

A New Wavelet Based Scheme for Blind Watermarking

Gupta Chirag S., Bhokare Ganesh, Jain Nishant, Ghone Chaitanya S.

Department of Electrical Engineering, IIT Bombay
chirag@ti.com, {ganesh, nishantj, csghone}@ee.iitb.ac.in

Abstract—Watermarking is a scheme for embedding a watermark into original multimedia content securely, imperceptibly and indelibly. As DWT provides simultaneous spatial and frequency localization of an image, it has been found suitable for watermarking techniques. In this paper we propose a wavelet-based blind watermarking technique. Instead of inter-block relations, our scheme uses intra-block relations to generate the watermarked image. The watermark is embedded into the middle frequency coefficients only. This can successfully resist several frequency and time domain attacks. By exchanging or replacing the coefficient in concern with maximum or minimum (depending on the watermark bit) coefficient from its local neighborhood, we come out with two algorithm of watermarking; replacement and exchange algorithm. Performance of both algorithms is evaluated based on HVS based measure, distance distortion measure, confidence measure and PSNR.

I. INTRODUCTION

DIGITAL watermarking is, to embed information into digital data in a secret and inconspicuous way [1]. The embedded information is called a watermark. From the viewpoint of media producers and content providers, the possibility of unlimited copying and distribution without fidelity is undesirable and lead to financial losses. Watermarking provides protection of intellectual property rights (IPR).

The data in which watermark is inserted is called source data. A digital key is used to embed a watermark into source data; the same key is used to extract the watermark. A watermarking technique is referred to as a blind or a public scheme if the original image is not needed for extraction of the watermark; it is semi-blind if it requires a secret key and the watermark bit sequence for extraction; and it is a non-blind or a private scheme if the original image and the secret key both are used in extraction. The size of the image is large and very often, in the real world scenarios the availability of the original multimedia data can not be warranted, thus it makes the non-blind algorithm useless and so a blind watermarking technique is preferable over the non-blind one.

Our main focus is on the wavelet based techniques due to many advantages of DWT like, performing an analysis similar to that of the HVS, no blocking artifacts, multi-resolution property offers more degrees of freedom compared with the DCT, lower computational cost than the FFT and DCT and better energy compaction [2], [3].

There are many existing non-blind schemes for robust watermarking. Cox et al. [4] uses spread spectrum to embed watermark in the discrete cosine transform (DCT) domain. In [5], the

so-called cocktail watermarking is proposed. Complementary modulation rules, positive modulation, and negative modulation are applied on wavelet coefficients for watermark embedding. Early blind watermarking schemes were build on the principle of spread spectrum. Although this technique allows for reliable communication even for strong attack, spread spectrum based system offer relatively little robustness. Hernandez et al. [6] uses 2-D multi-pulse amplitude modulation and spread spectrum to embed bit sequences in images and develops an optimal detector. In the tree marking method [7], the wavelet coefficients of the host image are grouped into so-called super trees, and the watermark is embedded by quantizing super trees.

In [8], a DCT-based algorithm using inter-block relation to implement the middle-band embedding is presented. Our scheme is different from [8]. Instead of inter-block relations, our scheme uses intra-block relations to generate the watermarked image. All the simulations are done for the 2-band filter structure, the same can be extended to M-band filter structure.

II. THE PROPOSED BLIND WATERMARKING TECHNIQUE

We present a variant of the watermarking scheme proposed in [9] which also uses intra-block relations to generate a watermarked image, but that is DCT based and a non-blind scheme. In [9], Duan takes a block based DCT of an image. If the watermark bit is 1, he swaps the near by two DCT coefficients of the block and does nothing if watermark bit is 0. At the decoder, he takes signs of the subtraction of near by DCT coefficients of the original image and the watermarked image and does digital XOR of the signs to extract the watermark bit.

Instead of DCT, our algorithm uses DWT to embed the watermark. A main advantage of our proposed scheme is that, it is a blind watermarking scheme, i.e. we do not require the original image at the decoder side to recover the watermark from the watermarked image. The watermark is embedded into the local maxima/minima of the DWT sub bands. The originality of the proposed technique is to insert one bit of a watermark sequence in sets of few significant wavelet coefficients, by observing their dependencies, and not only their individual absolute values.

