ROBUST IMAGE WATERMARKING METHOD USING WAVELET TRANSFORM

Omar Adwan

Computer Information Systems Department, The University of Jordan, Amman – Jordan

ABSTRACT

In this paper a robust watermarking method operating in the wavelet domain for grayscale digital images is developed. The method first computes the differences between the watermark and the HH1 sub-band of the cover image values and then embed these differences in one of the frequency sub-bands. The results show that embedding the watermark in the LH1 sub-band gave the best results. The results were evaluated using the RMSE and the PSNR of both the original and the watermarked image. Although the watermark was recovered perfectly in the ideal case, the addition of Gaussian noise, or compression of the image using JPEG with quality less than 100 destroys the embedded watermark. Different experiments were carried out to test the performance of the proposed method and good results were obtained.

KEYWORDS

Watermarking, data hiding, wavelet transform, frequency domain

1. INTRODUCTION

Digital watermarking is a relatively new area, and the search is still attracting many researchers in the area. Over the past few years, digital watermarking has emerged as a leading research area to solve problems of ownership and content authentications for digital multimedia data including audio, image and video. [1].

Digital watermarking can be defined as the practice of hiding information called message or watermark into a digital content such as audio, images and video, in such a way that the embedded message should be imperceptible (difficult to notice) and robust against different manipulations that may attempt to remove or alter it [2-4]. For example, a message might be hidden within an image.

Watermarks serve mainly as tools for digital copyright protection and to prove the ownership of the original work. [5]. In addition, Digital watermarking may also be used for a wide range of applications, such as: Source tracking when different recipients get differently watermarked content, Broadcast monitoring, i.e. television programs contains watermarked video from television agencies, Video authentication, Software crippling on screen casting and video editing software programs, to encourage users to purchase the full version to remove it, ID card security, Fraud and Tamper detection, Content management on social networks, and others.

Watermarking methods can be broadly divided into two categories: spatial domain methods, which embed the data by directly manipulating the pixel values of the cover image, and frequency (transform) domain methods, which embed the data by modulating the frequency domain coefficients [7].

It has been reported that embedding data in the frequency domain of an image can be much more robust than embedding in the spatial domain (8-9].

Wavelets have become a key technique in different applications including compression (JPEG-2000) and image watermarking [1], The multiresolution aspect of wavelets is helpful in managing good distribution of the message in the cover in terms of robustness versus visibility. The wavelet transform decomposes an image into multilevel spatial-frequency decomposition. Figure 1 shows a one level decomposition. The main objective of wavelet transform is to define the powerful wavelet basis functions and find efficient methods for their computation. Fourier methods are not always good tools to recapture the signal or image, particularly if it is highly non–smooth [10].
A digital watermark is called robust with respect to transformations if the embedded information may be detected reliably from the marked signal, even if degraded by any number of transformations. Typical image degradations are JPEG compression, rotation, cropping, additive noise, and quantization. For video content, temporal modifications and MPEG compression often are added to this list. A digital watermark is called imperceptible if the watermarked content is perceptually equivalent to the original; unwater marked content [11]. In general, it is easy to create either robust watermarks or imperceptible watermarks, but the creation of both robust and imperceptible watermarks has proven to be quite challenging. Robust imperceptible watermarks have been proposed as a tool for the protection of digital content, for example as an embedded no-copy-allowed flag in professional video content [11], [12].

A digital watermark is called "fragile" if it fails to be detectable after the slightest modification. Fragile watermarks are commonly used for tamper detection (integrity proof). Modifications to an original work that clearly are notice-able commonly are not referred to as watermarks, but as generalized barcodes [12].

In this paper, I propose a robust image watermarking method based on Discrete Wavelet Transform (DWT). The method first computes the differences between the watermark and the HH1 sub-band values of the cover image, and then embeds these differences in one of the frequency sub-bands. Different frequency sub-bands have been tested to find which frequency sub-band can give best results.

