

1-D Walsh Coding With DCT Block Watermarking Technique of Colour Images Using Y Channel

Kamal A. Ahmed^{1,*}, Hussain Al-Ahmad¹, Patrick Gaydecki²

¹Department of Electrical and Computer Engineering, Khalifa University of Science, Technology and Research, Sharjah, UAE

²School of Electrical and Electronic Engineering University of Manchester, UK

Abstract In this paper a new blind technique using one dimensional Walsh coding to improve the robustness of image watermarking is presented. The proposed technique inserts the binary bits of handwritten signatures in the DCT blocks of the Y channel of the digital colour image. Watermarking algorithm which uses 1-D Walsh coding to embed mobile phone digits in images captured by the phone camera is also introduced. The 1-D Walsh coding can be applied either horizontally or vertically. The results presented here were obtained for horizontal 1-D Walsh coding. These results prove that the use of Walsh coding has improved robustness against JPEG compression.

Keywords Watermarking, DCT, Walsh Coding, Colour, Zena Image

1. Introduction

Recently, digital watermarking has been proposed as one solution to the problem of intellectual property protection[1]. In digital image watermarking, copyright protection information are embedded in the image in the form of a watermark. The image must not be visibly degraded by the presence of this watermark. Another main requirement of watermarking for copyright protection applications is robustness. Thus, the watermark must be resistant to unauthorized detection and decoding. In addition, the watermark must be tolerant to normal image processing techniques (e.g. compression), as well as to intentional attacks (attempts to destroy or remove the watermark).

In order to make the watermark detectable after some common attacks, the watermark should meet a certain requirements. The watermark should be perceptually transparent and robust. Perceptually transparent means the difference between the watermarked image and the original one should not be observable. Robustness means the watermark should be difficult to be removed and it should be extractable even if some common signal processing operations are applied, such as filtering and JPEG compression.

Digital watermarking can be classified according to a number of different criteria. One such criterion is according to the insertion domain. The watermark can be inserted in either the spatial or the transformed domain. It was found

that the transform domain watermarking schemes are typically much more robust to image manipulation compared to the spatial domain schemes. Examples of transform domains are Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT)[2, 3, 4, 5, 6, 7]. Watermarks may also be classified as robust or fragile. Robust watermarks are those, which are difficult to remove from the object in which they are embedded, despite various attacks they might be subjected to. Fragile watermarks are those that are easily destroyed by any attempt to tamper with them. There are two types of watermarking techniques: first, blind techniques where the original image is not required and second, non-blind technique where the original image is required to extract the watermark information.

This paper proposes the use of Walsh functions to improve the robustness of digital image watermarking techniques. In the proposed algorithms: first, Walsh functions of eight sequences are used to encode the watermark before embedding it in the luminance component (Y) of the host colour image[8]. The second algorithm will allow the watermark to be embedded many times in grey images captured by a mobile phone camera to increase the robustness against many attacks[9]. Both methods are blinds and do not require the original image to recover the watermark. The paper consists of 4 sections. In section 2, Walsh coding functions are introduced and also the DCT watermarking technique using the low frequency components is presented. Results, discussion and comparison with other algorithms are presented in Section 3. Finally, section 4 contains the concluding remarks.

2. The New Watermarking Algorithms

* Corresponding author:

kamal.ahmed@postgrad.manchester.ac.uk (Kamal A. Ahmed)

Published online at <http://journal.sapub.org/ajsp>

Copyright © 2012 Scientific & Academic Publishing. All Rights Reserved

2.1. Walsh Coding of Signature

Walsh coding is used in this method to increase the robustness of the digital watermark. Walsh functions are orthogonal and contain length elements. The Walsh function is produced proportional to the value of the length elements, where this length is in terms of 2^n with n as an integer. In the proposed method, the 1-D Walsh function is used to encode the signature before being embedded in the host image. The 1-D Walsh coding can be applied either horizontally or vertically. The proposed technique is carried out using the horizontal 1-D Walsh coding. By utilizing this type of coding, each bit of the signature's vectors will be replaced by the Walsh code sequence. This process is carried on all signatures' pixels. This involves manipulations with Hadamard matrices as detailed in [10, 11]. An example of Walsh functions with length=8 is:

$$\begin{aligned} w_1 &= [1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1] \\ w_2 &= [1 \ 1 \ 1 \ 1 \ -1 \ -1 \ -1 \ -1] \\ w_3 &= [1 \ 1 \ -1 \ -1 \ 1 \ 1 \ -1 \ -1] \\ w_4 &= [1 \ 1 \ -1 \ -1 \ -1 \ -1 \ 1 \ 1] \\ w_5 &= [1 \ -1 \ 1 \ 1 \ -1 \ -1 \ 1 \ 1] \\ w_6 &= [1 \ -1 \ -1 \ 1 \ 1 \ -1 \ -1 \ 1] \\ w_7 &= [1 \ -1 \ 1 \ -1 \ 1 \ -1 \ 1 \ -1] \\ w_8 &= [1 \ -1 \ 1 \ -1 \ -1 \ 1 \ -1 \ 1] \end{aligned} \quad (1)$$