A. Watermark Embedding

- Take 2-band, N-level DWT of an image, let $C[i]$ be the i^{th} wavelet coefficient of an image, where wavelet

coefficients are scanned in Mortan scan order.

- Convert the Payload (watermark) in to binary, let $W[i]$ be the i^{th} bit of binary payload.
- If $W[j]=1$
 $C[i] = \max(C[i], C[i+1], C[i+2], C[i+3], C[i+4])$
- Else $C[i] = \min(C[i], C[i+1], C[i+2], C[i+3], C[i+4])$

B. Watermark Extraction

- Take N-level DWT of a watermarked image, let $X[i]$ be the i^{th} wavelet coefficient of an image.
- If $X[i] > \text{mean}(X[i], X[i+1], \dots, X[i+4])$
 $Wr[j] = 1$
- Else $Wr[j] = 0$

where $Wr[j]$ is retrieved watermark bit. Compare the extracted watermark with the original watermark on the basis of HVS measure, distortion measure, confidence measure and PSNR for authentication. Formulae for the Human Visual System (HVS) based measure, confidence measure, distant distortion measure and Peak Signal to Noise Ratio (PSNR) can be found in [10], [11].

With minor changes in the proposed algorithm, we came out with two approaches of the same scheme. The above mentioned approach is based on the replacement of a coefficient at encoder for watermarking and mean at decoder for the watermark extraction, while the other approach can be based on exchange of coefficients at encoder and median at decoder.

Watermarking has been applied to LH_1 , HL_1 part only because if we apply it in HH_1 part then there are higher chances that it can be removed by DCT based compression so robustness will not be achieved. If it is embedded in LL part (or higher decomposition level) will aggravate the quality of image and watermark may become perceptually visible. Thus by embedding watermark in middle frequency sub bands, we can preserve robustness and imperceptibility. Both the approaches of the scheme are applied to different images and tested for different attacks. At the encoder side the image has been watermarked and then attacks have been applied to the watermarked image to test robustness. At the decoder, watermark has been extracted out from the attacked image and HVS measure, distant distortion measure, correlation measure and PSNR is calculated between recovered and the original watermark.

III. RESULTS

We have used different images like, Lenna, Cameraman, Peppers for experiments. The images are of size of 256 by 256. For demonstration, results for the Lenna image are only shown. The watermark image used is of size 40 by 50 (i.e $40 \times 50 \times 8 = 16000$ bits). We have used a three-level

wavelet decomposition for the experiments in this paper. We have considered both non-geometric and geometric attacks, like blurring, JPEG compression, rotation, scaling, etc.

For the case when retrieved watermark is exactly equal to the original watermark, values of HVS measure and distant distortion measure would be zero, value of correlation measure would be one, and PSNR would be infinite. Without any attack on watermarked image, we get correlation coefficient one and PSNR infinite between the original watermark and the retrieved watermark. The PSNR between the original and watermarked image is 47.25 dB and 50.32 dB and the correlation coefficient is 0.97 and 0.99 respectively for the exchange and replacement algorithm. Thus the scheme (with both the approaches) provides better imperceptibility. The scheme can successfully survive common signal processing attacks like blurring and filtering too, as shown in fig 1 to 3. The scheme gives correlation coefficient as high as 0.935 even with the 30 percentage of the blur attack.