Section 2 of this article introduces some of the previous work related to watermarking methods namely the spatial and the frequency based methods. Section 3 presents the basics of the Discrete Wavelet Transform DWT. Section 4 describes the proposed method for watermarking. Section 5 presents the experimental results, and finally section 6 concludes this article.

2. PREVIOUS WORK

Several methods have been proposed in literature based on both spatial and frequency domains. The most straight-forward method of watermark embedding in the spatial domain is the Least Significant Bit (LSB) substitution method, where the Most Significant Bit (MSB) of the watermark is substituted with the LSB of the cover object [9], [12]. The advantages of the LSB methods are that they are simple and can be easily applied to any image. However, any addition of noise can defeat the watermark [12].

Frequency (or transform) domain methods became more attractive and many methods have been proposed in literature based on the frequency domain. These methods are more robust than those based on spatial domain [3, 8]. Most of these methods are based on the Discrete Cosine Transform (DCT). A review of different DCT based methods can be found in [8].

Discrete Wavelet Transform (DWT) methods became more attractive in the last years. This is because DWT can divide the image into different sub-bands, where each sub-band has some different coefficients [13]. This gives more freedom to researchers to embed messages. Our algorithm is based on the DWT and it will be discussed in the next section. In [16] the authors describe a watermarking method using wavelet transform. The method embeds the wavelet coefficients of the watermark and the image into different resolution levels. The wavelet coefficients of the watermark are modulated using a human visual model constraint based on a measure called saliency before the embedding process.

In [17], the authors performed one decomposition level using DWT. The watermark is added to the HH1 sub-band. They then compare the difference between the resultant HH1 sub-band (with watermark added) with the HH1 sub-band of the original image by calculating their cross correlations. If there is a peak in the cross correlations, the watermark is considered detected, otherwise they consider the HL1 and the LH1 sub-bands. If the watermark is still not detected, a new level of the DWT is computed. This process is continued until the watermark is detected or the last level of the DWT is reached.

In [16], the authors develop a simple watermarking method operating in the frequency domain for grayscale digital images. The proposed method embeds the message in the LL1 sub-band produced by the Discrete Wavelet Transform (DWT) of the original image by using the Least Significant Bit (LSB) substitution method. Three cover images were used to test the performance of the proposed method. Different experiments were carried out to test the performance of the proposed method and the results show that little and unnoticeable degradation, while the watermark was recovered perfectly, which is considered an acceptable result.

Other methods based on wavelet transform have been proposed in [1, 17 - 18]. The evaluation of digital watermarking schemes may provide detailed information for a watermark designer or for end-users, therefore, different evaluation strategies exist [21]. Often used by a watermark designer is the evaluation of single properties to show, for example, an improvement. Mostly, end-users are not interested in detailed information. They want to know if a given digital watermarking algorithm may be used for their application scenario, and if so, which parameter sets seems to be the best.

3. DISCRETE WAVELET TRANSFORM

Discrete Wavelet Transform (DWT) methods became more attractive in the last years [17]. DWT provides multiresolution Analysis, where the image is analyzed at different frequencies with different resolutions. When an image is passed through series of low pass and high pass filters, DWT decomposes the image into a set of band limited components, called sub-bands [3]. The decomposition is performed so that the sub-bands can be reassembled to reconstruct the original image without error. Each decomposition level produces four non overlapping sub-bands [15-16]: LL1, HL1, LH1, and HH1 as shown in Figure 1, where the first letter corresponds to applying either a low pass (L) or high pass (H) filtering to the rows, and the second letter corresponds to applying either a low pass or high pass filtering to the columns of the image; the number after the two letters refers to the decomposition level. The LL1 sub-band represents the approximate image, which holds most of the information of the original image, while the other three sub-bands are the high frequency (detail) components of the original image.

LL1	HL1
LH1	HH1

Figure 1. One level image decomposition.

The LL1 band can be further decomposed for another level of decomposition and so on.

4. PROPOSED METHOD

The information to be embedded in a signal is called a digital watermark, although in some contexts the phrase digital watermark means the difference between the watermarked signal and the cover signal. The signal where the watermark is to be embedded is called the *host* signal. A watermarking system is usually divided into three distinct steps, embedding, attack, and detection. In embedding, an algorithm accepts the host and the data to be embedded, and produces a watermarked signal [20].