In the proposed technique, the 16x64 signature is repeated and shuffled four times to become 64x64 binary bits. Then Walsh length of eight is used to replace each bit of the signature's row. The resulted Walsh coded signature would have 64x256 bits of values: +1 and -1 only. The effect of applying the Walsh coding to the signature is to spread it horizontally. The actual pixel values of the signature change from binary [0, 1] to integer values in the range [-1, +1]. Figure 1 shows the effect of applying the shuffling process to the signature.

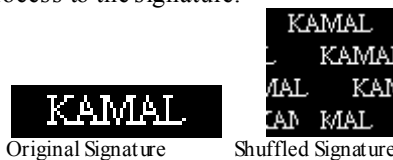


Figure 1. The effect of applying the four shuffling process on the original signature

2.2. DCT Blocks Algorithm Technique

The proposed algorithm scheme is based on feeding watermark bits into the low frequency band of the cover image DCT using 8x8 blocks. The eight low-frequency coefficients excluding the dc component of the 8x8 DCT blocks are used to hide the watermark bits [12, 13]. In the embedding, first, the signature is 1-D Walsh encoded and then the encoded signature's elements are inserted into the DCT blocks coefficients of the host image. The embedding process is achieved by placing the Walsh encoded signature's bits (either +1 or -1) into the stated (odd or even) coefficient value of the block and then taking the inverse DCT and constructing the watermarked image. The scale

factor is an absolute integer number which is multiplied by the embedded data bit to improve the robustness. After doing the block then it is transformed back to the spatial domain as shown in Figure 2.

The decoding process is achieved as follows, first is to convert the watermarked image into (8x8) blocks and applying the DCT to each block. Then Walsh coded coefficients are located for even or odd values. Then the signature is obtained by 1D Walsh decoding.

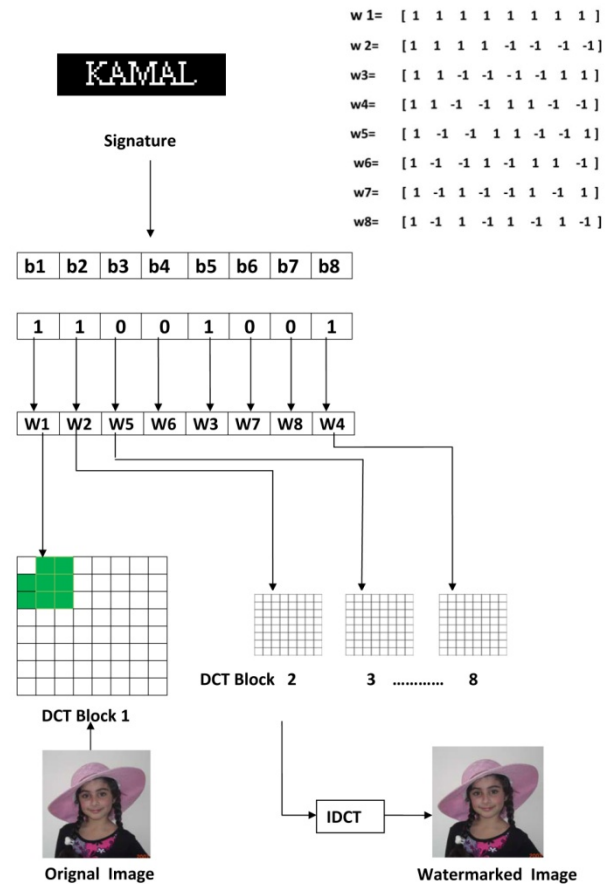


Figure 2. The DCT blocks decoder

2.3. Walsh Coding of Mobile Phone Number

The new watermarking scheme has also been implemented to hide mobile phone numbers in the host images. The reasons for choosing the phone numbers because each individual has a unique number (including the international code) which can be used to watermark his/her own images. For example the 14 digits of the UAE mobile phone number including the international country code (00971 50 3658212) can be used for this purpose. Also, the summation of the decimal digits is added to the 14 digits to make them 16 decimal digits (00971 50 3658212 49). The advantage of adding the summation to the 14 digits is to be able to check that the extracted number is correct or not. Each of the 16 decimal digits is converted into 4 bit binary number and Walsh coded. The size of the watermark is small compared to the host image so it can be embedded

many times[9].