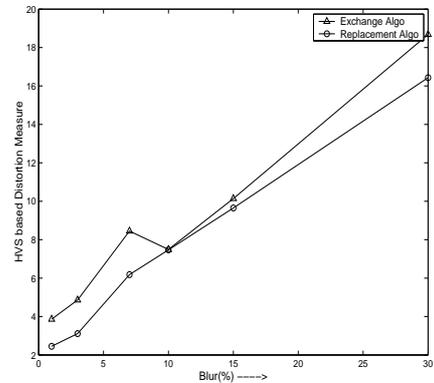


Fig. 1. HVS Based Distortion measure with blur attack

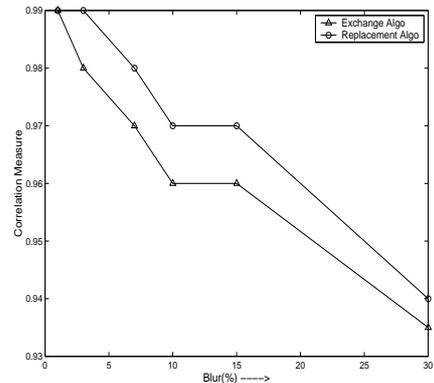


Fig. 2. Correlation measure with blur attack

JPEG is one of the most used compression technique, and is often an unintentional attack. Results for the attack are shown in fig 4 to 6. The proposed scheme (for both the algorithms) gives correlation coefficient near to 0.75 even with the quality factor of 20. Thus it can survive the compression attack very successfully. The geometric attacks like rotation can

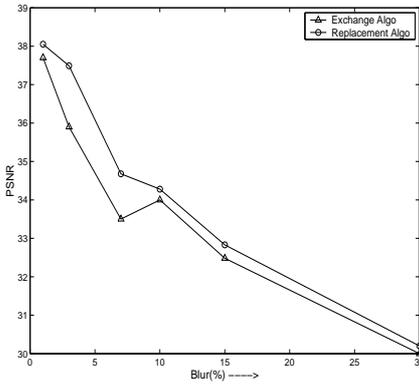


Fig. 3. PSNR(dB) measure with blur attack

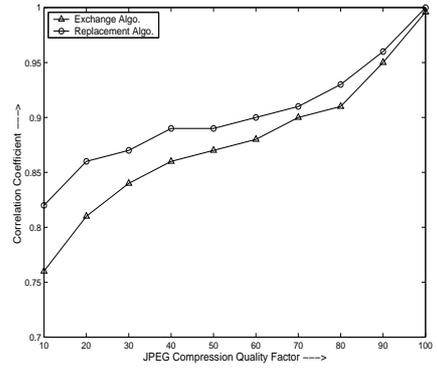


Fig. 6. Correlation measure with JPEG compression attack

severely affect watermark extraction, especially for pixel-based watermarking systems, but from the results fig 7 and 8 we can say that our approach can resist it effectively. We can see that the proposed scheme can resist a much larger rotation attack.

one.