Our proposed method is based on the wavelet transform discussed above. The method starts by decomposing the image into its four sub-bands using the Daubechies DWT (db2). The method first computes the differences between the watermark and the HH1 sub-band values of the cover image, and then embeds these differences in one of the frequency sub-bands. Different frequency sub-bands has been tested to find which frequency sub-band can give best results.

The embedding steps are as follows:

1. Read the cover image.
2. Read the watermark, W.
3. Perform DWT to the cover image.
4. Find the differences between the watermark and the LH1 values.
5. Embed the watermark in the LH1 sub-band as follows:
   Diff = (LL1 – W)/k,where k is a constant (k = 5).
   LH1 = LH1 + Diff.
6. Apply inverse Discrete Wavelet Transform (IDWT) to obtain the watermarked image, WI.

The extracting steps are as follows:

1. Read the watermarked image (WI).
2. Perform DWT to WI
3. Extract the watermark, W as follows:
   W = (LH1 –LL1)*k.

The robustness of the watermark was improved by introducing a watermark constant k chosen experimentally (k = 5 in all of our experiments). I should note that larger value of k increases robustness at the expense of visual quality of the watermarked image.

5. EXPERIMENTAL RESULTS

In order to test the performance of our proposed method, the well-known Lena images are used as a cover image and the eye image is used as a watermark. Both images are shown in Figure 2.

Figure 2. (a) Lena (cover) image. (b) Eye (watermark) image.

Table 1 shows the Root Square Mean Square Error (RMSE) and the Peak Signal to Noise Ratio (PSNR) of both the original and the watermarked images when the HL1, LH1 and HH1 sub-bands are embedded. The Table shows that embedding the watermark in the LH1 sub-band gave best results. Therefore, the LH1 sub-band will be used for embedding the watermark in our experiments.

Table 1. RMSE and PSNR for different cover and watermarked images

Sub-band	RMSE	PSNR
HL1	1.71	43.4
LH1	1.53	44.4
HH1	1.60	44.1

Figure 3 shows in (a) the watermarked Lena image and in (b) the extracted watermark. The Figure shows that the watermarked image shows little no noticeable degradation, while the watermark was recovered perfectly.
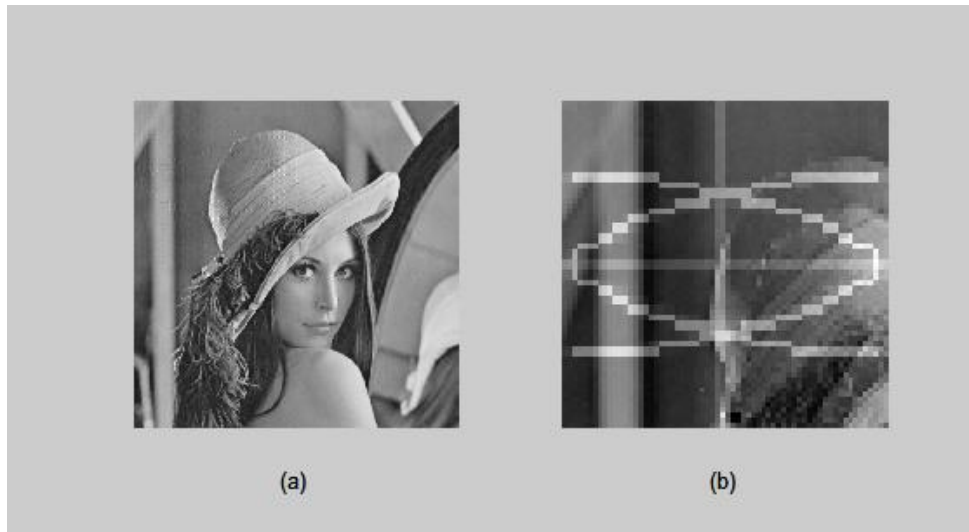
Figure 3. (a) The watermarked Lena image. (b) The extracted watermark.

