Two Levels Block Based Wavelet Watermarking Algorithm for Still Colour Images

Taha Jassim School of Engineering, University of Bradford, UK tahadawod @hotmail.com Hussain Al-Ahmad ECE Department, Khalifa University of Science, Technology and Research, UAE alahmad@kustar.ac.ae Raed Abd-Alhameed School of Engineering, University of Bradford, UK <u>r.a.a.abd@bradford.ac.uk</u> Ahmed Al-Gindy School of Engineering and Information Technology, Computer College, UAE agindy @hotmail.com

A robust watermarking technique is implemented for copyright protection. The proposed method is based on 2-level discrete wavelet transform (DWT). The embedded watermarking information is a mobile phone number including the international code. The first level of the DWT transformation is applied on 16×16 blocks of the host image. All the coefficients of the 8×8 low-low (LL1) first level sub-band are grouped into one matrix. The second level of the DWT is then applied to the grouped matrix from the first level transformation. The highest coefficient from the LL2 sub-band (4×4) is used for embedding the watermark information. The extracting process is blind since it does not require the original image at the receiver side. The distortion in the host image due to the watermarking process is minimal and the PSNR is greater than 60 dB. The proposed algorithm showed robustness against several attacks such as scaling, filtering, cropping, additive noise and JPEG compression.

Image processing. DWT. Watermarking.

1. INTRODUCTION

Digital media can be copied easily and therefore there is a need for protecting the copyright. One of the most important methods which deal with the protection of copyrights for the digital images is the use of the digital watermarking. Digital watermarking embeds secret information such as; logos, images, text, ..etc into the digital media by The spatial domain or the certain algorithms. frequency domain can be used for the embedding process and each one has their own pros and cons and is used in different scenarios (Singh 2013). In general, the frequency domain techniques are more robust than spatial domain ones (Manoharan 2010). The common transforms in frequency domain are: Wavelet Transform (DWT), Discrete Fourier Transform (DFT) and Discrete Cosine Transform (DCT). DWT has been used in watermarking due to the excellent spatial localization and multiresolution characteristics of the DWT (Kashyap 2012).

Many researchers have used the DWT. For example the author in (Xia 1997) has used the DWT in his proposed watermarking scheme. The middle and high frequency bands of the host image have been used for embedding the watermark information. The watermarking information was modelled as Gaussian noise. The drawback of this algorithm is the need for the original image during the extraction process. Another algorithm used 1level DWT for a robust image watermarking (Danavli 2009). Alpha technique blendina technique has been used as an embedding technique. However, the embedding and the extraction process are relying on the value of alpha (Shing 2011). The authors in (Bhatnagar 2008) proposed a semi-blind watermarking scheme by using the DWT. A grey scale logo image is used as the watermarking information. The host image is transformed into the wavelet domain and the directive contrast with wavelet coefficients have been used for embedding the watermark information. The singular values of the watermark information are embedded by modifying the singular values of the host image. The author in (Barni 2001) used pixel wise masking for watermarking in a wavelet-based algorithm. The adaptive watermark information is added to the largest detail bands. The product of data extracted from the HVS model is represented by the watermarking weighing function. The extraction

process of the watermarking information at the receiver side can be found by correlation. The proposed method showed robustness against several attacks. However, this method is more complex than other transform techniques (Barni 2001). The authors in (Lee 2007) applied a wavelet-based transform and discrete Hadamard transform (DHT) respectively. The proposed cascaded algorithms allowed them to choose the suitable coefficients that are close to the middle and low frequencies. However, the host image is required to recover the watermarking information at the receiver side.

In the previous techniques, the watermarking information used digital signature, images, logos and pseudo random numbers. However, the watermarking information that is used in our algorithm is the mobile number with the international code. It is a unique number all over the world (Lee 2007). Peak signal to noise ratio (PSNR) and the structured similarity index (SSIM) will be used to evaluate the distortion caused to the host image by the watermarking process (Al Gindy 2009).

In this paper, a robust two level wavelet watermarking technique is presented. The proposed method uses different block-based dimensions before embedding the watermark information. This paper is divided into 4 sections. Section II deals with the watermark embedding and extraction algorithms. The experimental results are given in section III, followed by the conclusions in section IV.

