HOST ADAPTIVE COLOUR IMAGE WATERMARKING USING COMPLEX WAVELETS

A. Bouridane[1], F. Kurugollu[1], M. Byrne[1] and S. Boussakta[2]

[1] School of Computer Science, Queen's University Belfast
Belfast, BT7 1NN, UK
[2] School of Electronic and Electrical Engineering,
University of Leeds, LS2 9JT, UK
{a.bouridane, f.kurugollu, b1248999}@qub.ac.uk
S.Boussakta@ee.leeds.ac.uk

ABSTRACT

The main conflict facing implementers of digital watermarking systems is the balance between imperceptibility and robustness. This paper introduces an algorithm that provides a means for embedding colour watermark images in colour host images. It produces high fidelity watermarked images that are capable of retaining a large amount of watermark data without the need for redundant embedding. The process ensures that similar fidelity and robustness characteristics are achieved regardless of the host image used.

Keywords: Watermarking, Data Hiding, Secure Communications, Multimedia, Complex Wavelets

1. INTRODUCTION

There are many different watermarking techniques currently under investigation, each catered to a particular role in the commercial world. The technique developed herein is an imperceptible, robust watermarking scheme for colour digital images. Obvious requirements of such a system are that it should have a minimum affect on the fidelity of the host image, and that the embedded watermark should be resilient against attempts to remove it from the host by means of image manipulation operations such as filtering, cropping, rotation, etc.

Importantly, an algorithm should be able to effectively watermark a wide range of host images and still achieve the same imperceptibility and robustness characteristics. Only in this way can an algorithm be deemed consistently reliable for general use. For this reason a watermarking scheme should be flexible enough to adjust its embedding procedure to match the target image. In this way it can best achieve the desired watermarking characteristics.

This philosophy regards the watermarking process as communications with side information. Cox *et al* “believe that modeling watermarking as communication with side information allows more effective watermark insertion and detection methods to be designed,” [4]. When host content is viewed purely as noise, no advantage is taken of the fact that the content is completely known to the watermark embedder (and detector, if implementing an informed watermarking system).

Whereas most current watermarking schemes use a pseudorandom sequence to represent watermark data (i.e. a simple binary logo), the watermark information embedded by this algorithm consists of a 24-bit colour image, which may be of any size or shape up to the size in bytes of the host image.

This algorithm utilises the Dual-Tree Complex Wavelet Transform (DT CWT) proposed by Kingsbury [6] to embed and extract watermark data. This transform overcomes the limitations of other commonly used transform domains. In particular the DT CWT provides approximate shift invariance and directional selectivity, the absence of which represent major drawbacks of the Discrete Wavelet Transform (DWT). The DT CWT also accurately models the Human Visual System (HVS) making it ideally suited for imperceptible watermarking. This domain has been proved successful in embedding imperceptible, robust watermarks in both greyscale and colour images [3]).

2. THE DT CWT

Up until the development of the DT CWT, complex wavelets had not been widely used in image processing due to the difficulties in designing complex filters that satisfy the perfect reconstruction (PR) property. However, by using two trees of real filters to generate the real and imaginary parts of the wavelet coefficients separately, Kingsbury overcomes this problem (see figure 1).

The top-level filters in the two trees operate on the odd and even samples of the input respectively. Even though the outputs of the two trees are downsampled, by summing the outputs during reconstruction approximate shift invariance is achieved.

As a result of having two trees the DT CWT has 2:1 redundancy for 1D signals. This means that the DT CWT consists of six different subbands at each level as opposed to three with the DWT. The orientations for these bands are 15°, 75°, 45°, -15°, -75°, and -45° thus overcoming the problem of directional selectivity.

