International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:1, No:7, 2007

A Novel Dual-Purpose Image Watermarking Technique

Maha Sharkas, Dahlia R. ElShafie, and Nadder Hamdy, Senior Member IEEE

***Abstract*—**Image watermarking has proven to be quite an efficient tool for the purpose of copyright protection and authentication over the last few years. In this paper, a novel image watermarking technique in the wavelet domain is suggested and tested. To achieve more security and robustness, the proposed techniques relies on using two nested watermarks that are embedded into the image to be watermarked. A primary watermark in form of a PN sequence is first embedded into an image (the secondary watermark) before being embedded into the host image. The technique is implemented using Daubechies mother wavelets where an arbitrary embedding factor α is introduced to improve the invisibility and robustness. The proposed technique has been applied on several gray scale images where a PSNR of about 60 dB was achieved.

***Keywords*—**Image watermarking, Multimedia Security, Wavelets, Image Processing.

I. INTRODUCTION

THE wide spread of multimedia data throughout the World Wide Web has created an urgent need to protect intellectual properties against theft, illegal duplication and/or manipulation. A watermark is in fact a copyright and authentication information in form of a digital image, sound,…etc. that is usually hidden in the work to be watermarked.

To watermark a digital image (host image), a signal, mostly an image too, is permanently embedded into it. The introduced watermark can be considered as an added noise that does not greatly affect the quality of the host image. To prove authenticity and/or ownership, it should be possible to extract the watermark by reversing the sequence of embedding. A watermarking technique is called a robust one if it can extract the watermark successfully even if the watermarked image has been subjected to malicious attacks. However, any attempt to remove the embedded watermark should result in destroying the watermarked image. On the other hand, a watermarking technique is fragile if the host image distorts and breaks due to any attack. Generally, the watermark is hidden in the host data in such a way that it is invisible and robust i.e. it can withstand many kinds of attacks while being detectable at a reasonable quality. Sometimes the watermark is required to be fragile, i.e. it breaks easily in response to any attack.

Moreover, digital watermarks besides providing proofs of authenticity; they can convey information about the ownership of the image and give the data a unique identity that can be used to track or control the image's distribution.

Recently, many watermarking algorithms have been proposed in the literature [1], [2]. Some of them operate either in the frequency domain using for example the DCT [3], [4], DFT [5] and DWT [6]-[10] or in the spatial domain [11]. Since some of the current image compression techniques are based on the wavelet domain, such as JPEG2000, DWT-based watermarking methods have been researched intensively.

The algorithm published in [12] performs two–level decomposition using the Haar wavelet filters. Pseudo Random Noise codes are only added to the large coefficients of the high and middle frequency bands of the DWT transformed image. Although the watermark was invisible, it proved to be fragile against low pass and median filtering. In [13], on the other hand, independent component analysis (ICA) is combined with DWT and DCT. The approximation of the DWT transformed host image is then DCT transformed where the watermark is added. The invisible watermark was easy to detect through ICA however it was not robust enough to survive high pass filtering.

II. THE SUGGESTED TECHNIQUE

An image watermarking algorithm that operates on the wavelet domain is suggested here. It features imperceptibility, high pay load, robustness as well as fragility. It is based on embedding two nested watermarks, rather than a single watermark. Such dual image watermarking technique, owing to its increased security level, can serve as a means for both copyright protection and authentication of intellectual properties.

A primary watermark, in form of a pseudo random (PN) sequence, is first embedded into an image, the cameraman image (secondary watermark), before being added to the host image (Lena image). They are both shown in Fig.1 and Fig.2 respectively.

The two images are first decomposed using a two level Discrete Wavelet Transform (DWT) employing the 'db4' mother wavelet. The obtained approximation and detail sub-bands of each image are depicted in Fig.3 and Fig.4 respectively.

The primary watermark is chosen to be a zero mean PN-sequence of length 1024 and is arranged in a two- dimensional matrix $w_p(i,j)$.

