World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:2, No:1, 2008

Digital Image Watermarking in the Wavelet Transform Domain

Kamran Hameed, Adeel Mumtaz, and S.A.M. Gilani

Open Science Index, Computer and Information Engineering Vol:2, No:1, 2008 publications.waset.org/7298/pdf

***Abstract*—**In this paper, we start by first characterizing the most important and distinguishing features of wavelet-based watermarking schemes. We studied the overwhelming amount of algorithms proposed in the literature. Application scenario, copyright protection is considered and building on the experience that was gained, implemented two distinguishing watermarking schemes. Detailed comparison and obtained results are presented and discussed. We concluded that Joo's [1] technique is more robust for standard noise attacks than Dote's [2] technique.

***Keywords*—**Digital image, Copyright protection, Watermarking, Wavelet transform.

I. Introduction

WITH the increasing use of internet and effortless copying, tempering and distribution of digital data, copyright protection for multimedia data has become an important issue. Digital watermarking emerged as a tool for protecting the multimedia data from copyright infringement. In digital watermarking an imperceptible signal "mark" is embedded into the host image, which uniquely identifies the ownership. After embedding the watermark, there should be no perceptual degradation. These watermarks should not be removable by unauthorized person and should be robust against intentional and unintentional attacks. Different watermarking techniques have already been published in the literature. Overviews on watermarking techniques can be found in (Langelaar et al., 2000) [3].

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 against 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) based watermarking techniques are gaining more popularity because 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 coding that can be exploited for both, image compression and watermarking applications. The compression standard JPEG2000 is based on the discrete wavelet transform (DWT) to meet the requirements. Therefore, we think it is imperative to consider the wavelet transform domain for watermarking applications. A detail survey on wavelet based watermarking techniques can be found in (Meerwald and Uhl 2001) [8].

Kamran Hameed, Adeel Mumtaz, Syed Asif Mahmood Gilani are with the faculty of computer science and Engineering, Ghulam Ishaq Khan Institute of Engineering, Sciences and Technology. Topi, N. W. F. P., Pakistan (e-mail: kjarral71@hotmail.com, adeel@giki.edu.pk, asif@giki.edu.pk).

II. Wavelet based Watermarking Techniques

This section gives an overview of the numerous wavelet based digital watermarking techniques that have been developed to help protect the copyright of digital images and to verify multimedia data integrity. Most watermarking techniques transform the host image into a domain that facilitates embedding of the watermark information in a robust and imperceptible way. The following principal embedding strategies that can be used to embed a watermark in a host image:

1. Linear additive embedding
   - i. Gaussian sequence
   - ii. Image fusion
2. Non-linear quantization embedding, via
   - i. Scalar quantization
   - ii. Vector quantization
3. Miscellaneous embedding techniques

Additive embedding strategies are characterized by the linear modification of the host image and the correlative processing in the detection stage. The quantization schemes on the other hand perform non-linear modifications and detect the embedded message by quantizing the received samples to map them to the nearest reconstruction point [9].

III. Imlemented Techniques

We studied in detail and implemented two wavelet domain techniques proposed in [1][2], in order to compare which technique is more robust for copyright protection of intellectual property.

A. A New Robust Watermark Embedding into Wavelet DC Components [1]

Embedding: Joo's [1] watermarking technique embed watermarks into the DC area while preserving good quality fidelity. The gray image is decomposed into several bands by wavelet transform. To embed watermark i.e. a pseudo-random binary sequence {-1,1}, a reference DC′ is prepared by taking low pass filtering to the original DC. The DC values are changed to values smaller or larger than the DC′ values in

Open Science Index, Computer and Information Engineering Vol:2, No:1, 2008 publications.waset.org/7298/pdf

accordance with the corresponding watermark bits. To reduce image degradation, the watermark bits are embedded into locations with smaller differences between the DC and DC′. This is depicted in the Fig. 1.

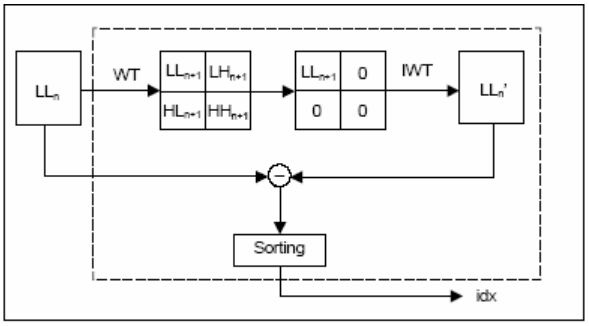


Fig. 1 Reference sub-band and location information for watermark embedding

Joo [1] replaced the DC values with the embedding formula LLn′ ± K×*w*(*i*) …(1), where K is a factor for controlling embedding intensity and w(i) is the watermark.

```
for i = 1:wm_length
  if(w(i) == +1)
    if(LLn(idx(i)) < LLn' (idx(i)) + K)
      LLn(idx(i)) = LLn' (idx(i)) + K
    end
  else if(w(i) == –1)
    if(LLn(idx(i)) > LLn' (idx(i)) – K)
      LLn(idx(i)) = LLn' (idx(i)) – K
    end
  end
end                                          (1)
```

