

ENHANCED DCT BASED TECHNIQUE WITH SHUFFLE SCHEME FOR ROBUST IMAGE WATERMARKING OF HANDWRITTEN SIGNATURES

Ahmed N. Al-Gindy¹, Hussain Al Ahmad², Ayman Tawfik¹ and Rami A. Qahwaji³

1- Ajman University, UAE 2- Etisalat University College, UAE 3- University of Bradford, UK

ABSTRACT

This paper deals with an enhanced technique for robust image watermarking in the DCT domain. The technique is based on embedding watermark information in the middle frequency band of the DCT blocks. Handwritten signature is used as the watermark information which is embedded multi-times in the host image; before each insertion process a different shuffle operation is applied to the watermark. This shuffle process ensures that no spatial correlation exists between the host image and the multi watermark copies. This provides more protection against cropping attacks. The enhanced technique with shuffle operation is proved to be more robust than existing DCT based techniques. The new scheme is blind and does not require the original host image for watermark extraction.

Index terms—Image processing, DCT, Watermark.

1. INTRODUCTION

Many authors are concerned of distributing their work in fear that it may be copied illegally or represented as another's work [1]. Authors can claim the ownership of such digital media by embedding additional information and only distribute the media that contains this information. The embedded information, such as copyright, license and authorship is known as watermark [1]. A digital watermark can be described as a visible or preferably invisible identification code that is permanently embedded in data [2]. Visible watermarks, by nature, are more intrusive to the media and act to deter theft of the media, such as a warning sign announces an alarm system even if one does not exist. Examples of such watermarks can be seen easily on most network television stations by the station's logo in the corner of viewable screen. These watermarks are typically confined to an area of the image, which is less intrusive to the overall image. Attackers have a visible target and can remove the watermark by cropping the image [1].

Invisible watermarks have an advantage over visible watermarks, in that their location may be unknown. A common practice is to distribute the watermark (or watermarks) across the entire image [1]. Attacks on the watermark may not necessarily remove the watermark, but disable its readability. Attackers usually use different image processing techniques and various transformations to destroy the watermark [3]. Multiple watermarks can be placed in an image to increase the robustness.

Digital watermarking techniques can be classified into two general categories based on the used domain the first category methods are using the spatial domain while the second category methods are using the frequency domain. Discrete cosine transform (DCT) is a common used transform for embedding a watermark [4-8]. Using the DCT an image can be split up in frequency bands and the watermark can conveniently be embedded in the middle band frequencies. This approach can survive different attacks [4, 5].

Most of the watermarking techniques use logos or images with text information as watermark. Recently handwritten signatures were used [6,7]. However, the algorithms used were incomplete i.e. they require the original image to extract the watermark. One powerful technique for robust complete invisible watermarking is presented in [8]. In this technique, the binary watermark information is embedded in the middle-frequency band of the DCT domain. Eight watermark bits are embedded into 16 middle-frequency-band DCT coefficients of the host image. This allows embedding several copies of the watermark information into the host image. Although the proposed technique in [8] has proved to be robust for many attacks such as horizontal cropping, compression and low-pass filtering operation, it can not survive any significant non-horizontal cropping attacks. The reason is that there is spatial correlation between the host image sub-blocks and the sub-blocks of the watermark copies.

In this paper, a modified scheme based on the technique in [8] and uses handwritten signatures is presented. In the proposed technique the watermark is shuffled before each insertion process. The shuffle scheme is different in each iteration, so that each watermark copy will occupy different arrangement of the 8x8 host image sub-blocks.

2. PROPOSED ROBUST IMAGE WATERMARK

The proposed watermarking scheme is based on the possibility of embedding multi copies of the same binary watermark in the host image. Each watermark copy is differently shuffled before the embedding process. A flow-graph of the proposed algorithm is shown in Figure 1. The embedding algorithm used is the one presented in [8] where the watermark data are essentially embedded in the middle band of the DCT-domain to make a tradeoff between visual degradation and robustness. No original host image is required for watermark extraction.

