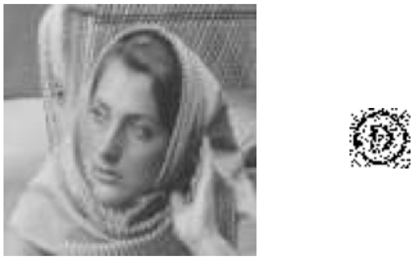


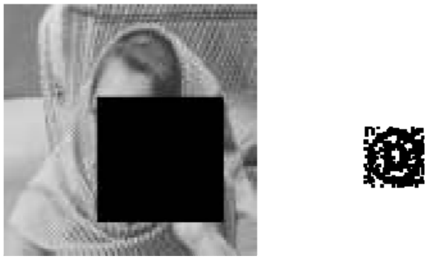
Fig. 5 Result for Median filtering: (a) degraded watermarked image for order 5*5, and (b) Extracted Watermark

3.4. Robustness against cropping

The effect of image cropping on watermark detection is shown in Table 5. Fig. 6 (a) shows the degraded watermarked image by cropping of size 256*256, and (b) shows the corresponding extracted watermark.

Table 5. Cropping

Cropping size	PSNR(dB)	BER (%)	Correlation (R)
16*16	32.5411	0	1
32*32	27.1865	0.20	0.9986
64*64	21.6680	0.88	0.9939
128*128	17.1061	4.30	0.9699
256*256	12.2104	16.50	0.8786



(a) (b)

Fig. 6 Result for Cropping: (a) degraded watermarked image for cropping of size 256*256, and (b) Extracted Watermark.

From the tables and figures, we can ensure the security and robustness of the embedded watermark against JPEG compression, Gaussian as well as salt & pepper noise, median filtering and cropping. The key, which is used to select blocks in sub-bands for embedding and extracting, makes it difficult to remove the embedded watermark.

4. CONCLUSION

In this paper, we have proposed a blind image-adaptive watermarking scheme in discrete wavelet domain; an human visual system (HVS) model based on contrast sensitivity has been incorporated to embed the watermark bit adaptively without degradation of the original image. And we embed a watermark bit through a PN sequence. Watermark extraction can be obtained without access to the original image. Simulations of various attacks shows that the scheme is robust to JPEG compression, Gaussian and salt & pepper noise, median filtering, as well as cropping. Since the scheme is blind, it is more practical. The future work is to develop a blind watermarking scheme robust to both JPEG compression and geometric attacks such as rotation and scaling

5. REFERENCES

[1] R.G. Van Schyndel, A.Z. Tirkel, and C.F.Osborne. "A digital watermark", proc. of IEEE Int. Conf. on Image Processing. Vol. 2, pp. 86-90, 1994.

[2] J.J.K.O Ruanaidh, W.J.Dowling, and F.M.Boland, "Phase watermarking of digital images", proc. of IEEE Int. Conf. on Image Processing. Vol. 143, Lausanne, Switzerland, pp. 239-242, Sept. 16-19, 1996.

[3] C.I.Podilchuk, W. Zeng, "Image-adaptive watermarking using visual models", IEEE Journal on Selected Areas in Communication, 16(4), pp. 525-539, 1998.

[4] Der-Chyuan Lou "Adaptive digital watermarking using Fuzzy clustering technique", IEICE Trans. Fundamentals. Vol.E84-A. No.8.2052-2060, Aug. 2001.

[5] M. D. Levine, Vision in Man and Machine,
New York: McGraw-Hill, Toronto, 1985.

[6] T.A. Wilson, S.K. Rogers, and L.R. Myers, "Perceptual-based hyperspectral image fusion using multiresolutional analysis", Opt. Eng., vol. 34, pp. 3154-3164, Nov. 1995.

[7] R. B. Wolfgang, E. J. Delp, "A Watermark for Digital Images", proc. of IEEE Int. Conf. on Image Processing. Lausanne, Switzerland. Sept. 16-19.

[8] B. Tao, and B. Dickinson, "Adaptive Watermarking in DCT Domain", Proc. Of IEEE Int. Conf. on Acoustics, Speech, and signal Processing. ICASSP-97, Vol. 4, pp. 1985-2988, 1997.

[9] I. J. Cox, J. Killian, F. T. Leighton, and T. Shamoon, "secure Spread Spectrum Watermarking for Multimedia", IEEE Trans. On Image Processing, Vol. 6, pp. 16731687, Dec. 1997.

[10] ***F. Hartung, and M. Kutter, "Multimedia watermarking Techniques", Proc. IEEE, Vol. 87, pp. 1079-1107,1999.***

T Mita Kumari was born in India in1981. she received the master degree from the National Institute of Technology Rourkela, India, in 2007, with a thesis entitled " Adaptive based Image Watermarking using DWT and HVS. She is currently working toward the Ph.D degree. She is currently an Sr. Lecturer of electronis and telecommunication Department in C.E.B Bhubaneswar , Biju Pattanaik University of Technology, Orissa. His research interest concerns the development of new watermarking techniques, which robust to both geometric and non-geometric attacks.