Extraction: In extraction Joo [1] used the original image as required in extracting watermarks. Such an extraction is classified as non-blind watermarking. The same wavelet decomposition is applied to both the original and embedded images. The watermark-embedding locations are obtained from the original image. Since LLn and LLn' are obtained from the watermark embedded image, the watermarks are extracted by comparing the two values, LLn and LLn'. Then the extracted watermarks are compared with the original watermarks generated by the user key. In this comparison, Joo [1] used the similarity measure given in (2), where '.' denotes the inner product.

$$Sim(w, w^*) = \frac{w \cdot w^*}{\sqrt{w^*.w}} \tag{2}$$

B. A Robust watermarking method for copyright Protection of Digital Images using Wavelet domain [2]

Embedding: Dote's [2] presented a multilevel wavelet transformation technique. The host image and watermark are transformed into wavelet domain. Dote [2] selected 5th level transformation for host image and 1st level for watermark. The transformed watermark coefficients were embedded into those of host image at each resolution level with a secret key. The Dote's [2] technique is depicted in the Fig. 2.

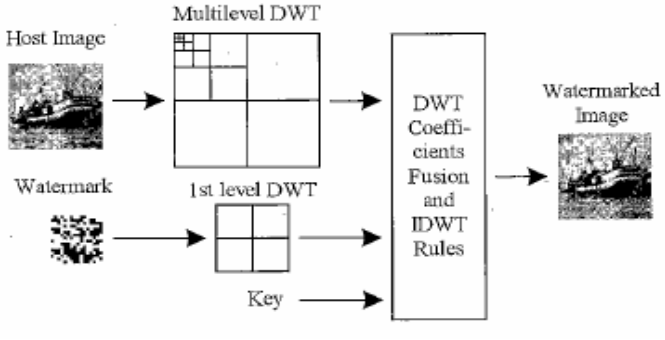


Fig. 2 Dote's proposed metod

Extraction**:** Dote [2] extracted the watermark by applying inverse procedure at each resolution level using the same secret key. Estimated the watermark by averaging the extracted watermarks and normalize it for binary values. In order to find out similarity between embedded and extracted watermarks first Dote [1] observed the host and the marked images perceptually. The correlation coefficients between them at different signal to noise ratios (SNR) values were calculated.

The correlation coefficient, ρ, used for similarity measurement, and SNR are defined in (3) and (4).

$$\rho(w, \hat{w}) = \frac{\sum_{i=1}^{N} w_i \hat{w}_i}{\sqrt{\sum_{i=1}^{N} w_i^2} \sqrt{\sum_{i=1}^{N} \hat{w}_i^2}} \tag{3}$$

$$SNR(W, \hat{W}) = 10 \log_{10} \frac{\sum_{i=1}^{N} w_i^2}{\sum_{i=1}^{N} (W_i - \hat{W}_i)^2} \tag{4}$$

Where N is the number of pixels in watermark, w and $\hat{w}$ are the original and extracted watermarks, respectively. The related measure of PSNR (in db) between host and marked image is computed using

$$PSNR = 20 \log_{10} [255/RMSE]$$

Where

$$RMSE = \sqrt{\frac{1}{M*N} \sum_{i=1}^{M} \sum_{j=1}^{N} [\tilde{f}(m,n) - f(m,n)]^2}$$

Open Science Index, Computer and Information Engineering Vol:2, No:1, 2008 publications.waset.org/7298/pdf

for the 8-bit (0-255)image.

IV. Experimental Results

In our experiments for Joo [1] and Dote [2] techniques, we performed fidelity tests to analyze the unobtrusiveness of the watermarks after watermark embedding, whether perceptual distortion occurred to the host images or not. Also we tested the robustness against standard noise attacks i. e. Gaussian, salt and pepper, Speckle and JPEG compression to the marked images. For our results we supposed that the correlation coefficient of about 0.75 or above is assumed as an acceptable value for the extracted watermarks from noisy images.