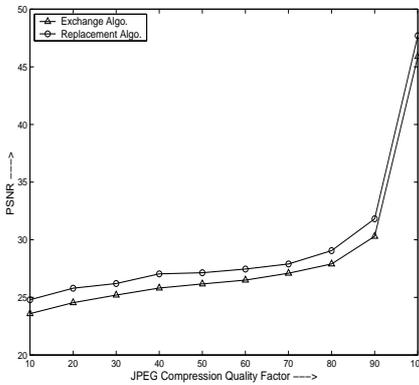


Fig. 4. PSNR(dB) measure with JPEG compression attack

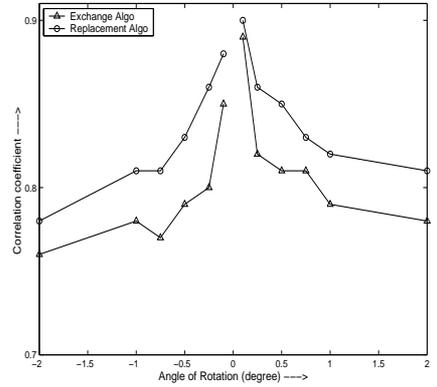


Fig. 7. Correlation measure with Rotation attack

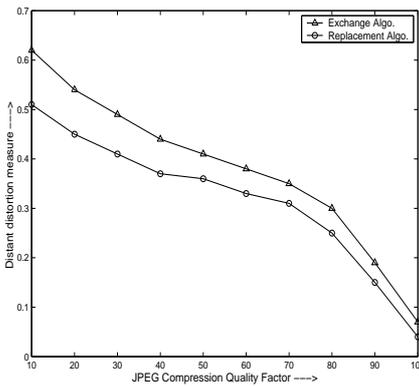


Fig. 5. Distance Distortion measure with JPEG compression attack

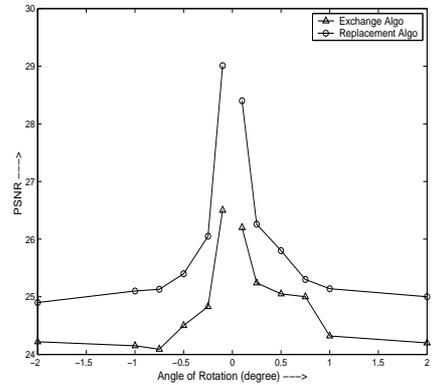


Fig. 8. PSNR(dB) measure with Rotation attack

From the results shown in fig. 1 to fig.8, we can conclude that, for all the attacks like blurring, JPEG compression, rotation, the replacement algorithm gives higher correlation coefficient, higher PSNR and lower distortion compared to the exchange algorithm. Thus the first one outperforms the later

IV. CONCLUSION

In this paper, we proposed a wavelet based blind watermarking technique. Watermark bit is embedded in the middle frequency band only. As a result, the watermarking technique is robust to attacks in both frequency and time domain. The scheme is more robust against localized distortions since it uses intra-block relations. Experimental results show that the

replacement algorithm performs better than the exchange algorithm. As compare to the scheme in [9], which also uses intra-block relations for watermarking, our scheme is a blind one and uses wavelet transform for watermarking. The other features of our scheme are, the watermark is perceptually invisible and it is robust against attacks like blurring, JPEG compression and rotation.

REFERENCES

- [1] Proceedings of the IEEE (Special Issue on Watermarking), vol. 87, July 1999.
- [2] Liu Yong Liang and Wen Gao, "General schemes for blind watermark," Proc. of IEEE Int. conf. on Robotics, Intell. systems and signal processing, vol. 2, pp. 1185-1190, Oct 2003.
- [3] S. Mallat, "A theory for multiresolution signal decomposition: The wavelet representation," IEEE Trans. Pattern Anal. Mach. Intell., vol. 11, pp. 2091-2210, Dec. 1990.
- [4] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoan, "Secure spread spectrum watermarking for multimedia," IEEE Trans. Image Processing, vol. 6, pp. 1673-1687, Dec. 1997.
- [5] C. S. Lu, S. K. Huang, C. J. Sze, and H. Y. Liao, "Cocktail watermarking for digital image protection," IEEE Trans. Multimedia, vol. 2, pp. 209-224, Dec. 2000.
- [6] J. R. Hernandez, M. Amado, and F. Perez-Gonzalez, "DCT-domain watermarking techniques for still images: detector performance analysis and a new structure," IEEE Trans. Image Processing, vol. 9, pp. 55-68, Jan. 2000.
- [7] Shih-Hao Wang and Yuan-Pei Lin, "Wavelet tree quantization for copyright protection watermarking," IEEE Trans. Image Processing, vol. 13, pp. 154-165, Feb. 2004.
- [8] C. Hsu and J. Wu., "Hidden signatures in image," IEEE Int. conf. on Image Proc., vol. 3, pp. 223-226, Sept. 1996.
- [9] F.Y.Duan, I.King, L.Xu, and L.W.Chan, "Intra-block algorithm for digital watermarking," IEEE 14th Int. Conf. on Pattern Recognition, volume II, pp. 1589-1591, Aug. 1998.
- [10] N.B.Nill, "A Visual Model Weighted Cosine Transform for Image Compression and Quality Assessment," IEEE Trans. on Comm., vol. 33, No. 6, pp. 551-557, 1985.
- [11] Wang, H.-J, and C.-C. J. Kuo, "Image Protection via Watermarking on Perceptually Significant Wavelet Coefficients", Proceedings of the IEEE Multimedia Signal Processing Workshop, pp. 279-284, Dec. 1998.