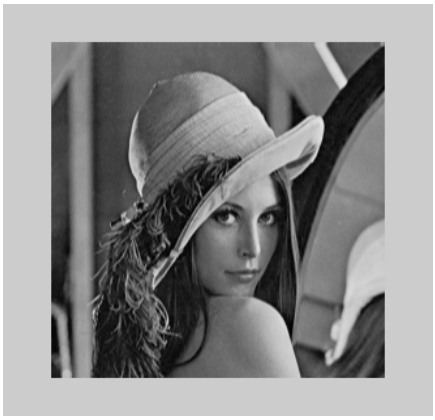


Fig. 1 Original Lena Image

Fig. 2 Original Cameraman

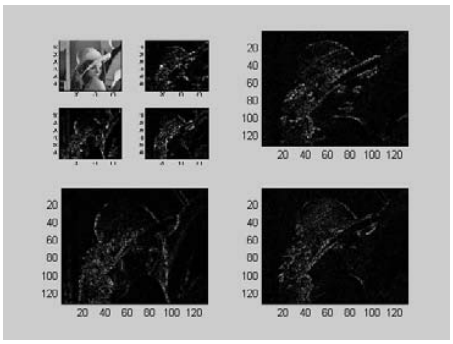


Fig. 3 Two-level wavelet decomposition of Lena image using 'db4'

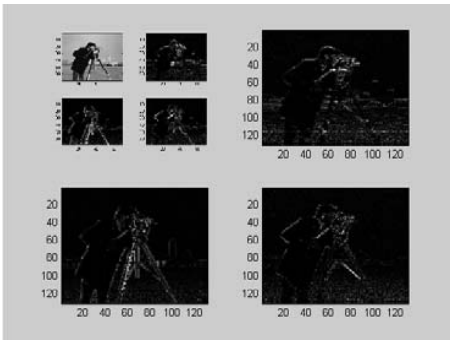


Fig. 4 Two-level wavelet decomposition

III. The Embedding Algorithm

The first stage of the watermark embedding procedure involves adding the generated primary watermark, the PN-Sequence, to the 2nd level DWT horizontal coefficients (LH_2) of the decomposed secondary watermark, the Cameraman image using 'db4', according to the following equation:

$$w^*_s(i,j)^{LH2} = w_s(i,j)^{LH2} + \alpha_o \cdot w_p(i,j) \quad (1)$$

In which $w_p(i,j)$ is the primary watermark, while $w_s(i,j)$ and $w^*_s(i,j)$ are the DWT coefficients of the secondary watermark and the watermarked secondary watermark respectively. The factor α_o is a weighing factor that is set to 1, in this case, for increased robustness against attacks while maintaining at the same time an acceptable level of imperceptibility. Apart from the 2nd level horizontal coefficients, the rest of the coefficients of $w^*_s(i,j)$ and $w_s(i,j)$ remain unchanged.

The watermarked Secondary watermark, shown in Fig.5, is obtained by performing an IDWT on the updated coefficients of $w^*_s(i,j)$.

Fig. 5 The watermarked secondary watermark using 'db4'

As a distortion metric, the PSNR is considered here to measure both the degree of the imperceptibility and the quality of the watermarked secondary watermark. It is estimated by first calculating the mean squared error MSE (the difference between the original image and the watermarked image) according to the following equation:

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \left(W(i,j) - W_{ex}(i,j) \right)^2 \quad (2)$$

from which the PSNR is calculated as follows:

$$PSNR = 10 \log \left(\frac{(\max(W(i,j)))^2}{MSE} \right) \quad (3)$$

Giving a PSNR for the watermarked cameraman image of 60.1092 dB.

The second step of the watermarking embedding procedure involves adding the approximation and the sub-bands of $w^*_s(i,j)$ to the horizontal, vertical and diagonal 2nd level DWT coefficients
$(I_1(i,j)^{LH2}, I_1(i,j)^{HL2}, I_1(i,j)^{HH2})$ of the original Lena image to obtain the dual watermarked Lena image I'(i,j) according to the following equations:

$$I'(i,j)^{LH2} = I_1(i,j)^{LH2} + \alpha . w^*_s(i=[1:\frac{M}{3}],\ j=[1:\frac{N}{3}]) \quad (4)$$

$$I'(i,j)^{HL2} = I_1(i,j)^{HL2} + \alpha . w_s(i=[\frac{M}{3}+1:\frac{2M}{3}], j=[\frac{N}{3}+1:\frac{2N}{3}]) \quad (5)$$

$$I'(i,j)^{HH2} = I_1(i,j)^{HH2} + \alpha \cdot w^*_s(i=[\frac{2M}{3}+1:M],\ j=[\frac{2N}{3}+1:N]) \quad (6)$$

in which α, as before, is a scaling factor that is introduced to guarantee invisibility of the watermark. It is set here to 0.005 in order to maintain an acceptable PSNR, reasonable imperceptibility as well as an acceptable degree of robustness.

Finally, applying an IDWT to the updated coefficients of I'(i,j), the Dual Watermarked Lena Image is obtained as shown in Fig. 6.