For Joo's [1] technique a pseudo-random binary sequence is used as a watermark. Sequence is generated from seed no. 500 of length 1000. The watermarks are embedded in the 512*512 gray-level Lena image. A three level DWT is employed and thus the size of the DC area to be embedded is 64*64. We set K to 28, the resulting PSNR was 43.08db. The host image, watermarked image, watermark, and extracted watermark are shown in Fig. 3.

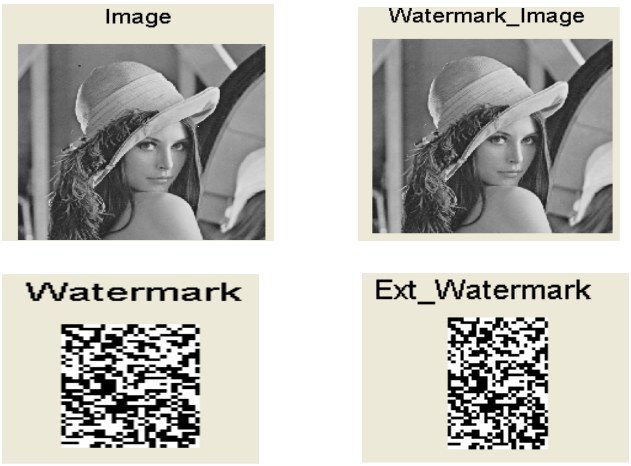


Fig. 3 Fidelity test on Joo's technique

There is no perceptual distortion in the original and watermarked image, which means that scheme has satisfied the criteria that an efficient watermark should be unobtrusive, discreet and easily extracted.

For robustness, the obtained PSNRs between host image and watermarked images under standard noise degradations, between original watermark and extracted watermarks and the correlation coefficients were calculated, respectively as shown in Table I.

TABLE I
Effect of Noise Attacks on Joo's Technique

Attacks	Images PSNRs	Watermarks PSNRs	Correlation Coefficients
Gaussian	25.59	10.14	0.89
Salt & pepper	34.99	14.44	0.99
Speckle	36.33	15.83	0.99
JPEG	35.86	17.75	0.98

The watermarked images and extracted watermarks after Gaussian, salt and pepper, Speckle and JPEG noise distortion are shown in the Fig. 4.



Fig. 4 Noise distortion attacks on Joo's Technique

For Dote's [2] technique we choose 256*256 gray intensity image and 16*16 binary watermark which is randomly generated. We set key to 500, the resulting PSNR was 47.27db. The original image, watermarked image, watermark, extracted watermark are shown in Fig. 5.

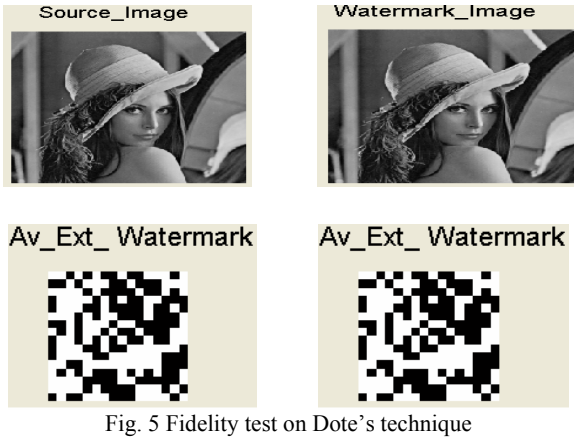


Fig. 5 Fidelity test on Dote's technique

There is no perceptual distortion in the original and watermarked image, which means that scheme has satisfied the criteria that an efficient watermark should be unobtrusive, discreet and easily extracted.

For robustness, the obtained PSNRs between host image and watermarked images under standard noise degradations,

between original watermark and extracted watermarks and the correlation coefficients were calculated, respectively as shown in Table II.

TABLE II
EFFECT OF NOISE ATTACKS ON DOTE'S TECHNIQUE

Attacks	Images PSNRs	Watermarks PSNRs	Correlation Coefficients
Gaussian	25.83	4.54	0.38
Salt and pepper	34.46	6.52	0.57
Speckle	31.28	4.78	0.33
JPEG	34.35	6.22	0.56

The watermarked images and extracted watermarks after Gaussian, salt and pepper, Speckle and JPEG noise distortion are shown in the Fig. 6.