2. THE PROPOSED WATERMARKING ALGORITHM

The proposed algorithm uses two level DWT block based process to embed the watermarking information. The first level wavelet transformation is applied on the (16×16) blocks of the original image. Each block is divided into four groups of coefficients; LL1 (low-low frequencies), LH1 (lowhigh frequency), HL1 (high-low frequencies) and HH1 (high-high frequencies). The second level of DWT is applied on the LL1 part of each block. Accordingly, the LL2 are selected to embed the watermark information. The highest coefficient in the LL2 is used to embed one bit from the watermarking information. The watermark is embedded multiple times using a shuffling process applied to the host image (Khatkale 2012).

2.1 The Embedding Algorithm

The colour image is separated into three components R, G and B. In this algorithm, the green component (G) has been chosen for the embedding process (Al Gindy 2008) The mobile

phone number with the international code (14 decimal digits) is used as watermarking information. The sum of the 14 digits (2 extra decimal digits) is added to make it 16 decimal digits. These two digits will be used as checksum error detection at the receiver side. In order to embed the watermarking information, the 16 decimal numbers are converted to 64 BCD bits. The watermarking information is scrambled by using a secret key. The scramble process is important to reduce the correlation between the host image and the embedded watermark.

The host image is divided into 16×16 blocks in the spatial domain. The first level of DWT is then applied to convert each block to DWT domain. Following this, the second level of DWT is applied on each LL1 (8×8) blocks. The LL2 sub block is used for embedding process. The highest weight coefficient from each block of the LL2 is used to embed one bit for the watermarking information. The embedding process will be repeated several times because the size of the host image is much bigger than the 64 bits watermark. A shuffling process will be used to increase the robustness of the algorithm against the vertical cropping attack (Al Gindy).

Assume that f(i,j) represents the pixel of the Green component of the RGB representation of the colour host image, w(i, j) represents the binary pixel of the watermark.

$$F_k(u,v) = DWT\{f_k(i,j)\},\$$

If w(i,j)=1 then

$$F_{k}(x, y) = \begin{cases} \Delta Q_{e}(\frac{F_{k}(x, y)}{\Delta}) & x, y \in H_{k} \quad 1 \le k \le N_{HB} \\ F_{k}(x, y) & x, y \notin H_{k} \quad 1 \le k \le N_{HB} \end{cases}$$

If w(i,j)=0 then (1)

$$F_{k}(x, y) = \begin{cases} \Delta Q_{o}(\frac{F_{k}(x, y)}{\Delta}) & x, y \in H_{k} \quad 1 \le k \le N_{HB} \\ F_{k}(x, y) & x, y \notin H_{k} \quad 1 \le k \le N_{HB} \end{cases}$$

Where Qe is the quantization to the nearest even number and Qo is the quantization to the nearest odd number. Δ is a scaling quantity (watermarking strength) and it is also the quantization step used to quantize to either even or odd number. The 4×4 LL2 block is converted back to the first level by using the inverse DWT. The result from the first inverse is the LL1 (8 ×8) block from the 16×16 original block. Then 16×16 original block is converted to the spatial domain by using inverse DWT again and the process is repeated with the other blocks. The watermarked G component is added to the R and B components, to produce the watermarked colour image. Figure 1 illustrates the embedding process.

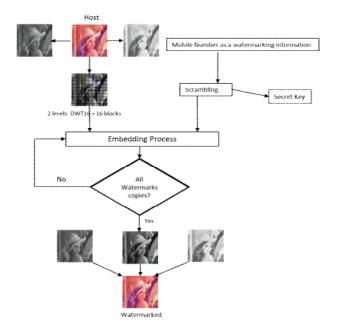


Figure 1: Graphical representation for Embedding Process.

2.2 The Extraction Algorithm

At the receiver side, the watermarked colour image is separated into RGB components. The G component is divided into16×16 blocks. The DWT transformation is applied in each block to get the first level of the DWT. Then the DWT level two is applied on each LL1 (8 \times 8) block. The watermarking information recovery is the inverse of the embedding process. Each predefined frequency coefficient is quantized by Δ and rounded to the nearest integer. The formula which is used for extracting the embedded bits is defined as follows:

If
$$Q(\frac{F_k(x, y)}{\Delta})$$
 is odd then $w(i,j)=0$
If $Q(\frac{F_k(x, y)}{\Delta})$ is even then $w(i,j)=1$ (2)

Where, Q is rounded to the nearest integer. Δ is the same as that used in the embedding process. The watermark can be retrieved by using the same secret key. The extraction process is shown in Figure 2.