Top

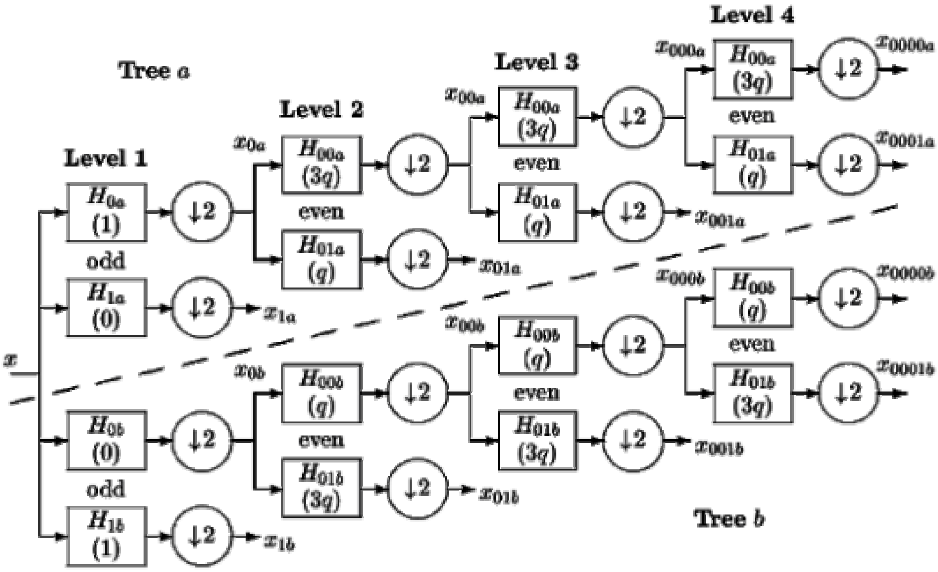


Figure 1: The Dual-Tree implementation of the Complex Wavelet Transform

3. DESCRIPTION OF THE PROPOSED ALGORITHM

Embedding a watermark redundantly in a host image has been shown to increase robustness [3]. However this replication of information adversely affects the fidelity of the watermarked image. This algorithm removes the need for the redundant embedding while maintaining accurate watermark retrieval. It interprets the host image and determines the areas most suitable for containing watermark information. In this case these areas are defined as those pixel values capable of sustaining the most watermark energy, i.e. the lowest valued pixels.

The overall watermarking process is similar to those implemented by Kundar *et al* [7] and Hsu *et al* [5] except that they restrict their watermarks to simple binary logos and focus on the DWT.

The first stage of the process sorts each colour channel of the host image is into ascending order by pixel magnitude. This ordering is used to identify the pixels in the host with the lowest values in that particular channel.

The watermark image is rearranged so that its coefficients will be fused with the lowest values in the host image as shown in figures 2 and 3. Adding the watermark data to the lowest valued pixels ensures that in the vast majority of cases the host image will be able to retain all of the watermark energy. Also by spreading the watermark image throughout the host any regular form the image might have is removed.

Top

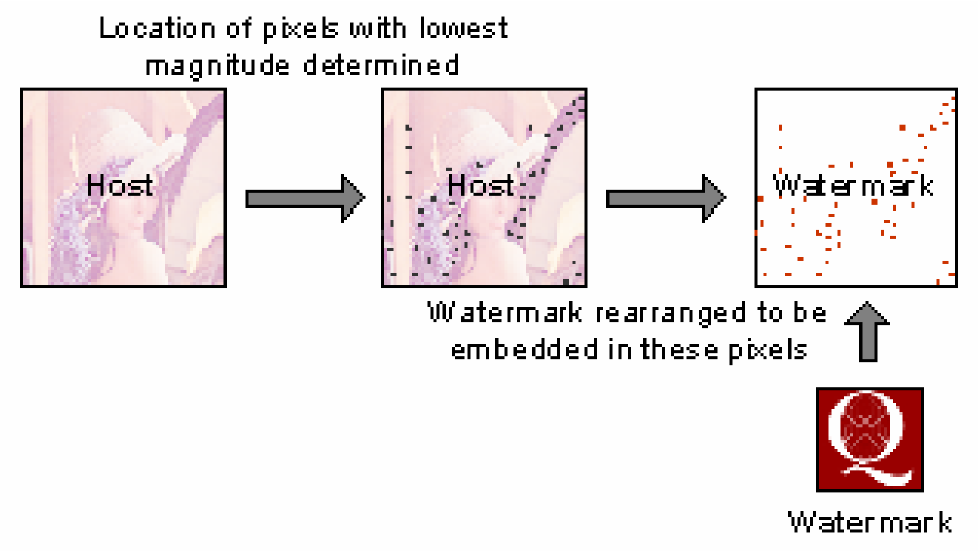

Location of pixels with lowest magnitude determined
Host
Host
Watermark
Watermark rearranged to be embedded in these pixels
Watermark

Figure 2: Adapting the watermark image to the host's content

The host and modified watermark are then transformed to the complex wavelet domain by applying a four level CWT decomposition with the Antonini filter. The watermark and host coefficients are then fused as described in equation (1).

$$\hat{s}^{i}_{o,l}(m,n) = s^{i}_{o,l}(m,n) + \alpha_{o,l} w_{o,l}(m,n) \quad \textbf{(1)}$$

Where $\hat{s}$, s, and w correspond to the wavelet coefficient domains of the watermarked image, host image, and watermark image respectively. o, l and i denote the subband, decomposition level, and segment number respectively. m and n give the coefficient location and α determines the watermark strength.

