DUAL WATERMARKING ALGORITHM EXPLOITING THE LOGARITHMIC CHARACTERISTIC OF THE HUMAN EYE'S SENSITIVITY TO LUMINANCE

Zhe Wang, Stephen Marshall

Department of Electronic and Electrical Eng, University of Strathclyde, 204, George Street, Glasgow, G1 1XW, UK
phone: (0086)01063054951, 0044141548 2199, email: wangzhe_doc@hotmail.com, s.marshall@eee.strath.ac.uk

ABSTRACT

The proposed colour image watermarking algorithm exploits the human visual system to optimise the trade off between the visibility and the robustness of the watermark. A less sensitive colour channel is selected to be watermarked and central watermarking is used to give the algorithm an extra robustness to image cropping. The DWT and DCT transforms are combined to pack the most energy into a few coefficients. The logarithmic sensitivity of the Human eye to luminance is exploited by assigning pixels into groups with different luminance ranges and watermarking them with different insertion powers. Test results show that the proposed algorithm has very good performance and is robust to several common image manipulations.

1. INTRODUCTION

With the global growth of the Internet and the forthcoming deployment of the 3 G mobile network, digital multimedia such as images, audio and video can be easily distributed and shared worldwide. A serious problem caused by this convenience is that digital multimedia contents can also be easily duplicated or altered without the authorization from the owners of the contents. Copyright violation has become a considerable source of financial loss. It is estimated that MPAA(Motion Picture Association of America) companies lost approximately 3.8 billion US Dollars worldwide to physical piracy and 2.3 billion US Dollars to Internet piracy in 2005[1]. And for music industries a total 4.6 billion US Dollars pirates were sold worldwide in 2004[2]. The digital watermarking is a technique which has developed as a potential solution to this violation of copyright protection for digital content.

The digital watermarking of still images is essentially a technique to imperceptibly embed a digital watermark sequence into the host content and detect it later to verify ownership. Existing watermarking algorithms can be classified into two categories: spatial domain and transform domain. In the former case the watermark is embedded into the host image by directly altering the pixel values. In the latter case the watermark embedding is performed by altering the coefficients of the transformed version of the host image. The two most important properties of a digital watermark are its imperceptibility and robustness. The *imperceptibility* requirement means that it should not be possible to see the watermark during normal viewing. The HVS (Human Visual System) is commonly exploited to achieve this requirement. Similarly *robustness* requires that the embedded watermark can be successfully detected following successive image manipulations and even hostile attacks. More general information on digital watermarking can be found in [3].

In the proposed algorithm, the watermark bits are first encoded using 15 repetition code. The original RGB colour space of the host image is transformed to YUV for a potential multi-channel watermarking and the U channel is selected for single channel watermarking as it is less sensitive to the eye. Only the central region of the U channel image is used for further processing to make it robust against cropping. As the human eyes possess a logarithmic characteristic of sensitivity to luminance, watermark bits can be embedded into pixels with different insertion powers depending on their luminance values. Thus after a DWT transform, pixels in the LL sub-band of the DWT decomposed U channel image are organised into 5 groups each of which covers a specified luminance range. A DCT is then applied to the 4 groups with the highest luminance range. The largest DCT coefficients are identified and mixed together to form the feature vector into which watermark bits will be embedded. Finally by following the watermark embedding formula, DCT coefficients in the feature vector from different groups are watermarked with different insertion powers.

2. WATERMARK EMBEDDING SCHEME

There are two types of watermark: single-bit watermark and multi-bit watermark. The single-bit watermark is an arbitrary binary sequence which is detected as either present or not present by the detector. The multi-bit watermark is a complete binary sequence which is required to be correctly recovered. In the proposed algorithm a multi-bit watermark W is first encoded with 15 repetition code. The encoded watermark is then uniquely randomised by a private key *k*. The error correction coding and the watermark randomisation effectively spread the errors which might occur during image manipulation over all encoded watermark bits.

The colour space of the original colour image is RGB which is highly correlated between colour channels. In the proposed algorithm multi-channel watermarking can be applied i.e. channels can be independently watermarked and therefore RGB colour space is not suitable for this purpose. S.A.M.Gilani and A.N.Skodras[4] have shown that YUV colour space is a better choice for watermarking applications compared to other colour transforms including YIQ, HIS and L*a*b*.