Figure 4 below, shows the watermarked image when adding Gaussian noise. The figure shows that the watermark was recovered.
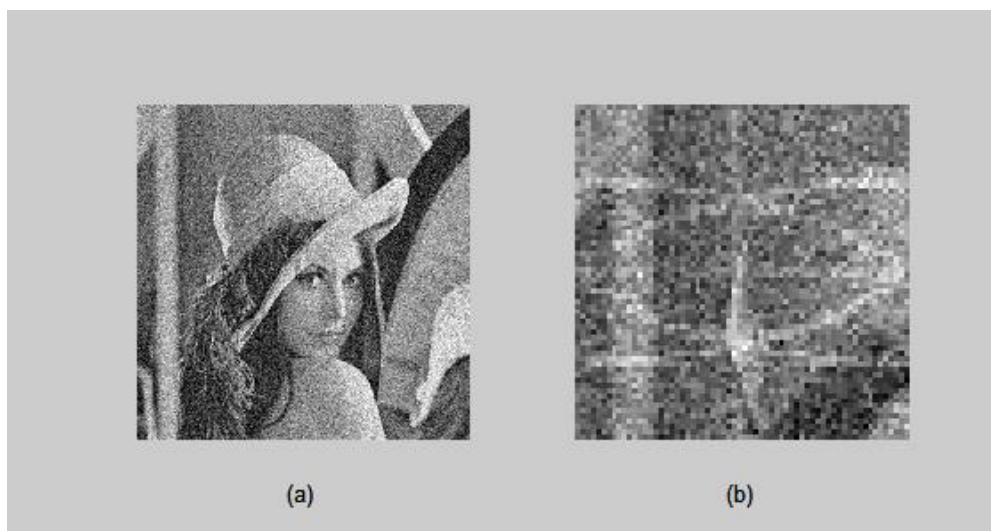

Figure 4. (a) The noised Lena image. (b) The extracted (noised) watermark.

Figure 5 shows the watermarked image when JPEG compression is applied, with quality = 50. The figure shows that the watermark was also recovered.

Figure 5. (a) The compressed Lena image. (b) The extracted (compressed) watermark.

Figure 6 show the watermarked image when rotated by 30 degrees is applied. The watermarked image is also cropped. The figure shows that the watermark was recovered.
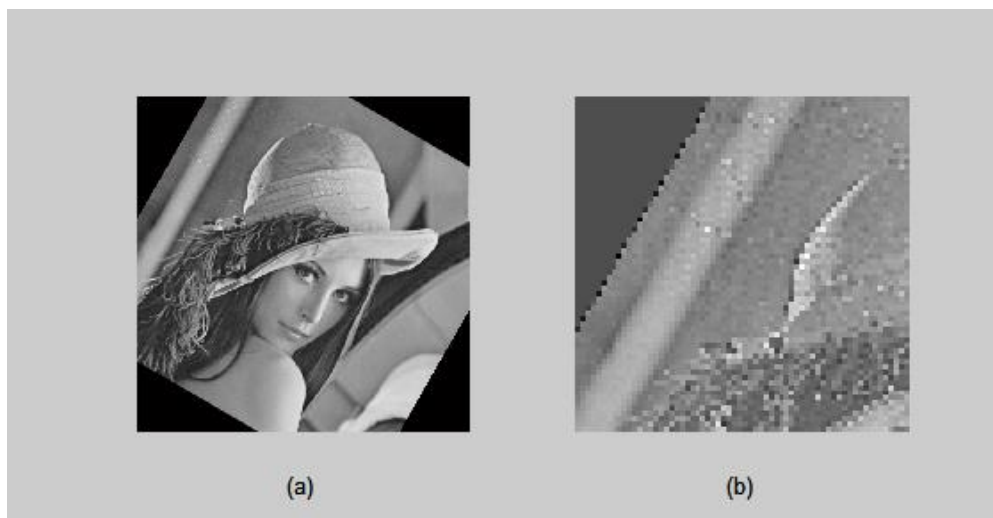

Figure 6. (a) The rotated and cropped Lena image. (b) The extracted (rotated and cropped) watermark.