One dimensional Walsh functions are used to encode the phone digits before embedding them in the cover image. This algorithm was carried out using the horizontal 1-D Walsh coding. To implement this type of coding, each row's vector of the binary numbers will be replaced by its relevant Walsh code and then added to the DCT components. The method is implemented by swapping the binary representation of the 16 digits with the above Walsh codes (W1, W2, W3 and W4). The resulted Walsh coded phone numbers would have 64x64 bits of values: +1 and -1. Figure 2 shows the effect of applying 1D Walsh coding on the phone number with 4 Walsh sequence length. In this technique Walsh functions with length=4 are used:

$$\begin{aligned} w_1 &= [+1 \ +1 \ +1 \ +1] \\ w_2 &= [+1 \ +1 \ -1 \ -1] \\ w_3 &= [+1 \ -1 \ -1 \ +1] \\ w_4 &= [+1 \ -1 \ +1 \ -1] \end{aligned} \quad (2)$$

3. Results and Discussion













Image Scale= 10	Original Image	Watermarked Image
Lena PSNR=38 SSIM=0.9492		
Mosque PSNR=38 SSIM=0.9188		
Airplane PSNR=38 SSIM=0.9396		
Baboon PSNR=38 SSIM=0.9809		
Peppers PSNR=38 SSIM=0.9492		
Zena PSNR=38 SSIM=0.9256		

Figure 3. Six different test images and their watermarked versions

In order to verify the robustness and functionality of the first algorithm, a number of 24-bit colour images with

512x512 pixels have been used to test the proposed algorithms. Also a 16x64 binary signature image has been used as a watermark. Figure 3 shows samples of some images that have been used as host images in the watermarking algorithm. It is clear that the distortion caused by the new watermarking scheme is invisible. The test also, covered the use of different scaling factors for the watermarking and their effect on the fidelity of the watermarked image. Investigation is carried out to assess the fidelity of the images by using the Peak Signal to Noise Ratio (PSNR) and the Mean Structural Similarity (SSIM)[14]. Table1 shows the PSNR and SSIM values of different images using DCT blocks with Walsh coding. Table 2 shows the values of the JPEG quality below which the watermark cannot be extracted. It is clear that increasing of the scaling factor enhances the robustness of the algorithm at the expense of increasing the distortion caused to the watermarked images. Table 3 shows the different attacks using the Stir mark software. The algorithm survived JPEG and some other attacks.

In this section, the robustness of the second algorithm using mobile phone number as a watermark has been tested and compared with the case without using Walsh sequences. The analysis covered the use of different scaling factors for the watermarking and their effect on the fidelity of the watermarked image. Figure 4 shows samples of some images that have been used as host images in the watermarking algorithm. It is clear that the distortion caused by the new watermarking scheme is invisible.

Table 1. PSNR and SSIM with Walsh coding

WALSH CODED		
Extracted Signature SSIM and PSNR under JPG attack		
Zena Image		
Scaling factor	SSIM	PSNR
2	0.9955	48
4	0.9855	45
6	0.9699	42
8	0.9499	40
10	0.9256	38.2
Lena Image		
Scaling factor	SSIM	PSNR
2	0.9970	48.6
4	0.9902	45
6	0.9798	42
8	0.9659	39.8
10	0.9492	38
Peppers Image		
Scaling factor	SSIM	PSNR
2	0.9969	48.7
4	0.9902	45
6	0.9798	42.1
8	0.9659	40
10	0.9492	38.1

Table 2. The lowest JPEG factors with Walsh coding where the watermark can be recovered

