International Journal of Computer Networks and Communications Security

VOL. 6, NO. 4, APRIL 2018, 61–75
Available online at: www.ijcncs.org
E-ISSN 2308-9830 (Online) / ISSN 2410-0595 (Print)

A Robust Watermarking Technique Using Video Compression Standard H.264 Integer Discrete Cosine Transformation

Ahmed Al-Gindy

School of Engineering and Technology, AlDar Universiy College, Dubai, UAE

[1]*indri_mtc@yahoo.com*

ABSTRACT

This paper presents a robust watermarking algorithm for copyright protection of digital images. The proposed algorithm uses 4×4 block-based integer discrete cosine transformation (intdct) used in the video compression standard h.264. The intDCT is used rather than the conventional DCT. The most significant advantage of this transform is that it is free from any floating-point or fixed-point multiplication required by the original dct and all operations can be carried out with integer arithmetic, without loss of accuracy. The 24 bits/pixel rgb images are used and the watermark is placed on the green channel of the rgb image. Handwritten signature has been used as a watermark and embedded into the host image using different watermarking strengths. Comparison between the DCT and intDCT algorithms is presented. The algorithm's performance is evaluated using attack tools. Experimental results show that this proposed algorithm can survive attacks such as jpeg compression, common signal processing attacks, cropping, and scaling.

Keywords: *Integer dct, Video Compression Standard H.264, Image Watermarking*.

1 INTRODUCTION

Digital multimedia has witnessed an extreme growth during the last decade due to the advances of computer technology, efficient storage, ease of manipulation and transmission and growth of high speed internet connection. Unfortunately, this made the work of the pirates and hackers easier, since it enables easy modifications and reproduction of digital files (video, audio and images). Hence, the need to develop counter techniques to protect data against duplication and copyright infringements. Broadcasting, medical, satellite and forensic digital images require identity authentication and content verification, to detect forgeries and tampered image blocks. Amongst numerous available techniques, digital watermarking is a means used to identify owners of files and validate their copyrights. Basically, a watermark is a digital signal mainly characterized by robustness against various forms of attacks. Digital watermarks represent secret messages, stamps, or contact details, related to the owner or distributor of the original image.

Digital watermark strategies fall into two major categories: spatial-domain and transform-domain techniques. In spatial domain techniques, one of the simplest methods of inserting a digital watermark in a still image is called Least-Significant-Bit (LSB) Watermarking [1]. However, this technique has relatively low information hiding capacity and can be easily erased by lossy image compression. Watermarks can also be inserted in the frequency domain by applying transforms like Fast Fourier Transform (FFT) [2], Discrete Cosine Transform (DCT) [3], and Discrete Wavelet Transform [4] and then altering the values of selected transform coefficients to store the watermark in still images. Watermarking in the frequency domain is more robust than watermarking in the spatial domain [5], because the watermark information can be spread out to the entire image.

2 LITERATURE REVIEW

The robustness of watermarking techniques lies in its survival against attacks. The watermark is considered robust if it cannot be impaired without rendering the attacked data useless. There are some well-known attacks that are carried out on watermarking systems [6]. The are powerful attack tools [7,8] such as, Strimark, inZign and attachmark for generating attacks on watermarking algorithms for evaluation purposes.

Authors in [9] compared the performance of 4x4 Integer DCT with the conventional 8x8 DCT on the basis of computational time and PSNR. The 4x4 integer DCT was 0.30ms times faster than the conventional 8x8 DCT.

Authors in [10] proposed a new watermarking system by using the technologies of 4x4 Integer Discrete Cosine Transform (IntDCT) and adaptive AC estimation. They use 4x4 IntDCT transform to reduce blocking artifacts caused from 8x8 DCT transform with AC estimation scheme to predict AC (1,1) as error-checking code. Using the error-checking code, we can enhance the robustness of watermark.

A proposed 2-dimensional integer DCT based approach is presented in [11]. The paper used the bit-shift operation successfully in reversible watermarking for images. They compared their research with the authors from Philips Research proposed a reversible image watermarking scheme [12] which also exhibits high capacity, but this scheme is not based on bit-shift operations.

Other techniques were based on embedding many copies of the same watermark into the host image. Saeed and Kunhu in [13] proposed three algorithms to secure satellite images captured by DubaiSat-1 by embedding a gray logo of Emirates Institution for Advanced Science and Technology (EIAST). All three algorithms were based on embedding two bits of the binary logo (once, twice, thrice) in each 8x8 DCT blocks of the host green channel. The Odd/Even insertion method was used as the embedding technique. Results showed that each method was characterized by surviving particular attacks. Method I was robust against flipping and noise attacks. Method II was robust against resize and rotation. Finally, Method III resulted in a lower PSNR compared to the first two methods.