The final stage of the embedding process involves transforming the watermarked coefficients back to the spatial domain by applying the inverse DT CWT. Figure 4 describes the watermarking process visually.

The current requirement for extraction is that the original host image be available. The original and watermarked images are transformed to the complex wavelet domain by applying the same four level CWT decomposition. The watermark coefficients are then extracted according to equation (2)

$$w_{o,l}(m,n) = \frac{\hat{s}^{i}_{o,l}(m,n) - s^{i}_{o,l}(m,n)}{\alpha_{o,l}} \quad \textbf{(2)}$$

The extracted watermark coefficients are transformed to the spatial domain by applying the inverse DT CWT transform. The host image pixel ordering, which may be

Top

either retained from embedding or generated from the original host, is then used to reconstruct the extracted watermark.

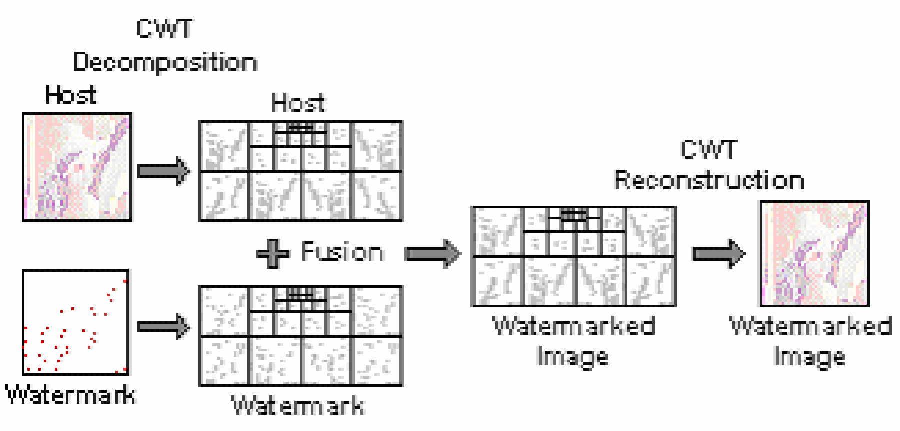


Figure 4: Creating the watermarked image

4. RESULTS & ANALYSIS

The algorithm has been extensively tested on various standard host images. These tests included watermark extraction after the application of a wide range of common attacks.

Directly comparing the proposed algorithm to that of Bouridane *et al* [3] produces the results shown in figure 5. This provides a comparison of watermarked image fidelity and extracted watermark correlation before attack.

The proposed algorithm demonstrates remarkable consistency across all host images tested, much more so than that of reference [3]. PSNR values for watermarked images exceeded 45dB for all host images. Correlation for the extracted watermark exceeded 0.996 in all cases. The proposed algorithm is clearly less dependent on host image content than that of [3].

By embedding only in the necessary number of lowest valued pixels, the host image becomes somewhat insignificant (up to a point) when using the proposed algorithm. As long as the lowest valued pixels of the host are capable of containing all of the watermark data without any exceeding the maximum pixel value (255) then all host images become equivalent.

Extraction was tested after various attacks of varying severity were applied to the watermarked images. These attacks included JPEG compression, median filtering, Gaussian blurring, cropping, rotating, and additive noise. The results of these tests show that both the proposed and reference [3] algorithms are reasonable at withstanding moderate changes to the watermarked image. Figure 6 gives a sample of some of these

Top

results. An increase in attack severity however causes the rapid degradation of the embedded watermark for the proposed algorithm.

Comparing the proposed algorithm to those of Barni *et al* [1, 2] uncovers some fundamental differences in approach. Whereas the proposed algorithm and that of reference [3] use a 24-bit colour image to represent the watermark, Barni *et al* instead embed a pseudorandom sequence. Therefore the proposed algorithm is embedding a substantially greater payload than those aforementioned (on average 32 times more watermark energy).