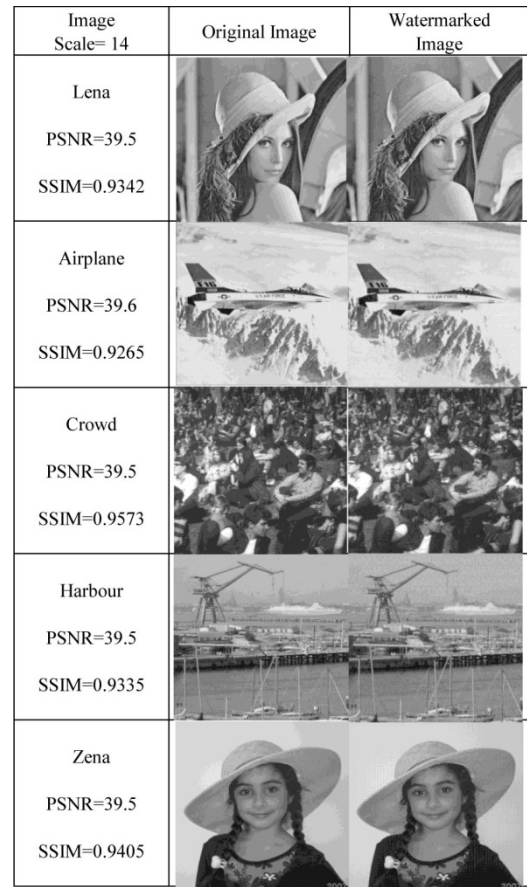
WALSH CODED	
Extracted Signature under JPEG attack	
Zena Image	
Scaling factor	JPG factor(Q)
2	100
4	73
6	57
8	43
10	35
Lena Image	
Scaling factor	JPG factor(Q)
2	100
4	77
6	61
8	47
10	35
Peppers Image	
Scaling factor	JPG factor(Q)
2	100
4	77
6	63
8	47
10	35

Table 3. The Normalized correlation (NC) for Lena under Stir mark attack at scale factor= 1

1-D Walsh Coded_ NC at scale factor= 10	
Attack	NC
Additive noise 0.1	1
Additive noise 0.3	1
Additive noise 0.5	1
Additive noise 0.7	1
Additive noise 0.9	1
Affine_1	0
Affine_8	0
Conv_1	0
JPEG30	1
JPEG35	1
JPEG40	1
JPEG45	1
PSNR_10	1
PSNR_20	1
PSNR_30	1
PSNR_50	1
PSNR_70	1
PSNR_90	1
Median 3x3	0
Median 5x5	0
Rotation:0.5 degree	0

The fidelity of the images is assessed by using the Peak Signal to Noise Ratio (PSNR) and the Mean Structural Similarity (SSIM)[14]. It is clear that the algorithm is more

robust with Walsh coding.

**Figure 4.** Six different test images and their watermarked versions**Table 4.** PSNR and SSIM of extracted Mobile Phone Number with Walsh coding

WALSH CODED		
Extracted Mobile Phone Number SSIM and PSNR under JPG attack		
Zena Image		
Scaling factor	SSIM	PSNR
2	0.9986	56.4
4	0.9943	50.3
6	0.987	46
8	0.9788	44.4
14	0.9405	39.5
Lena Image		
Scaling factor	SSIM	PSNR
2	0.9739	56.4
4	0.9713	50.5
6	0.9669	46.9
8	0.9608	44.4
14	0.9342	39.5
Peppers Image		
Scaling factor	SSIM	PSNR
2	0.9991	56.4
4	0.9965	50.4
6	0.9923	46.9
8	0.9862	44.4
14	0.9593	39.5

Table 5. The lowest JPEG factors with Walsh coding where the watermark can be recovered

WALSH CODED	
Extracted Mobile Number under JPEG attack	
Zena Image	
Scaling factor	JPG factor(Q)
2	99
4	81
6	71
8	59
14	35
Lena Image	
Scaling factor	JPG factor(Q)
2	100
4	90
6	75
8	59
14	35
Peppers Image	
Scaling factor	JPG factor(Q)
2	100
4	85
6	75
8	69
14	45

Table 6. The Normalized correlation (NC) for Lena under Stir mark attack at scale factor= 14

1-DWalsh Coded_ NC at scale factor= 14	
Attack	NC
Additive noise 0.1	1
Additive noise 0.3	1
Additive noise 0.5	1
Additive noise 0.7	1
Additive noise 0.9	1
Affine_1	0
Affine_8	0
Conv_1	0
JPEG30	1
JPEG35	1
JPEG40	1
JPEG45	1
PSNR_10	1
PSNR_20	1
PSNR_30	1
PSNR_50	1
PSNR_70	1
PSNR_90	1
Median 3x3	0
Median 5x5	0
Rotation:0.5 degree	0

Table 4 shows the PSNR and SSIM values of different images using DCT algorithm with Walsh coding. Table 5 shows the extracted phone number under different values of

JPEG attack and using different values of scaling factors, respectively. It is clear that increasing of the scaling factor enhances the robustness of the algorithm at the expense of increasing the distortion caused to the watermarked images. The algorithm is also tested using Stir mark attacks by using Lena image with scaling factor 14. Table 6 shows the Stir mark attacks and their normalised correlation (NC) values. The algorithm survived JPEG and some other attacks. It should be noted that the phone number is either recovered or not and therefore the NC is either 1 or 0.