To evaluate the quality of the image, the PSNR was calculated and was found to be 58.2919dB.

Fig. 6 The dual watermarked Lena image using 'db4'

IV. Watermark Detection

In order to prove ownership of a gray-level image such as Lena image, the primary watermark (the PN-Sequence) should be detected. Anyone who just succeeds in extracting the secondary watermark, here the Cameraman image, can not claim ownership unless he extracts the primary watermark, namely, the embedded PN sequence.

To extract the secondary watermark, both the original and the watermarked Lena images undergo two level DWT decomposition. Knowing α, the DWT coefficients of the secondary watermark $w_s'^{*}(i,j)$ are extracted according to the following equations:

$$w'^{*}_{s}(i=[1:\frac{M}{3}],j=[1:\frac{N}{3}]) = \frac{I'(i,j)^{LH2} - I_1(i,j)^{LH@}}{\alpha} \quad (7)$$

$$w'^{*}_{s}(i=[\frac{M}{3}+1:\frac{2M}{3}],\ j=[\frac{N}{3}+1:\frac{2N}{3}]) = \frac{I'(i,j)^{HL2} - I_1(i,j)^{HL2}}{\alpha} \quad (8)$$

$$w'^{*}_{s}(i=[\frac{2M}{3}+1:M],j=[\frac{2N}{3}+1:N]) = \frac{I'(i,j)^{HH2} - I_1(i,j)^{HH2}}{\alpha} \quad (9)$$

Applying the IDWT to the resulting coefficients, the watermarked cameraman image, shown in Fig. 7, can be extracted. The measured PSNR was 11.1527 dB which reflects very low level of imperceptibility and noticeable distortion as can be seen in Fig. 7.

Fig. 7 Extracted watermarked cameraman

The primary watermark w_p is then extracted by subtracting the second level horizontal DWT coefficients of the original cameraman image from their corresponding coefficients in the watermarked cameraman. The resulting sequence is then correlated with the other 25 generated PN sequences of the same length. A distinguished peak should be pronounced at the specific sequence used as a watermark, here sequence number 10 out of 25 sequences as depicted in Fig. 8.

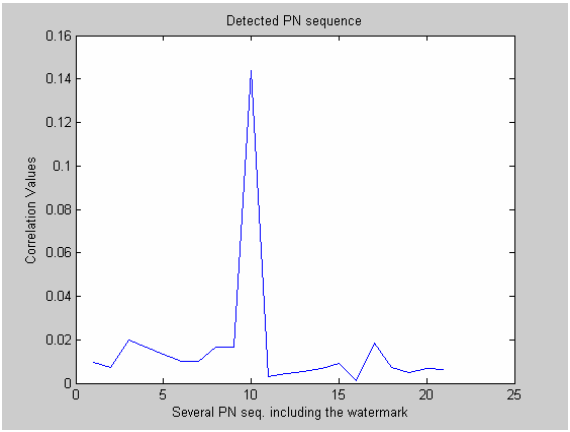


Fig. 8 Detection of the primary watermark

Although the secondary watermark seems to be severely distorted, the suggested technique succeeds in detecting the primary watermark.

V. Using the Mother Wavelet 'db1'

Aiming at improving the obtainable PSNR of the extracted secondary watermark, the mother wavelet 'db1' has been tried to replace 'db4'.

In wavelet decomposition and reconstruction using 'db4', decimation/interpolation is done using fractional numbers, the fact that results in a respectful truncation error. Using 'db1', on the other hand, does greatly reduce such errors since it decimates/interpolates exactly by an integer, mostly 2.

Both the host (Lena) and the secondary watermark (cameraman) images are decomposed into a 2-level DWT using 'db1'. The primary watermark (again a PN sequence of length 1024) is then added to the horizontal coefficients of the 2nd level DWT of the secondary watermark. The watermarked cameraman can then be obtained, as before, by taking the IDWT of the updated DWT coefficients.

The second step is embedding the DWT coefficients of the cameraman into the DWT coefficients of the host (Lena) image in exactly the same way as was done using 'db4'. The obtained watermarked Lena image was found to have a PSNR of 57.9938dB which is very close to that obtained when using 'db4'.

The advantage of using the mother wavelet 'db1' is evident in the process of watermark detection.

The extracted cameraman image, shown in Fig. 9, has a PSNR of 18.0962 dB which is better than that obtained using 'db4'. Moreover, the primary watermark when detected by correlating the extracted coefficients from the secondary watermark, as mentioned before, with other PN sequences having the same length showed a better peak as depicted in Fig.10.