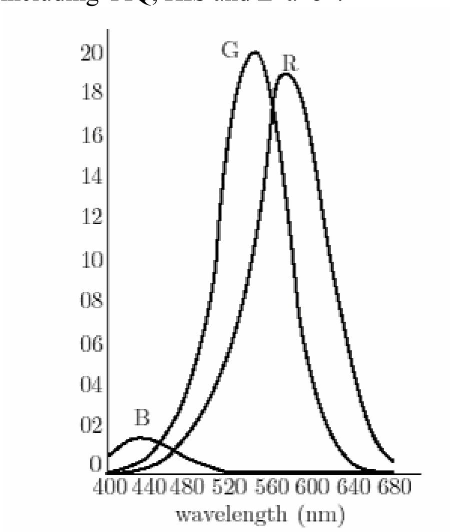

Figure 1. Fraction of light absorbed by each type of cone

YUV colour space has less inter-channel correlation than RGB. The Y channel represents the luminance components of the image to which the human eye is more sensitive than it is to the chrominance components. The U channel and the V channel represent orthogonal colour components. Figure 1 shows the fraction of light absorbed by each type of cone in the human eye. It can be seen that the human eye's sensitivity to blue light is much lower than to red and green. Thus for single channel watermarking the U channel is superior to the Y and V channels due to the higher tolerance to distortion.

Consider a case in which the watermark bits are uniformly embedded over the whole U channel image. If 1/8 of the length of the side is cropped from the edge to the centre of the watermarked image in each of the four directions, 7/16 of the original area will be removed i.e. nearly half of the watermark information will be lost. This information loss will significantly affect the correct recovery of the watermark in the detector. Therefore in the proposed algorithm only the central part of the U channel image U_c (the remaining 9/16 portion of the original area as shown in Figure 2) is selected to be watermarked. This gives the algorithm an extra robustness against geometrical cropping.

To make the watermark robust, its bits should be bounded to the significant regions of the host image. Pixels in these regions hold the most energy of the image. In the frequency domain this energy is held mainly by low frequency coefficients. The wavelet decomposition is thus used in the proposed algorithm to separate the low frequency components from higher frequency components. The selected central part of the U channel image U_c is first processed by a 1-level wavelet transform. The wavelet basis used in this algorithm is the 'Haar' wavelet. The U_c image is decomposed into 4 sub-bands which are denoted by HH, HL, LH and LL respectively with a descending order in frequency. HH, HL and LH sub-bands contain relatively

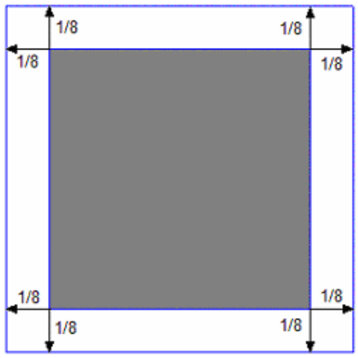

Figure 2. Illustration of U_c ,the central portion of U channel for watermark embedding

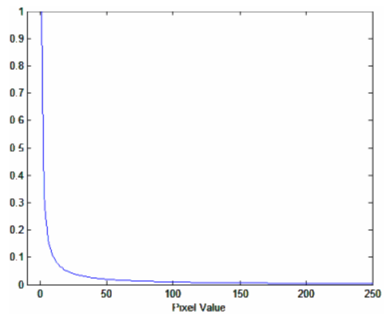

Figure 3. The logarithm characteristic of human eye's sensitivity to luminance

higher frequency components thus they are not suitable for watermark embedding. The LL sub-band which is an approximation of U_c holds the most energy and thus is used for further processing.

At this stage some existing watermarking algorithms embed the watermark bits into the DWT coefficients of the LL sub-band or the LL subband after more levels of DWT decomposition[5][6][7][8][9][10] or further transform the LL sub-band by other frequency domain transforms then simply embed the watermark[11].

In the proposed algorithm the Human Visual System (HVS) is exploited at this point to further enhance the robustness of the watermark. By doing this, pixels with different luminance will be watermarked with different insertion power to obtain an appropriate trade off between the watermark's visibility and the robustness. The sensitivity of the human eyes to changes in luminance has an approximately logarithm characteristic which in this work is modelled by the function 1/x as shown in Figure 3. The higher the luminance value of the pixel, the more tolerant the human eyes are to the distortion. Hence in the proposed algorithm pixels in the LL sub-band are organised into 5 groups with different luminance ranges:

Group0: 0-20
Group1: 21-50
Group2: 51-100
Group3: 101-180
Group4: 181-255

	Position1	Position2	Position3	Position4	……
Group1	$(x1, y1)_1$	$(x2, y2)_1$	$(x3, y3)_1$	$(x4, y4)_1$	……
Group2	$(x1, y1)_2$	$(x2, y2)_2$	$(x3, y3)_2$	$(x4, y4)_2$	……
Group3	$(x1, y1)_3$	$(x2, y2)_3$	$(x3, y3)_3$	$(x4, y4)_3$	……
Group4	$(x1, y1)_4$	$(x2, y2)_4$	$(x3, y3)_4$	$(x4, y4)_4$	……

