International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:1, No:5, 2007

A Dual Digital-Image Watermarking Technique

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

***Abstract*—**Image watermarking has become an important tool for intellectual property protection and authentication. In this paper a watermarking technique is suggested that incorporates two watermarks in a host image for improved protection and robustness. A watermark, in form of a PN sequence (will be called the secondary watermark), is embedded in the wavelet domain of a primary watermark before being embedded in the host image. The technique has been tested using Lena image as a host and the camera man as the primary watermark. The embedded PN sequence was detectable through correlation among other five sequences where a PSNR of 44.1065 dB was measured. Furthermore, to test the robustness of the technique, the watermarked image was exposed to four types of attacks, namely compression, low pass filtering, salt and pepper noise and luminance change. In all cases the secondary watermark was easy to detect even when the primary one is severely distorted.

***Keywords*—** DWT, Image watermarking, watermarking techniques, wavelets.

I. Introduction

THE large-scale communication of multimedia data has created a pressing need to protect digital information against illegal duplication and manipulation. Digital watermarking addresses the growing concerns of theft and tampering through the use of advanced signal processing strategies to embed copyright and authentication information within media content.

A digital image watermark is a signal permanently embedded into a digital image that can be detected or extracted later by means of some operations for authentication purposes. The hidden watermark should be inseparable from the *host* image, robust enough to resist any manipulations while preserving the image quality. Thus through watermarking, intellectual properties remains accessible while being permanently marked.

For any watermarking technique to be valid, it must satisfy three important requirements namely: perceptual invisibility, robustness against various image processing attacks, as well as security.

Maha Sharkas is a lecturer at the Arab Academy for Science and Technology, Alexandria, Egypt. (e-mail: msharkas@aast.edu).

Dahlia ElShafie is a teaching assistant & a M.Sc. student at the Arab Academy for Science and Technology, Alexandria, Egypt.(e-mail: dahlia@aast.edu).

Nadder Hamdy is a chairman of the Electronics and Communications Engineering Department and a professor at the Arab Academy for Science and Technology, Alexandria, Egypt. (e-mail:nhamdy@ieee.org).

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 Algorithm

The original gray-scale 256*256 image of Lena (host image) shown in Fig.4 and the resized 110*110 Camera man (primary watermark) image shown in Fig.2 are each decomposed into 2 resolution levels using Daubechies-4 filter as shown in Fig.1.

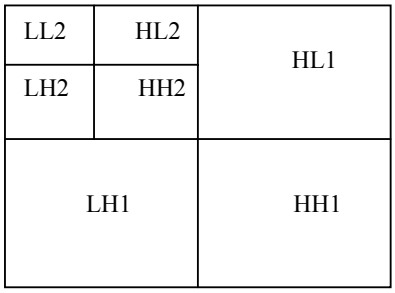

Fig.1 Decomposition into 2 resolution levels using DWT

A Pseudo Random Noise (PN) Sequence $w_2(i,j)$ (secondary watermark) having a length of 1024 bits and zero mean is generated and added to the horizontal coefficients (HL2) of the decomposed primary watermark image according to (1).

$$w_1(i,j) = I_2(i,j) + w_2(i,j) \quad \ldots\ldots\ldots \quad (1)$$

With $I_2(i,j)$ and $w_1(i,j)$ representing the DWT coefficients of

the primary watermark and the watermarked primary watermark respectively.

The resulting $w_1(i,j)$ coefficients are then added to the horizontal, vertical and diagonal DWT coefficients (HL2, LH2, HH2) of the original Lena image according to (2).

$$I'(i,j)=I_1(i,j)+\alpha .w_1(i,j) \quad \ldots\ldots\ldots\ldots\ldots \quad (2)$$

In which $I_1(i,j)$ is representing the DWT coefficients of the original Lena image, $I'(i,j)$ is the watermarked DWT coefficients of the original Lena image and α is a scaling factor that is usually used to adjust the invisibility of the watermark, here is set to 0.0001.

Finally, applying the IDWT to $w_1(i,j)$ and $I'(i,j)$ we can get the watermarked primary watermark image and the watermarked Lena image as shown in Fig. 3 and Fig. 5 respectively.

Fig.2 Primary Watermark

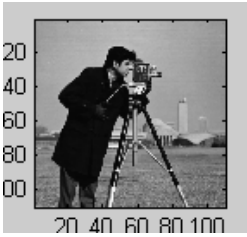

Fig.3 Watermarked Primary Watermark

Fig.4 Original Lena

Fig.5 watermarked Lena

III. THE DETECTING STRATEGY

To detect the PN Sequence, a 2 level DWT is applied to the watermarked Lena image to obtain $I'(i,j)$. Knowing the key α and the 2 levels DWT transformed original Lena image $I_1(i,j)$, the watermarked camera man DWT coefficients can be extracted using (3).

$$w_1(i,j)=\frac{I'(i,j)-I_1(i,j)}{\alpha} \quad (3)$$

Cross correlating the watermarked primary watermark and other generated watermark codes including, the embedded PN sequence in one of the watermark codes, $w_2(i,j)$ can be easily detected as shown in Fig. 6.