Fig. 9 The extracted secondary watermark using 'db1'

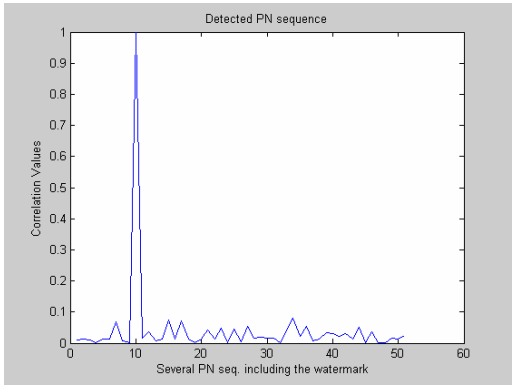
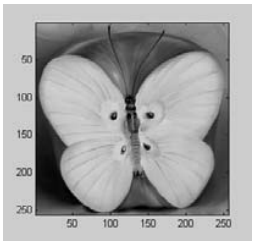


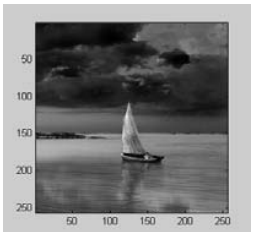
Fig. 10 Detecting the primary watermark ('db1')

Applying the same algorithm, using 'db1', on several test images, the algorithm succeeds in extracting the secondary watermark and detecting the primary one as previously shown in case of the Lena image yet at a slightly different PSNR as shown in Fig. 11.

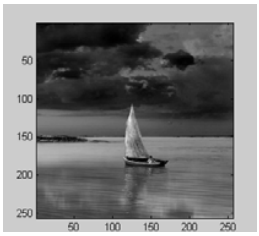
Any attack that aims at removing the embedded watermark by modifying the pixel values of the watermarked image; should make it difficult to detect the presence of the watermark. There is no such system that will remain robust against all kind of attacks. Every watermarking technique is robust within certain limits and boundaries.



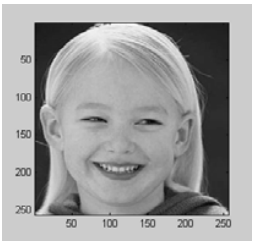
PSNR=57.6890



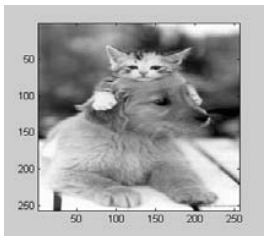
PSNR=58.2883



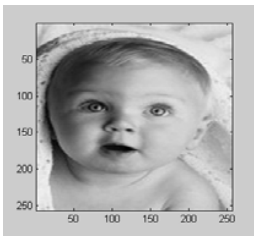
PSNR=58.5028



PSNR=58.5380



PSNR=58.7121



PSNR=58.8149

Fig. 11 Different test images with their PSNR

VI. Testing the Algorithm

To check the efficiency of the suggested dual watermarking algorithm, the Lena image was dual watermarked then subjected to several attacks such as: Bidirectional change in the luminance, low pass filtering at different cut off frequencies ω_c, JPEG compression and multi-threshold wavelet compression (MTWC).

The results, summarized in Table I, demonstrate that the proposed algorithm combines both fragility and robustness at the same time. In particular, the results indicates that when a watermarked image is altered through any attack, the secondary watermark which is a fragile watermark breaks very easily and its PSNR falls below the value to be expected under no attack, equal to 18.0962 dB. This change in the value of the PSNR could be used as a mean of authenticity indicating whether an image under suspicion is an original one or not. On the other hand, the detection of the primary watermark which is the robust watermark could be used for copyright protection in order to prove ownership of images.

VII. Conclusion

A novel dual image watermarking technique combining both robustness and fragility is suggested and tested. The technique succeeded in surviving several attacks where it was possible to detect the primary watermark in most cases even if the secondary watermark is severely distorted. Moreover, The Daubechies mother wavelet 'db1' was found to outperform the 'db4' mother wavelet concerning the PSNR of the extracted secondary watermark. In addition, the correlation result for detecting the primary watermark showed a more pronounced peak while the PSNR of the watermarked image remains almost the same.