Table 1. Illustration of mapping table MT1. $(xn,yn)_m$ denotes the coordinates pair of the n^{th} pixel in group m

	Position1	Position2	Position3	……
Group Number	3	1	4	……
Coordinates	$(x, y)_1$	$(x, y)_2$	$(x, y)_3$	……

Table 2. Illustration of mapping table MT2. For example: The second DCT coefficient in the feature vector V is from group 1 in the location of $(x, y)_2$

Group 0 has the highest sensitivity to luminance in its range (see Figure 3) and is therefore not suitable for watermark embedding, thus only the remaining 4 groups are used. The groups with the highest luminance range, have watermarks embedded with the highest insertion power. Groups 1 to 4 are DCT transformed respectively. The Discrete Cosine Transform (DCT) is a transform that packs most of the image energy into the top left corner of the DCT coefficient matrix. Its excellent energy compaction property can be exploited here to further congregate the image energy into a minority of DCT coefficients for watermark embedding. Let the number of the original watermark bits be n. The $n\times15$ largest DCT coefficients of the 4 groups are selected to form the feature vector. Watermark bits are embedded into the feature vector using the following watermark embedding formula:

$$V' = V * (1 + \alpha W)$$

where V' represents the watermarked feature vector, V represents the original feature vector, W represents the watermark sequence and α is a scaling factor. The scaling factor α for a particular DCT coefficient in feature vector V depends on which group the coefficient come from. In the proposed algorithm the value of α for group 1 to 4 is set to 0.2, 0.3, 0.5, 0.8 respectively.

3. WATERMARK DETECTION SCHEME

In the proposed algorithm the original host image is required for watermark detection. The recovered encoded watermark Wre may be obtained using the inverse embedding formula:

$$Wre = (1/\alpha)[(Vs - V)/V]$$

where Wre is the recovered encoded watermark, Vs is the feature vector of the suspected image, V is the feature vector of the original host image, α is the scaling factor. To get the feature vector Vs of the suspected image Is, pixels in LL subband of U_c of the original image I are first grouped into the 4 groups G4 (group 1 to 4) following the same principle as

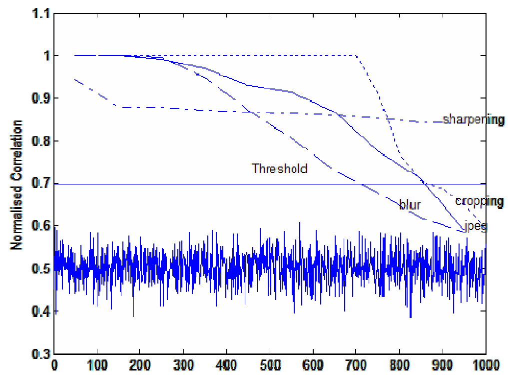

Figure 4. Statistical determination of the threshold T

in the watermark embedding scheme. A mapping table MT1 is established containing the group numbers and the coordinates of the pixels belonging to them. An illustration of MT1 is shown in Table 1.

By looking up the coordinate pairs in the mapping table MT1, corresponding pixels in LL sub-band of U_c in the suspected image Is are placed into the 4 groups G4s respectively. The 4 groups G4 of the original image are then DCT transformed and the $n\times15$ largest DCT coefficients are selected out to form the feature vector V. Another mapping table MT2 is established here containing the position numbers in the feature vector and their corresponding DCT coefficients' group number and location coordinates in their groups. MT2 is illustrated in Table 2. With this mapping table feature vector Vs of the suspected image Is is thus obtained by taking the corresponding DCT coefficients from the DCT transformed G4s.