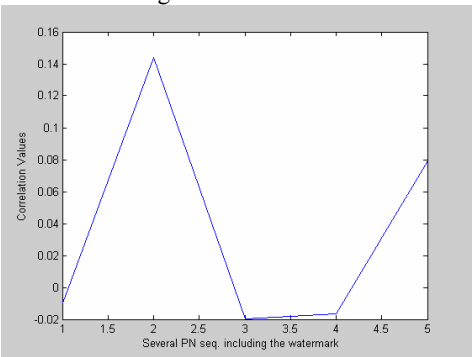

Fig.6 Detected Secondary Watermark

IV. EXPERIMENTAL RESULTS

To judge the performance of the proposed technique it has been extensively applied to various standard images and attempting different kind of attacks.

The secondary watermark was still detectable even when multi threshold DWT compression technique was applied on the watermarked Lena image, shown in Fig. 7. The corresponding correlation result is diagramed in Fig. 8.

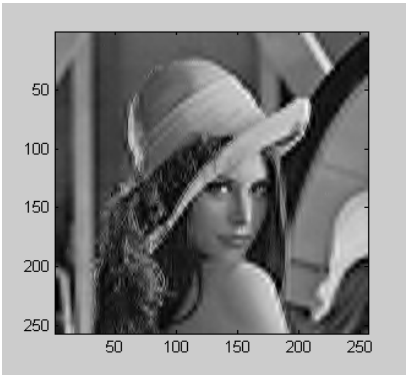

Fig.7 Compressed Watermarked Lena

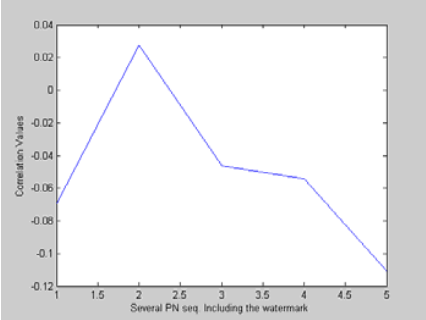

Fig.8 Detected Secondary Watermark

Furthermore, the secondary watermark was still detectable when the watermarked Lena image was subject to Low Pass Filtering, shown in Fig. 9 using a Kaiser FIR filter of length 71. The obtained correlation result is demonstrated in Fig. 10.

Fig.9 Low Pass Filtered Watermarked Lena

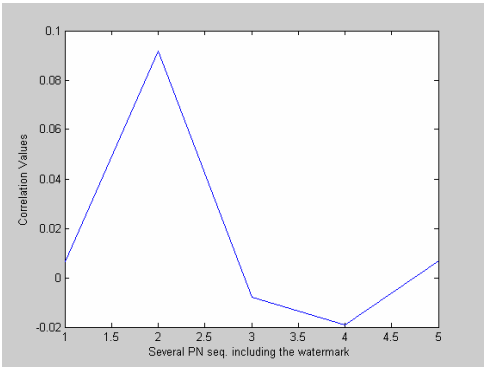

Fig.10 Detected Secondary Watermark

When the watermarked Lena image was attacked by a 5 % salt and pepper noise density as shown in Fig. 11 and which was filtered using a third order median filter as shown in Fig. 12, the secondary watermark was still detectable as illustrated in Fig. 13.