TABLE I
Results Due to Different Kinds of Attacks on the Watermarked Image

Type of Attack	PSNR of the Watermarked Host Image	PSNR of Extracted Secondary Watermark	Detected Primary Watermark
+25 % Luminance	11.4661 dB	-65.5974 dB	YES
-5 % Luminance	24.1118 dB	-56.4952 dB	YES
JPEG Compression (Q=85)	39.3974 dB	-58.5164 dB	YES
MTW C (Threshold=2 ,1st level sub-bands)	47.7124 dB	-53.049 dB	YES
MTW C (Threshold=10, 1st level sub-bands)	40.3153 dB	-53.0419 dB	YES
MTW C (Threshold=2, all sub-bands)	47.2261 dB	-54.0609 dB	YES
MTW C (Threshold=10, all sub-bands	37.3014 dB	-65.6453 dB	NO
LPF, ω_c =0.9	39.4172 dB	-53.5948 dB	YES
LPF, ω_c =0.6	32.7925 dB	-68.2604 dB	YES
LPF, ω_c =0.5	30.9787 dB	-73.3259 dB	YES

References

[1] E.-H. Fu, "Literature survey on digital image watermarking," *Technical Report*, submitted to EE 381K Multidimensional Signal Processing.

[2] F. Hartung and M. Kutter, "Multimedia watermarking techniques," *Proc. IEEE*, Vol.87, no.7, pp 1079-1107, 1999.

[3] W. Chu, "DCT-Based image watermarking using subsampling." *IEEE Transactions on Multimedia*, pp. 34-38, Mar. 2003.

[4] M.-J. Tsai, H.-Y. Hung**,** **"**DCT and DWT-Based image watermarking by using subsampling," *Proceedings of the 24th International Conference on Distributed Computing Systems Workshops*, MNSA (ICDCSW'04), Hachioji, Tokyo, Japan, pp. 184-189, March 23 - 24, 2004.

[5] Xiangui Kang, Jiwu Huang, Yun. Q.Shi, and Yan Lin, "A DWT-DFT composite watermarking scheme robust to both affine transformation and JPEG compression." *IEEE transactions on Circuits and Systems for Video Technology*, Vol.13, no.8, August 2003.

[6] P. Meerwald, and A.Uhl, " A survey of Wavelet-Domain watermarking algorithms," in P.W. Wong and E.J. Delp, (eds.), *Proceedings of electronic Imaging 2001, Security and Watermarking of Multimedia Contents III*, San Jose, CA, January pp. 505-516,2001.

[7] H. Inoue, et al. "A digital watermark technique based on the Wavelet Transform and its robustness on image compression and transformation," *Proceedings of the 1998 IEEE International Conference on Image Processing(ICIP-98),* Vol.2, Chicago, pp. 391-395, October 1998.

[8] H.-J. Wang, P.-C. Su, and C.-C. J.Kuo, "Wavelet-based digital image watermarking," *Optics Express*, Vol.3, No.12,pp. 491-496, December 1998.

[9] D. Kundur, and D. Hatzinakos, "Digital watermarking using multiresolution Wavelet decomposition," *International Conference on Acoustics, Speech and Signal Processing (ICASSP),* Seattle, pp.2969-2972, May 1998.

[10] R. Safabakhsh, S. Zaboli, A. Tabibiazar, "Digital watermarking on still images using Wavelet transform," *Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04)*, Volume 1, April 05-07, 2004, Las Vegas, Nevada.

[11] W. Bender, D. Gruhl, and N. Morimoto, "Techniques for data hiding," *in Proceedings of the SPIE 2420, Storage and Retrieval for Image and Video Databases III*, pp. 164-173, 1995.

[12] X. Xia, C. Boncelet, and G. Arce, "A multiresolution watermark for digital images," *in Proc. IEEE Int. Conf. Image Processing 1997(ICIP'97)*, vol.1, Santa Barbara, CA, pp. 548-551, Oct. 1997.

[13] J. Liu, X. Zhang, J. Sun and M. A. Lagaunas, "A digital watermarking scheme based on ICA detection," *Proceedings of the 4th International Symposium on Independent Component Analysis and Blind Signal Separation(ICA2003)*, April 2003, Nara, Japan.

[14] E. T. Lin and E. J. Delp, "A review of fragile image watermarks," *Proceedings of the Multimedia and Security Workshop (ACM Multimedia '99) Multimedia Contents*, Orlando, FL, October, pp. 25-29, 1999.

[15] E. T. Lin, C. I. Podilchuk, and E. J. Delp, "Detection of image alterations using semi-fragile watermarks," *Proceedings of the SPIE International Conference on Security and Watermarking of Multimedia Contents II*, vol. 3971, San Jose, CA, January 23 - 28, 2000, pp. 152-163.