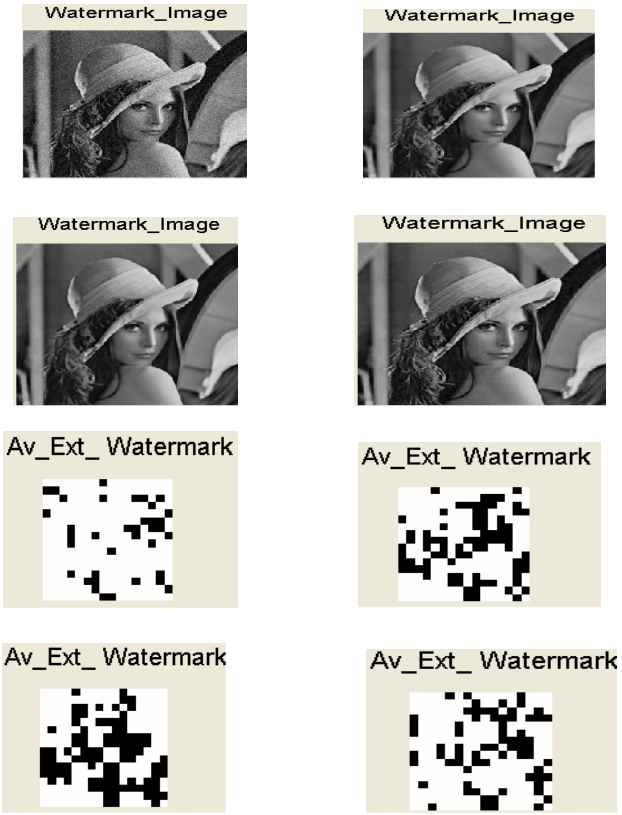


Fig. 6 Noise distortion attacks on Dote's Technique

Through experimental results, for fidelity test, we were able to strongly embed watermarks while preserving good fidelity in both Joo [1] and Dote's [2] techniques. While for robustness, we found Joo's [1] technique more robust than Dote's [2] technique under standard noise degradation i. e. Gaussian, salt and pepper, Speckle and JPEG, by comparing correlation coefficients values of Table I with Table II.

V. CONCLUSION

We review the various watermarking techniques in the wavelet transform domain. We simulated two of the techniques in detail to analyze the robustness for copyright scenario. Both the techniques were found non-obtrusive in gray level images. For robustness, Joo's [1] technique shows better results when compared with Dote's [2] technique. We extracted the watermarks from the noisy images to an acceptable degree of correlation in Joo's [1] technique. Therefore, we say that Joo's [1] technique has coped the added noise degradation and is more robust for such standard attacks.

ACKNOWLEDGMENTS

We thank Ghulam Ishaq Khan Institute (GIKI) for providing very conducive research environment as well as financial and moral support.

REFERENCES

[1] Sanghyun Joo, Youngho Suh, Jaeho Shin, and Hisakazu Kikuchi, "A New Robust Watermarking Embedding into Wavelet DC Components", ETRI Journal, Volume 24, No. 5, October 2002.
[2] Yasuhiko Dote, and Muhammad Shafique Shaikh "A Robust Watermarking Method for Copyright Prot. of Digital Images using Wavelet Trans." Trans. of the Institute of Electrical Engineering of Japan, vol. 122, No.2, Jan. 2003.
[3] Langelaar, G.C., Setyawan, I., Lagendijik, R.I., 2000. Watermarking digital image and video data. IEEE signal Process. Magazine (September), 20-46.
[4] A. G. Bors and I. Pitas., " Image watermarking using DCT domain constraints", Proc. of IEEE Int. Conf. on Image Processing, vol. 3, pp. 231-234 (1996).
[5] R.G. van Schyndel, A. Z. Tirkel, and C. F. Osborne, "A digital watermark", Proc. of Int. Conf. in Image Processing, vol. 2, pp. 86-90, (1994).
[6] J. Ohnishi and K. Matsui, "Embedding a seal into a picture under orthogonal wavelet transformation," Proc. of Int. Conf. on Multimedia Comp. and Systems, pp. 514-521(1996-6).
[7] D. Kunder and D. Hatzinakos, " A robust digital image watermarking method using wavelet-based fusion", Proc. of IEEE Int. Conf. on Acoustics, Speech and Sig. Proc., vol. 5, pp. 544-547 Seattle, Washington (1997-5).
[8] Meerwald, P., Uhl, A., 2001. A survey of wavelet-domain watermarking algorithms. In Proc. of SPIE, Electronics Imaging, Security and Watermarking of Multimedia Contents III, CA, USA 4314 (January), pp. 505-516.
[9] D. Kunder and D. Hatzinakos." Digital watermarking using multi-resolution wavelet decomposition . In Proceedings of IEEE ICAPSSP '98, volume 5, pages 2969 – 2972, Seattle, WA, USA, May 1998.

Open Science Index, Computer and Information Engineering Vol:2, No:1, 2008 publications.waset.org/7298/pdf