Barni *et al* describe a DWT watermarking algorithm in their research [1]. Comparing the proposed algorithm with that of reference [1] it becomes apparent that the proposed algorithm produces watermarked images of much higher fidelity (see table 1). For the Lena image at an alpha value of 2.14%, for instance, the resulting PSNR value is 46.55dB with the proposed algorithm. This compares to the value of 35.76dB achieved by the Barni *et al* algorithm. This is a considerable improvement especially given the increased payload.

As stated previously, severe attacks cause the rapid degradation of embedded watermarks with the proposed algorithm. For example, watermark data can be effectively lost if JPEG quality is less than 50%. A comparison with the Barni *et al* algorithm shows that it is robust against JPEG compression to a remarkable quality factor of 8%.

The proposed algorithm exhibits good resilience against the cropping attack being capable of extracting the watermark image when the cropped portion is of size 72x72. This is only slightly poorer than the Barni *et al* algorithm which can correctly detect watermark presence when the cropped portion has a size of 32x32.

5. CONCLUSIONS

This algorithm has shown that a watermark can be accurately retained in a host image without the need for redundant embedding. This has the added bonus of greatly increasing imperceptibility in the watermarked image. Initially images watermarked using this technique withstand attack quite well but the extracted watermark quickly becomes degraded as the watermarked image is more significantly modified. At this point the absence of redundant watermark data becomes noticeable.

It seems likely that no one watermarking scheme will be universally acceptable to all users. Rather a range of algorithms are likely to be needed that allow a user to select the properties they desire for their particular watermarked image; whether this be high fidelity at the cost of robustness, high robustness at the cost of imperceptibility, or a balance somewhere between the two.

Top

This algorithm then offers potential users a high level of imperceptibility if they are sure their image will not be significantly modified. It achieves this by embedding only the necessary amount of watermark information while exploiting the properties of the DT CWT in modelling the HVS. The algorithm may prove to have uses both as a robust watermarking scheme and for a fragile watermarking.

6. REFERENCES

[1] M. Barni, F. Bartolini, and A. Piva, *"Improved wavelet-based watermarking through pixel-wise masking,"* IEEE Trans. on Image Processing, vol. 10, May 2001

[2] M. Barni, F. Bartolini, and A. Piva, *"Multichannel watermarking of colour images,"* IEEE Trans. on circuits and systems for video technology, vol. 12, Mar 2002

[3] A. Bouridane, F. Kurugollu, R. Beggs, and S. Boussakta, *"Colour image watermarking in the complex wavelet domain,"* in Proc. of IEEE ICECS, 2003

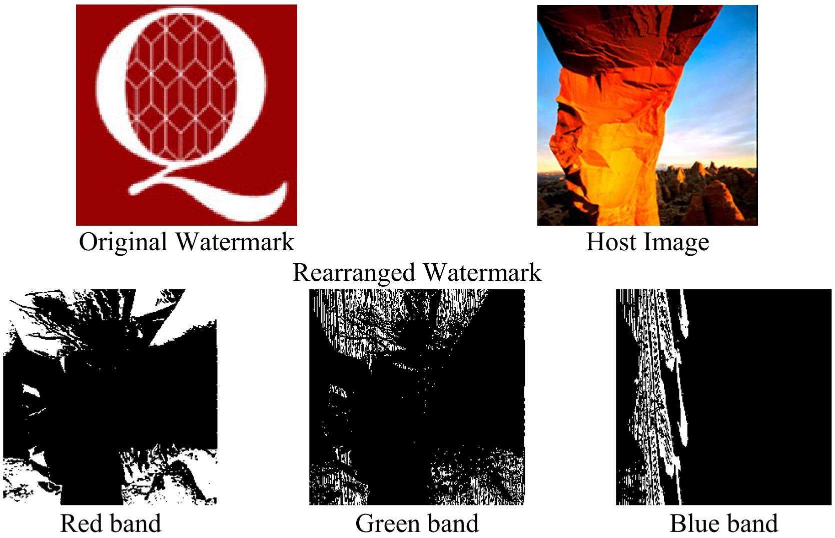
[4] I. J. Cox, M. L. Miller, and A. L. McKellips, *"Watermarking as communications with side information,"* in Proc. of the IEEE, Special Issue on Identification and Protection of Multimedia Information 87, pp. 1127 1141, July 1999