The LL1 sub-band represents the approximate image can be fed again in the filter bank and the same process is repeated again which gives further sub images HH2, HL2, LH2 and LL2 .LL2 is the next approximation image and can be further compressed as shown in Figure 7. Applying muti-level decomposition as shown in figure 8 is left to future work.
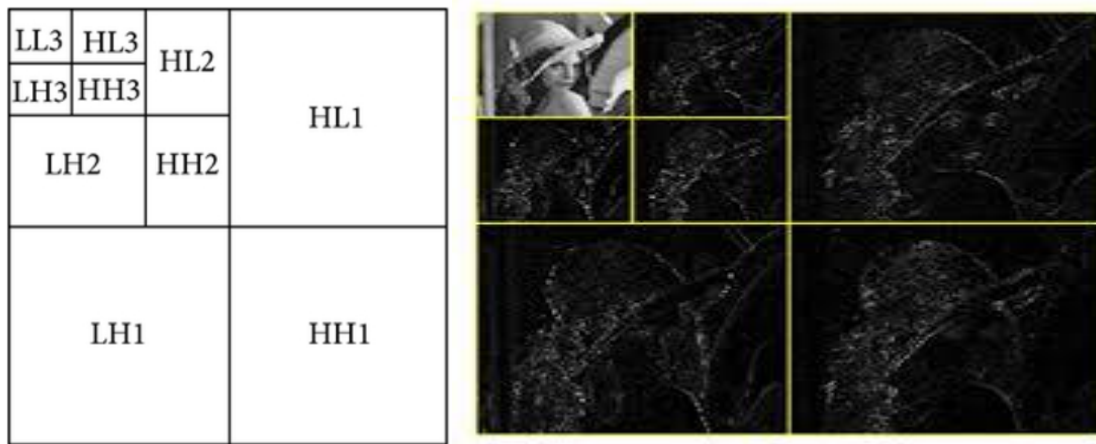
Figure 7. Multi-level decomposition.   Figure 8. Multi-level decompositions on Lena image

6. CONCLUSION

Watermarks serve as tools for digital copyright protection and to prove the ownership of the original work. In this paper we propose a simple method for image watermarking. The method applies both DWT and LSB techniques. The results show that embedding the watermark in the LH1 sub-band gave the best results. The results were evaluated using the RMSE and the PSNR of both the original and the watermarked image. Although the watermark was recovered perfectly in the ideal case, the addition of Gaussian noise, or compression of the image using JPEG with quality less than 100 destroys the embedded watermark.

The LL1 sub-band can be further fed the filter bank and the same process is repeated again which gives further sub images HH2, HL2, LH2 and LL2 .LL2 is the next approximation image and can be further compressed. Applying muti-level decomposition is left to future work.

REFERENCES

[1]   J. Dugelay and S. Roche, "A servey of current watermaking techniques", in S. Katzenbeisser and F. Petitcolas (eds), Information hiding techniques for steganography and digital watermarking, Artech House, USA, pp. 121-148, 2000.

[2]   I. Cox, M. Miller, J. Bloom, J. Fridrich and T. Kalker "Digital watermarking and steganography", Morgan Kaufman, 2008.

[3]   R. Gozalez, R. Woods, Digital Image Processing, 3rd ed., Prentice Hall, 2008..

[4]   M. Kutter and F. Hartung, "Introduction to Watermarking Techniques", in S. Katzenbeisser and F. Petitcolas (eds), Information hiding techniques for steganography and digital watermarking, Artech House, USA, pp. 97-120, 2000.

[5]   S. Lai and F. Buonaiuti, "Copyright on the internet and watermarking", in S. Katzenbeisser and F. Petitcolas (eds), Information hiding techniques for steganography and digital watermarking, Artech House, USA, pp. 191-213, 2000.