4. Conclusions

In this paper, a new technique to embed 1-D Walsh coded handwritten signatures and mobile phone number as a watermark into grey level and colour images is presented. The proposed method used a block DCT based algorithm. It was found that the use of 1-D Walsh coding with DCT blocks provides high robustness against JPEG attacks compared to the method of embedding without coding. It was also found that the use of scaling factor with Walsh coding improves the robustness against JPEG compression but at the expense of degrading the quality of the watermarked image. The new scheme is blind and the watermark can be extracted without the original image.

REFERENCES

- [1] A. Bin Sewaif, H. Al-Ahmad, and M. E. Al-Mualla, "Walsh-Coded Signatures for Robust Digital Image Watermarking," Accepted for publication in the 2004 IEEE Region 10 Conference Analog and Digital Techniques in Electrical Engineering (TENCON), Thailand, November 2004, pp.431-434.
- [2] I. Cox, M. Miller, and J. Bloom, Digital Watermarking
- [3] Morgan Kaufmann Publishers, San Francisco, 2001.
- [4] S. Katzenbeisser, and F. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, London, 2000.
- [5] P-L. Lin, "Robust Transparent Image Watermarking System with Spatial Mechanisms", The Journal of Systems and Software, vol. 50, 2000, pp. 107-116.
- [6] M. Barni, F. Bartolini, V. Cappellini, and A. Piva, "A DCT-Domain System for Robust Image Watermarking," Signal Processing, vol. 66, 1998, pp. 357-372.
- [7] Al-Gindy, A. Tawfik H. Al- Ahmad and R. Qahwaji, "Enhanced DCT Based Technique with Shuffle Scheme For Robust Image Watermarking of Handwritten Signatures", International Conference for Communication, Computer and Power (ICCCP), Oman, February 2007, pp.450-455.
- [8] A. Al-Gindy, A. Tawfik H. Al- Ahmad and R. Qahwaji, "A New Blind Image Watermarking Of Handwritten Signatures using Low-Frequency Band DCT coefficients", IEEE

- International Conference on Signal Processing and Communications (ICSPC), November 2007, pp.1367-1370.
- [9] A. Al-Gindy, H. Al-Ahmad, R. Qahwaji and A. Tawfik, "Watermarking of Color Images in the DCT Domain Using Y Channel", IEEE/ACS International Conference on Computer Systems and Applications, May 2009, pp.1025-1028.
- [10] K. A. Ahmed, H. Al Ahmad, and P. Gaydecki, "A New Algorithm for Watermarking Images Captured by Mobile Phone Cameras", International Conference on Trends in Information Technology and Applications 2010 Ajman, UAE, December, 2010
- [11] K. A. Ahmed H. Al Ahmad, P. Gaydecki, "A Blind Block Based DCT Watermarking Technique for Gray Level Images Using One Dimensional Walsh Coding", International Conference on Current Trends in Information Technology (CTIT), December 2009, pp.79-84.
- [12] K. A. Ahmed, H. Al Ahmad, and P. Gaydecki, "1-D Walsh Coded Watermarking Technique for Colour Images Using the Y Chanel", 2011 IEEE GCC Conference and Exhibition, Dubai, UAE, February 2011, pp.299-302.
- [13] A. Al-Gindy, A. Tawfik, H. Al- Ahmad, R. Qahwaji and A. Tawfik, "A New Watermarking Scheme For Color Images Captured By Mobile Phone Camera", IJCSNS International Journal of Computer Science and Network Security, Vol. 9 No.7, July 2009, pp248-254.
- [14] A. Al-Gindy, A. Tawfik H. Al Ahmad and R. A. Qahwaji, "A New Blind Image Watermarking Technique for Dual Watermarks Using Low-Frequency Band DCT Coefficients", IEEE International Conference on Electronics, Circuits and Systems (ICECS), 2007, pp.538-541.
- [15] Hou Wang, A. C. Bovik, H. R. Sheikh, E. P. Simoncelli "Image Quality Assessment: From Error Visibility to Structural Similarity", IEEE Transaction on Image Processing, Vol.13, No.4, April 2004, pp.600-612.