[5] C. -T. Hsu and J. -L. Wu, *"Multiresolution watermarking for digital images,"* IEEE Trans. Circuits Syst. II vol. 45, Aug 1998

[6] N. Kingsbury, *"The dual-tree complex wavelet transform: a new technique for shift invariance and directional filters,"* IEEE Digital Signal Processing Workshop, DSP 98, Bryce Canyon, pp. Paper no 86, 1998

[7] D. Kundur and D. Hatzinakos, *"A robust digital image watermarking method using wavelet based fusion,"* in Proc. 4th IEEE Int. Conf. Image Processing '97, Santa Barbara , CA, Oct 1997

Top


Original Watermark

Host Image

Rearranged Watermark

Red band

Green band

Blue band

Figure 3: Rearranged watermark data as a result of sorting the Skyline Arch image. White areas represent watermark data.

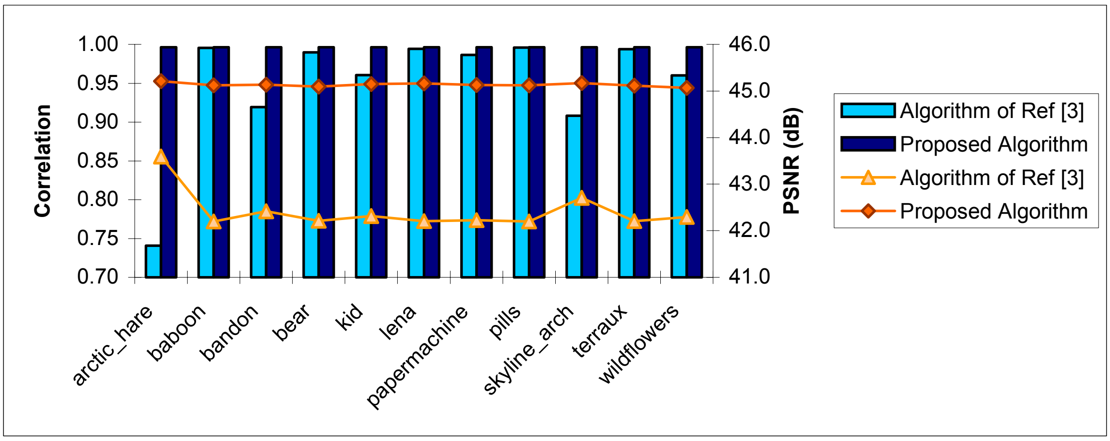


Figure 5: Watermarked image fidelity and extracted watermark correlation for a selection of host images at an alpha value of 3%. Lines show fidelity and bars show extracted watermark correlation.

Top

Image	Alpha	Proposed Algorithm	Algorithm of Ref [1]	Algorithm of Ref [3]
Peppers	1.68	47.6135	37.98	44.8065
Boat	2.10	46.5067	35.44	43.65.69
Airplane	1.98	46.7327	35.87	43.7968
Lena	2.14	46.55	35.76	43.6463

Table 1: PSNR comparison of watermarked images

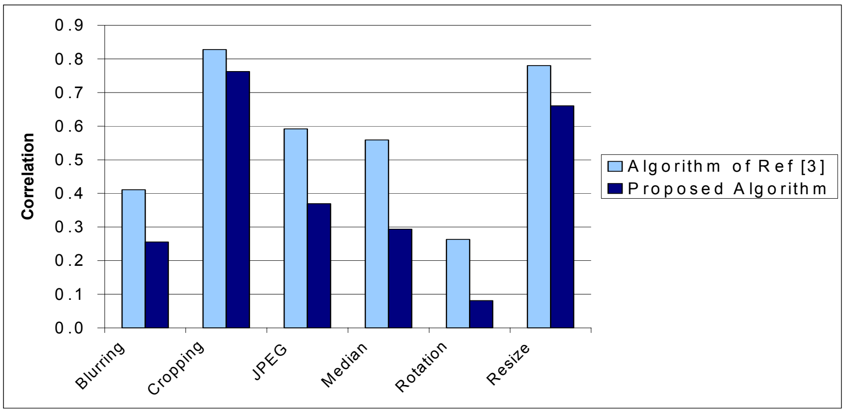


Figure 6: Extracted watermark correlation after moderate attacks have been applied

Top