Fig.11 Watermarked Lena subjected to Salt and Pepper Noise

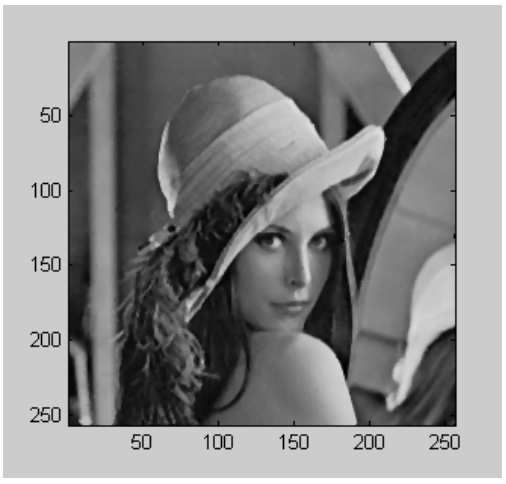

Fig. 12 Median Filtered Watermarked Noisy Lena

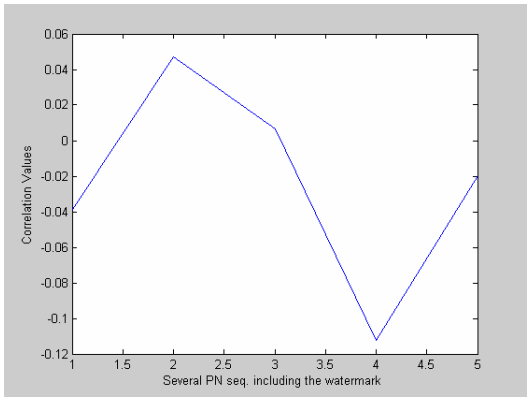

Fig.13 Detected Secondary Watermark

Finally, subjecting the watermarked Lena image to a 15 % bi- directional change in the luminance, as shown in Fig. 14 and Fig. 16, the secondary watermark was still detectable as demonstrated in Fig. 15 and Fig. 17.

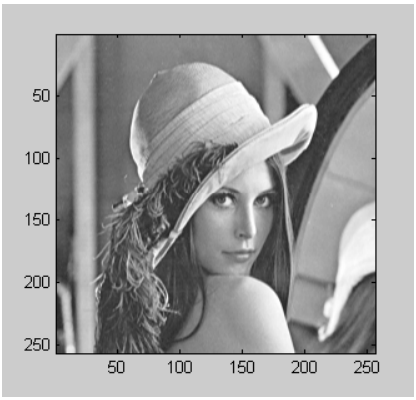

Fig. 14 Watermarked Lena after being subjected to an Increase in the Luminance

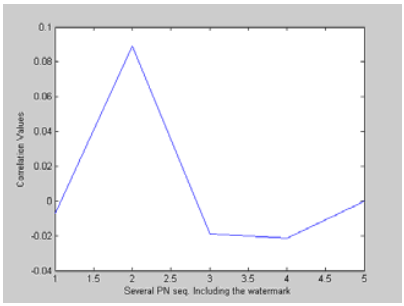

Fig. 15 Detected Secondary Watermark

Fig. 16 Watermarked Lena after being subjected to a Decrease in the Luminance

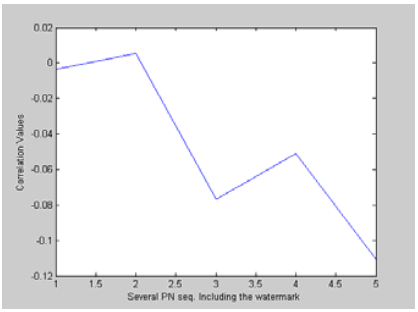

Fig.17 Detected Secondary Watermark

V. Conclusion

In this paper, a dual watermarking technique in the DWT domain is suggested and implemented using the MATLAB software. The measured performance of the technique proves its robustness against several kinds of attacks. Hence it can serve as a good means to prove the authenticity and ownership of intellectual properties and it can also detect any alteration or modification by any illicit user since the correlation peak that corresponds to the presence of the secondary watermark differs every time the watermarked picture is exposed to a different attack as illustrated in the experimental results.

References

[1] Er-Hsien Fu, "Literature Survey on Digital Image Watermarking". 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] Wai Chu, "DCT-Based Image Watermarking Using Subsampling." IEEE Transactions on Multimedia, Mar. 2003. pp. 34-38.

[4] Min-Jen Tsai, Hsiao-Ying Hung**,** "DCT and DWT-Based Image Watermarking by Using Subsampling" Proceedings of the 24th International Conference on Distributed Computing Systems Workshops, MNSA (ICDCSW'04), March 23 - 24, 2004, Hachioji, Tokyo, Japan, pp. 184-189.

[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 Sysytems for Video Technology, Vol.13, no.8, August 2003.

[6] Meerwald, P., 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 2001, pp. 505-516.

[7] Inoue, H., 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, October 1998,pp. 391-395.

[8] Wang, H.-J.M., P.-C.Su, and C.-C. J.Kuo, "Wavelet Based Digital Image Watermarking," Optics Express 491, Vol.3, No.12, December 1998.

[9] Kundur, D., and D. Hatzinakos, "Digital Watermarking Using Multiresolution Wavelet Decomposition," International conference on Acoustics, Speech and Signal Processing(ICASSP), Seattle, May 1998, pp.2969-2972.

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

[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, Oct. 1997, pp. 548-551.

[13] Ju Liu, Xiangang Zhang, Jiande Sun and Miguel Angel 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 1999, pp. 25-29.

[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.