The above method is used to extract one bit of the embedded watermarking from each coefficient of the watermarked image. The embedded watermarks information w(i,j) are created from the extracted bits. The reverse shuffling process is applied to achieve the original watermarking bits order. The obtained watermark is descrambled to get the correct one by using the same secret key I. Checksum error detection process is used at the extraction process to discover the wrong extracted watermarks and discard them before applying the averaging process. The averaging process is important to enhance the quality of the extracted watermarks.

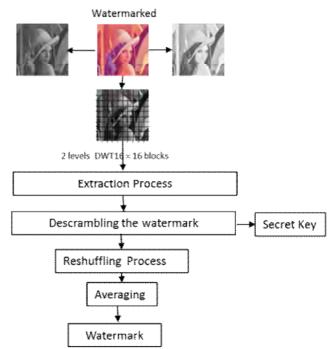


Figure 2: Graphical representation for Extraction *Process.*

3. SIMULATION AND RESULTS

Different colour images of size 512×512 with 24 bits per pixel have been used to examine the proposed algorithm. The watermarking information in the proposed algorithm is the mobile number with the international code. In order to evaluate the distortion caused to the host image by the watermarking process, two well known techniques are being used. The first one is the PSNR between the host image and the watermarked image. The perceptual invisibility of the proposed algorithm at different embedding strengths is shown in Table I. The second technique is the SSIM between the host image and the watermarked image. When the highest value of the SSIM is equal to one, it means that the watermarked image becomes the same as the host image. Table 1 illustrates the similarity difference between the host image and the watermarked image which is assessed by SSIM at different embedding strength.

Colour images such as "Lena", "Pepper" and "Baboon" have been used to test the perceptual quality at different embedding strengths as shown in Table 1. The PSNR achieved for different images are higher than 49 dB. The SSIM is also higher

than 0.99. Figure 3 shows the images using different strengths. It is clear that the distortion caused to the images is invisible even with high values of Δ .

The robustness of the proposed algorithm has been examined by applying several attacks. Stirmark software package was used for this purpose. The normalized correlation (NC) is used to measure the similarity between the original and the extracted watermark as shown in Table 2. The algorithm survived 3x3 and 5x5 low-pass filtering, cropping up to 75% horizontally and vertically, high JPEG compression, Gaussian, salt and pepper noise. Figure 4, shows some attacks on watermarked image.

Table 1: PSNR and SSIM at Different Embedding
Strength.

Image	Lena	Pepper	Baboon
PSNR at $\Delta = 8$	63.0502	63.0612	63.25698
PSNR at $\Delta = 14$	58.8864	59.0664	58.86391
PSNR at $\Delta = 16$	57.71243	57.5872	57.4448
PSNR at $\Delta = 20$	55.73828	55.6462	55.6975
PSNR at $\Delta = 24$	54.0071	54.05791	53.7889
PSNR at $\Delta = 30$	52.1089	52.26684	52.3058
PSNR at $\Delta = 34$	51.1137	50.95428	51.1093
PSNR at $\Delta = 40$	49.7376	49.7313	49.7601
SSIM at $\Delta = 8$	0.9998	0.9997	0.99995
SSIM at $\Delta = 14$	0.9995	0.9994	0.99987
SSIM at $\Delta = 16$	0.99945	0.9992	0.99982
SSIM at $\Delta = 20$	0.99914	0.9988	0.99976
SSIM at $\Delta = 24$	0.99866	0.9984	0.99960
SSIM at $\Delta = 30$	0.99809	0.9978	0.99944
SSIM at $\Delta = 34$	0.99756	0.9972	0.99931
SSIM at $\Delta = 40$	0.9966	0.99642	0.99905

Table 2: Normalized correlation (NC) for Lena image with different attacks at Δ = 20.