Two watermark detection methods are adopted in the proposed algorithm: a normalised correlation method for detecting the single-bit watermark or the presence of the multi-bit watermark and a majority decoding method for correctly recovering the multi-bits watermark. The normalised correlation (NC) of the original watermark and the recovered watermark is calculated as follow

$$NC = (We \times Wre) / \sqrt{(We \times We)(Wre \times Wre)}$$

where NC is the normalised correlation of We and Wre with a maximum value of 1, We is the encoded original watermark, Wre is the recovered encoded watermark. If NC is above a pre-defined threshold T, a watermark is detected, otherwise no watermark is detected. Figure 4 shows the statistical method of determining the threshold T. The normalised correlations of the original watermark and 1000 random watermarks are plotted in figure 4. Above them 4 curves are plotted which represent the normalised correlations NCs of the original watermark and recovered watermarks under different image manipulations. The jpeg curve in figure 4 represents the NCs of the original watermark and recovered watermarks for watermarked images with JPEG compression quality from 95 to 15. The blur curve represents the NCs of the original watermark and recovered watermarks for watermarked images with blur radius from 0.5 to 2.0. The sharpening curve represents the NCs of the original watermark and recovered watermarks for watermarked images with sharpening intensity from 0 to 100. Curve cropping represents the NCs of the original watermark and recovered watermarks for watermarked images with cropped area from 0% to 56.03%. It can be seen that statistically the threshold T could be set to a value of 0.7. T could vary depending on the expected probability of false alarm.

To correctly recover the multi-bits watermark a majority detector is applied to each block of 15 adjacent bits in the recovered encoded watermark Wre. Each bit in the decoded watermark Wr is compared in turn to its corresponding bit in the original watermark W. If they are not the same, one error is counted. After the comparison is done over all the bits, the number of non-error bits is divided by the total number of bits in W. The quotient is the similarity measure result S. Figure 5 shows the similarity measure results S of a 16-bit watermark and 1000 randomly generated 16-bit watermarks. In this case a threshold of 0.75 would be acceptable with a false alarm probability around 3.8%.

4. TEST RESULTS AND DISCUSSION

The proposed algorithm was tested under several commonly used image manipulations. The test image was chosen to be a

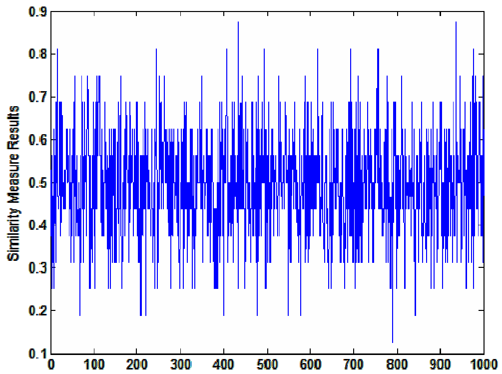

Figure 5. Similarity measure result of a 16-bit watermark and 1000 randomly generated 16-bit watermarks

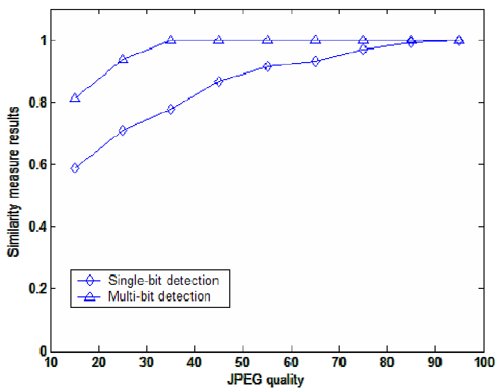

Figure 6. Robustness performance to JPEG qualities from 100 to 15

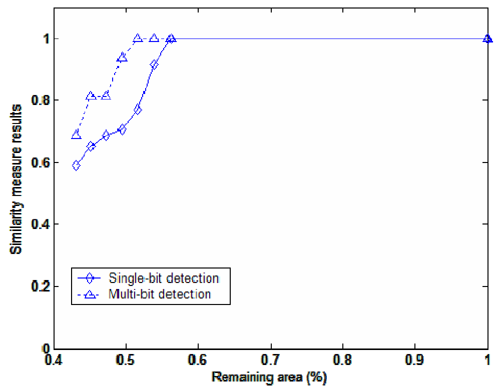

Figure 7. Robustness performance to cropping with remaining area from 100% to 43.07%

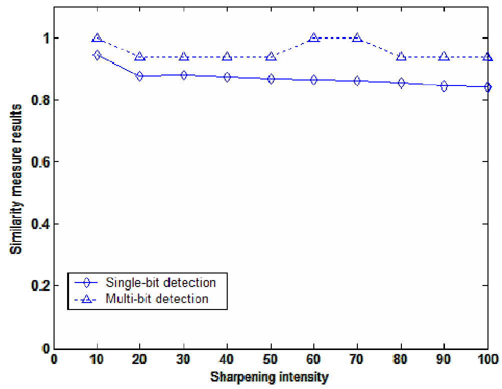

Figure 8. Robustness performance to sharpening with sharpening intensity from 10 to 100