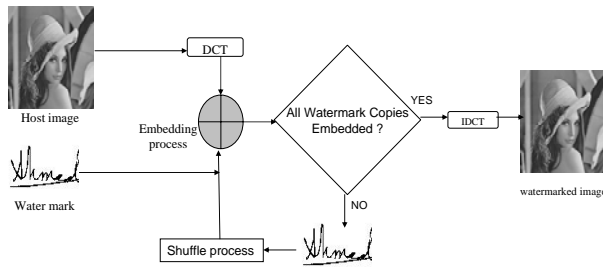


Figure 1. A flow-graph of the proposed watermarking scheme.

3. EMBEDDING ALGORITHM

The proposed embedding algorithm is based on hiding watermark bits into the middle frequency band of the host image DCT using 8x8 blocks. Sixteen mid-frequency band coefficients of the 8x8 DCT sub-block are used to hide 8 watermark bits. The used sixteen DCT coefficients of one 8x8 sub-block is shown in Figure 2. Each two horizontal DCT coefficients are used to hide one watermark bit

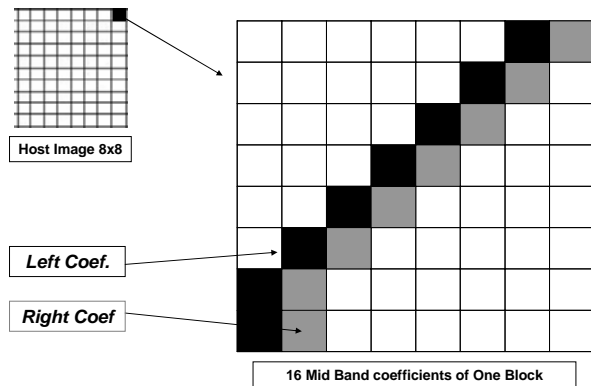


Figure 2. Mid band frequencies in one 8x8 bock in the host Image

The embedding of one watermark bit in the host image can be made after Reshape the binary watermark as a vector and apply the following steps:

- (1) Extract the watermark bit
- (2) Calculate the DCT of the Host image
- (3) Calculate the average of each two horizontal adjacent coefficients in the mid band frequencies for each 8x8 sub-block (see Fig. 2)

$$Average = (Left_Coef + Right_Coef) / 2$$

- (4) The embedding equation can be defined as follow :

$$Mid\ band = \begin{cases} w=1 & \begin{matrix} Left_Coef = average - \Delta \\ Left_Coef = average + \Delta \end{matrix} \\ w=0 & \begin{matrix} Left_Coef = average + \Delta \\ Left_Coef = average - \Delta \end{matrix} \end{cases} \dots (1)$$

Where Δ is a constant quantity and w is the watermark bit to be embedded.

The previous embedding steps are shown in Figure 3

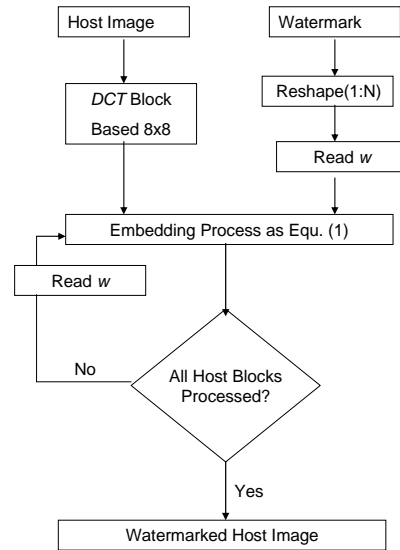


Figure 3. A flow graph representing the embedding steps.

The one-bit embedding operation is repeated to embed 8 bits in one 8x8 sub-block. Then the operation is repeated till one complete watermark is embedded in portion of the host image. The whole operation is repeated to embed the other copies of the same watermark. The number of the watermark copies that can be embedded in the host image depends on sizes of both the watermark and the host images. Each bit of the watermark w was embedded into the desired sub-block of the host image. Numbers of watermark copies that can be embedded can be given by:

$$WI = N_{HB} / N_{WB} \dots (2)$$

Where WI is the number of watermark copies, N_{HB} is the number of 8x8 host image blocks and N_{WB} is the numbers of 1x8 watermark blocks after reshaping.