Attacks	NC	Attacks	NC
Cropping 80% V	1	Low pass 3×3	1
Cropping 50% V	1	Low pass 5×5	1
Cropping 75% H	1	Wiener 3×3	1
Cropping 50% H	1	Wiener 5×5	1
Scale 2	1	Median 3×3	1
Scale 0.4	1	Median 5×5	1
Gaussian noise m=0, v=0.002	1	JPEG 75	1
Gaussian noise m=0, v=0.001	1	JPEG 50	1
S&P noise, d=0.02+ Median 3×3	1	JPEG 35	1
S&P noise, d=0.05+ Median 3×3	1	JPEG 30	1
JPEG 28	1	JPEG 25	0



Host Image



Watermarked image at $\Delta = 24$ Watermarked image at $\Delta = 34$

Figure 3: Original Lena with different watermark strength (green channel).

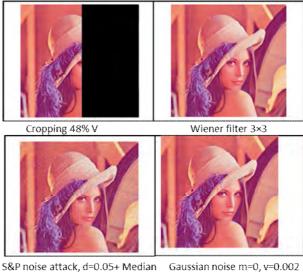


Figure 4: Several attacks for colour watermarked image

4. CONCLUSIONS

A block based blind watermark algorithm for colour image has been presented. Two levels of DWT have been applied on the colour host images. The highest magnitude coefficient from the LL2 has been used for the embedding process to increase the robustness of the algorithm. The proposed algorithm has been tested on different colour images and the best value of the embedding strength is Δ = 20. PSNR and SSIM have been used to evaluate the distortion caused to the original image due to the watermarking data. PSNR larger than 55 dB and SSIM larger than 0.99 have been achieved. The proposed algorithm showed resistance against several attacks such as: vertical cropping, horizontal cropping, scaling, JPEG compression, additive noise, low-pass filter, and Gaussian filter.

5. REFERENCES

- Al-Gindy, A., Al-Ahmad, H., Qahwaji, R., and Tawfik, A. (2009), A new watermarking scheme for colour images captured by mobile phone cameras: International Journal of Computer Science and Network Security, vol. 9 No. 7, pp248-254.
- Al-Gindy, A., Al-Ahmad, H., Qahwaji, R., and Tawfik. (2008), A novel blind image watermarking technique for colour RGB images in the DCT domain using green channel: Communications, Computers and Applications, MIC-CCA 2008. Mosharaka International Conference on, pp26-31.
- Barni, M., Bartolini, P.(2001), An Improved Wavelet Based Watermarking Through Pixelwise Masking: IEEE transactions on image processing, Vol. 10, No. 5, pp 783-791.
- Bhatnagar, G.and Raman, B., Elsevier B.V.(2008), A new robust reference watermarking scheme based on DWTSVD: All rights reserved.
- Danyali, H., Makhloghi, M. and Tab, F. (2009), Robust Blind DWT Based Digital Image Watermarking Using Singular Value Decomposition: International Journal of Innovative Computing, Information and Control, Vol.8, No. 7(A), pp.4691-4703.
- Kashyap, N.,G. SINHA, G. I.J.(2012), Image Watermarking Using 3-Level Discrete Wavelet Transform (DWT): Modern Education and Computer Science, pp. 50-56.

- Khatkale, P.,Jadhav, K. and Khasne, M. (2012), Digital Watermarking Technique for Authentication of Color Image: International Journal of Emerging Technology and Advanced Engnieering, vol. 2, Issue 7, pp454-460.
- Lee, S., et..al, (2007), Reversible Image Watermarking Based on Integer to Integer Wavelet Transform: IEEE Transaction on Information Forensics and Security, vol. 2, No. 3, pp. 321-330.
- Manoharan, J., et al. (2010), Performance Analysis of Spatial and Frequency Domain Multiple Data Embedding Techniques towards Geometric Attacks: International Journal of Security (IJS), Volume (4), Issue (3).
- Shing, A. Mishra, A (2011), Wavelet Based Watermarking on Digital Image: Indian Journal of computer Science and Engineering.
- Singh, P., Chadha, R (2013), A Survey of Digital Watermarking Techniques, Applications and Attacks: International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 9.
- Xia, X., Boncelet, C., and Arce,G.(1997), A Multiresolution Watermark for Digital Images: Proc. IEEE Int. Conf. on Image Processing.