[6]   I. Cox, M.L. Miller, J.M.G. Linnartz, T. Kalker, "A Review of Watermarking Principles and Practices" in Digital Signal Processing for Multimedia Systems, K.K. Parhi, T. Nishitani, eds., New York, New York, Marcel Dekker, Inc., 1999, pp. 461-482.

[7]   U. Qidwai and C. Chen, Digital image processing: An algorithmic approach with Matlab, CRC Press, 2010.

[8]   Cox, M. Miller, J. Kilian, F. Leighton and T. Shamoon, "Secure spread spectrum watermarking for multimedia", IEEE Transactions on Image Processing, Vol. 6, No. 12, pp. 1673-1687, 1997.

[9]   N. Johnson and S. Katzenbeisser, "A survey of steganographic techniques," in S. Katzenbeisser and F. Petitcolas (eds), Information hiding techniques for steganography and digital watermarking, Artech House, USA, pp. 43-78, 2000.

[10]   A.H.M. Jaffar Iqbal Barbhuiya1 , K. Hemachandran (2013), "Wavelet Tranformations & Its Major Applications In Digital Image Processing", International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 3, March - 2013 ISSN: 2278-0181

[11]   Khan, Asifullah; Mirza, Anwar M. (October 2007). "Genetic perceptual shaping: Utilizing cover image and conceivable attack information during watermark embedding". Information Fusion. 8 (4): 354-365. doi:10.1016/j.inffus.2005.09.007.

[12]   C. Shoemaker, Hidden Bits: "A Survey of Techniques for Digital Watermarking", http://www.vu.union.edu/~shoemakc/watermarking/, 2002. Last access: June, 2012.

[13]   M. Weeks, "Digital signal processing using Matlab and Wavelets, 2nd ed.", Jones and Bartlett publisher, 2011.

[14]   D. Kundur and D. Hatzinakos, "A robust digital watermarking method using wavelet-based fusion", in Proceeding of the International conference on image processing, Santa Barbara, pp. 544-547, 1997.

[15]   X. Xia, C. Boncelet and G. Arce, "Wavelet transform based watermark for digital images", Optics Express, Vol. 3, No. 12, pp. 497-511, 1998.

[16]   O. Adwan, et al., "Simple Image Watermarking Method using Wavelet Transform", Journal of Basic and Applied Science, Vol. 8, No. 17, pp. 98-101, 2014.

[17]   B. Gunjal and S. Mali, "Secured color image watermarking technique in DWT-DCT domain", International journal of computer science, engineering and information technology, Vol. 1, No. 3, pp. 36-44, 2011.

[18]   P. Reddy, M. Prasad and D. Rao, "Robust digital watermarking of images using wavelets", International journal of computer and electrical engineering, Vol. 1, No. 2, pp. 111-116, 2011.

[19]   G. Langelaar, I. Setyawan, R.L. Lagendijk, "Watermarking Digital Image and Video Data", in IEEE Signal Processing Magazine, Vol. 17, pp. 20-43, 2000.

[20]   Tanya Koohpayeh Araghi, Azizah B T Abdul Manaf (2017), "Evaluation of Digital Image Watermarking Techniques", International Conference of Reliable Information and Communication Technology, IRICT 2017: Recent Trends in Information and Communication Technology pp 361-368.

[21]   A.S.Kapse1, Sharayu Belokar2, Yogita Gorde3, Radha Rane4, Shrutika Yewtkar, (2018) "Digital Image Security Using Digital Watermarking". International Research Journal of Engineering and Technology (IRJET), Volume: 05 Issue: 03 | Mar-2018.

AUTHORS

Omar Adwan is an Associate Professor in the Department of Computer Information System at the University of Jordan, where he has been since 2010. From 2012 to 2016 he served as Department Chair. He received a B.S. in Computer Science from Eastern Michigan University in 1987. Dr Adwan received his M.S. and Ph.D. in Computer Science majoring in Software Engineering from The George Washington University. Currently Dr. Adwan is the Deputy Dean of Student Affairs at the University of Jordan. Dr Adwan research interests are in Image Processing, software engineering, with focus on software testing, software analytics, software security, intelligent software engineering, and both data mining and machine learning.