4. RECONSTRUCTION ALGORITHM

The watermark information w can be extracted by the following steps

- (1) Perform DCT transform for the watermarked host image
- (2) Indicate the 8x8 sub-blocks that carry the same 8 bits of the watermark copies
- (3) Indicate the two coefficients (right one and the left one) in each sub-block that carry the watermark information
- (4) Calculate the summation of indicated right coefficients of the indicated 8x8 sub-blocks
- (5) Calculate the summation of indicated left coefficients of the indicated 8x8 sub-blocks
- (6) Form the resultant summation watermark w as follows :

If ($Sum\ of\ Right\ -Coefs$) > $Sum\ of\ left\ -coefs$
 Then $w=1$... (3)
 If ($Sum\ of\ Left\ -Coefs$) > $Sum\ of\ Right\ -coefs$
 Then $w=0$

The block diagram of the extraction process is shown in Figure 4.

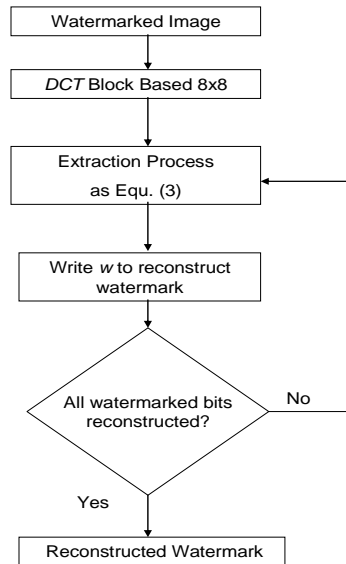


Figure 4. A block diagram representing the extraction process

This watermarking scheme can survive horizontal cropping provided that the cropped image contains at least one complete watermark. If non-horizontal cropping is applied, the cropped host image will not contain one complete watermark and a degraded watermark will be extracted. To reconstruct the original watermark, a shuffle scheme for watermark copies must be applied in the embedding process.

5. SHUFFLE SCHEME

A shuffle scheme is applied for each watermark copy before embedding as shown in Fig. 1. Different shuffle schemes could be applied. Simple shuffle technique is to reshape the watermark copy as vector and shift the vector by different shifts before the embedding process. The shift operation must be in cyclic way. The number of watermark shifted bits depends on the host image size and watermark size. It can be calculated as follows:

$$W_{SB} = Z_{wm} / WI \quad \dots (4)$$

Where W_{SB} is the number of watermark shifted bits, Z_{wm} is the size of the watermarked image and finally WI is the number of watermark copies to be embedded in the host image.

The watermark information can be retrieved by using a reverse process to the shift scheme which has been applied in the embedding process. This will yield the original bits order. Although the proposed shuffle scheme is applied for the technique presented in [8] to improve its

performance for non-horizontal cropping attacks, it may be applied also for other techniques such as the one presented in [9] and [10] that allow the possibility of embedding multiple copies of the watermark in the host image. It is worth to mention that although the proposed scheme is blind since it does not require the original host image for reconstruction, but it requires information such as the sizes of both host image and watermark image.

6. RESULTS




To test and verify the robustness of the new proposed scheme the watermarked image is attacked by cropping and JPEG compression. "Lena" gray level image of size 512x512 is used as a host image and a binary handwritten signature of size 96x64 was used as the watermark as shown in Figure 5. A comparison between the technique presented in [8] and the proposed new scheme is conducted in Tables (1), (2) and (3). The similarity measurement between the original watermark and the extracted watermark is illustrated using the Mean Square Error which provides objective judgment of the extracting fidelity



Figure 5 . The original host image "Lena" (a), and the watermark hand written signature (b).

Table 1 Shows the MSE values and remaining ratios of the watermarked "Lena" after cropping. The water mark can still be fully recovered with MSE=0 having the horizontal and non horizontal cropped area up to 75% of the original image. Also, the results illustrated in Table1(c) proves that the watermark cannot be fully recovered without the shuffle scheme MSE=0.0540, MSE=0.0562 and MSE=0.0563 respectively. Table 2 and table 3 demonstrates the effect of the JPEG compression at various levels of quality factors and show the Mean Square Error MSE of the retrieved watermark with the shuffle scheme (Table 2) and without the shuffle scheme (Table 3).