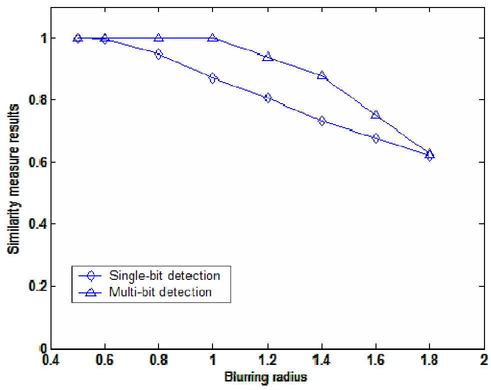

Figure 9. Robustness performance to blurring with blurring radius from 0.5 to 1.8

256×256 Lena. The watermark used was a 16 bit multi bit watermark. Watermarks of more than 16 bits were found to have worse robustness performance than the 16 bit watermark. There 16 bits is the limit of the watermarking embedding capacity for a 256×256 image. However, with the increase of the host image size the watermark embedding capacity will increase proportionally. The fidelity of the watermarked image was assessed by a group of observers using the subjective 5 level image quality contrast assessment under normal viewing conditions. The result 4.025 gives an good subjective image quality. Figure 6, 7, 8, 9 give the test results of the robustness performance of the proposed algorithm under JPEG compression, cropping, sharpening and blurring. For each case the similarity measure results of both the two detection methods presented in previous section are plotted. From the test results it can be seen that the proposed algorithm has excellent robustness performance for JPEG compression. Multi-bit watermark can be perfectly extracted with a JPEG quality factor as low 35 and can be detected with a JPEG quality even below 15. Excellent results again image cropping can also be seen in Figure 7. As a central watermarking method is adopted in the proposed algorithm, the watermark can be successfully detected even after more than half of the outer area of the image is removed. Both the two detection methods can strongly resist sharpening over the whole range of intensity. Figure 8 shows 2 very high and steady curves.

Figure 9 shows the algorithm's robustness to blurring with a linear function of increasing radius.

5. CONCLUSION

The concept of dual watermarking has existed for some time and the DWT, DCT are widely used in various watermarking algorithms. The proposed algorithm aims to optimise the trade off between the visibility and the robustness of the watermark. The idea here is to keep a minimum acceptable level of visibility while raising the watermark insertion power as much as possible. Both watermarking in the U channel and the multi-power insertion are designed for this purpose. Test results indicate that good robustness performance has been achieved without losing any visual quality of the watermarked image.

REFERENCES

[1]MPAA, http://mpaa.org/piracy.asp, 10/May/2006.

[2]IFPI, "Commercial Piracy Report 2005", London, 2005.

[3]E. H. Fu, "Literature Survey on Digital Image Watermarking," EE381K-*Multidimensional Signal Processing* 8/19/98.

[4]S. A. M. Gilani, A. N. Skodras, "MULTIPLE CHANNEL WATERMARKING OF COLOR IMAGES," TECHNICAL REPORT No. TR2002/02/03.

[5]C. T. Hsieh, Y. K. Wu, "Digital Image Multiresolution Watermark Based on Human Visual System Using Error Correcting Code," *Tamkang Journal of Science and Engineering*, Vol. 4, No. 3, pp. 201-208 (2001).

[6]J. Z. Wang, G. Wiederhold, "WaveMark: Digital Image Watermarking Using Daubechies' Wavelets and Error Correcting Coding," *Proceedings of SPIE*, vol. 3528, pp. 432-439, November 1998

[7]J. J. Chae, B. S. Manjunath, "A Robust Embedded Data from Wavelet Coefficients,"*Proceeding of the SPIE. Storage and Retrieval for Image and Video Data-Base VI,* Vol. 3312, pp. 308-317, San Jose, Feb. 1998.

[8] J. Shapiro, "Embedded image coding using zero trees of wavelet coefficients,"*IEEE Trans. on Signal Processing*, Vol. 41, No. 12, pp. 3445-3462. Dec.1993.

[9] X. G. Xia, C. G. Boncelet and G. R. Arce, "A Multiresolution Watermark for Digital Images," *Proc ICIP*, p.548-51, 1997.

[10]M. ÈANDÍK , E. MATÚŠ, D.LEVICKÝ, "Digital Watermarking in Wavelet Transform Domain," *Radio engineering*, Vol. 10, No. 2, July 2001.

[11]M. Shen, X. J. Zhang, L. S. Sun and P. J. Beadle, F. H. Y. Chan, "A METHOD FOR DIGITAL IMAGE WATERMARKING USING ICA," *4th International Symposium on Independent Component Analysis and Blind Signal Separation (ICA2003),* April 2003, Nara, Japan.