Table1:

(a): Host image cropping	(b): Result of cropping with shuffle scheme	(c): Result of cropping without shuffle scheme
		
50% Vertical	MSE=0	MSE=0.0540







		
75% Vertical	MSE=0	MSE=0.0562
		
75% Non-Horizontal	MSE=0	MSE=0.0563

Table2:

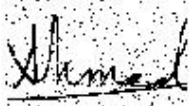



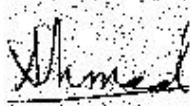



	
(a): JPEG attack with shuffle scheme at $q=85$ MSE=0.0341	(b): JPEG attack with shuffle scheme at $q=80$ MSE=0.1105
	
(c): JPEG attack with shuffle scheme at $q=75$ MSE=0.2158	(d): JPEG attack with shuffle scheme at $q=70$ MSE=0.2891

Table3:

	
(a): JPEG attack without shuffle scheme at $q=85$ MSE=0.0358	(b): JPEG attack without shuffle scheme at $q=80$ MSE=0.1174
	
(c): JPEG attack without shuffle scheme at $q=75$ MSE=0.2244	(d): JPEG attack without shuffle scheme at $q=70$ MSE=0.3125

7. CONCLUSIONS

An enhanced invisible robust watermark algorithm has been presented. The new technique used handwritten signatures as the watermark image. The new technique was used on images with a ratio of host image and watermark image sizes that allows multiple copies of the watermark to be embedded. The scheme provides high robustness against attacks such as horizontal and non-

horizontal cropping and jpeg compression. The new scheme is blind and the watermark can be extracted without the original image. The results show that this proposed technique survives powerful horizontal and non-horizontal cropping attacks while maintaining excellent robustness against compression and invisibility qualities.

REFERENCES

[1] Neil F. Johnson, "An introduction to watermark recovery from images," SANS Intrusion Detection and Response Conference (IDR'99), San Diego, CA, pp. 1-6, February 1999.

[2] I.J. Cox, and M.L.Miller. A review of watermarking and the importance of perceptual modeling. SPIE Electronic Imaging 97, storage and Retrieval for image and video Databases V, San Jose, CA February 1997.

[3] S. Craver, N.Memon, B.Yeo, N.M.Yeung, "resolving Ownerships with invisible watermarking Techniques: Limitations, attacks, and implications," IEEE Journal on selected Areas in Communications, Vol. 16, no. 4, pp. 573-586, 1998.

[4] F.M.Boland, J.J.K. Ruanaidh, and C. Dautzenberg, "Watermarking digital images for copyright protection," IEE Int. Conf. on Image processing and its Applications, Edinburgh, U.K, PP313-336, July 1995.

[5] C.-T. Hsu and J.-L.Wu, "Hidden signatures in images," ICIP-96 IEEE Int. Conf. Image Processing, Vol. 3, Lausanne, Switzerland, pp. 223-226, September 1996.

[6] A. Ben Sewaif, M. Al-Mualla and H. Al-Ahmad, "Walsh-Coded Signatures for Robust Digital Image Watermarking", In Proceedings of the 2004 IEEE Region 10 Conference - Analog and Digital Techniques in Electrical Engineering (TENCON2004), Chiang Mai, Thailand, pp. 431-434, 21-24 November, 2004

[7] A. Ben Sewaif, M. Al-Mualla and H. Al-Ahmad, "2 D Walsh Coding for Robust Digital Image Watermarking", proceedings of the 4th IEEE International Symposium on Signal Processing and Information Technology (ISSPIT2004), Rome, Italy, pp. 302-305, 18-21 December, 2004

[8] Wen-Nung Lie, Guo-Shiang Lin, Chih-Liang Wu, and Ta Chum Wang, " Robust Image Watermarking on DCT Domain," ISCAS 2000- IEEE Int. Symposium on circuits and Systems, Geneva, Switzerland, pp. 228-231, May 2000.

[9] I. J. Cox, J. Kilian, F. Thomson Leighton, and Talal Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," IEEE Trans. On Image Processing: Vol. 6, No.12: pp. 1673-1687, December 1997.

[10] M. Barni, F. Bartolini and V. Cappellini, "Copyright protection of digital images by embedded unperceivable marks," Image and Vision Computing, Vol. 16: pp. 897-906, 1998.