Several attempts were made to design algorithms that would survive geometric attacks such as rotation, scaling, and translation. Kunhu and Al-Ahmed in [14] proposed a composite algorithm which applied multi-embedding watermarking techniques to color satellite images. The index color map was embedded in the frequency domain using DCT coefficients of the image. A hash function, applied to the DCT watermarked image, was embedded using an ‘SHA256’ 64 Hex unique hash key in the least significant bits of the spatial domain. The proposed algorithm showed excellent results for hiding the embedded watermark and survived image geometric attacks.

Wei et al in [15] proposed a genetic algorithm (GA) based on Discrete Cosine Transform (DCT). The watermark was embedded in the modified AC coefficients of the host image in the DCT domain. The insertion and extraction processes were engaged to speed up the genetic watermarking and to avoid loss of the watermark. The proposed GA was designed to be a robust and invisible algorithm. It showed good robustness

against watermark attacks and high reliability. Some algorithms used mobile phones as a platform to run their algorithms. Delgado-Guillen in [16] implemented watermarking algorithm using mobile computing platforms, Motorola MB511 mobile phone with a camera resolution of 3.1 megapixel and running Android 2.1 operating system. A digital watermark was retrieved after undergoing digital-to-analog and analog-to-digital conversion as well as rotation, scaling, and translation attacks.

3 INTEGER DCT WATERMARKING

The proposed watermarking technique uses the Integer DCT (IntDCT) which is used in H.264 video standard. The proposed technique applies block-based 4×4 IntDCT transformation to help reduce blocking artifacts caused by using traditional 8×8 DCT. IntDCT basically has the same properties as the original DCT, but there are some fundamental differences. First, it is an integer transform. All operations can be carried out with integer arithmetic, without loss of accuracy. The core part of the transform is free from multiplications. It only requires additions and shifts. It does not need floating-point and fixed-point multiplications required by DCT. This reduces the computational complexity and it is much easier in case of further hardware implementation. The host image is divided into 4×4 sub-blocks and is IntDCT transformed. So

$$F_K(u,v) = IntDCT\{S_K(i,j)\}, where\ 1 \leq k \leq N_{hb}$$

Where k is the host image block number where IntDCT will be applied and N_{hb} is the total number of the 4×4 sub-blocks in the host image. Mathematically, integer DCT can be derived from discrete cosine transforms and is described as:

$$F_{uv} = (C_f . S_{ij} . C_f^T) \otimes E_f$$

$Where\ by$:

$$C_f = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 2 & 1 & -1 & 2 \\ 1 & -1 & -1 & 1 \\ 1 & -2 & 2 & -1 \end{bmatrix}$$

$$E_f = \begin{bmatrix} a^2 & ab/2 & a^2 & ab/2 \\ ab/2 & b^2/2 & ab/2 & b^2/2 \\ a^2 & ab/2 & a^2 & ab/2 \\ ab/2 & b^2/4 & ab/2 & b_2/4 \end{bmatrix}$$

$$And\ a = 1/2 \quad , b = \sqrt{\frac{2}{5}}$$

Matrices S_{ij} and F_{uv} and are the input and output respectively. E_f is the post-scaling matrix which is incorporated in the quantization process while C_f is the transform matrix and C_f^T is the transpose. The operator $\otimes$ means multiplying the corresponding elements of two matrices.

The watermark information is embedded into the selected frequency coefficients where 8 bits are embedded in one 4×4 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* is embedded into the desired sub-block of the host image. Assume that *S(i,j)* represents the pixel of the G component of the RGB representation of the colour host image, *w(i,j)* represents the binary pixel of the watermark and

Fk (u,v)= IntDCT{ Sk (i, j)},
If w(i,j)=1 then

$$\mathrm{F(u,v)} = \begin{pmatrix} \Delta\, \mathrm{Q_e}\left(\frac{\mathrm{F_k(u,v)}}{\Delta}\right) & \mathrm{u,v} \in \mathrm{H_k} & 1 \leq \mathrm{k} \leq \mathrm{N_{HB}} \\ \mathrm{F_k\ (u,v)} & \mathrm{u,v} \notin \mathrm{H_k} & 1 \leq \mathrm{k} \leq \mathrm{N_{HB}} \end{pmatrix}$$

If w(i,j)=0 then

$$\mathrm{F(u,v)} = \begin{pmatrix} \Delta\, \mathrm{Q_o}\left(\frac{\mathrm{F_k(u,v)}}{\Delta}\right) & \mathrm{u,v} \in \mathrm{H_k} & 1 \leq \mathrm{k} \leq \mathrm{N_{HB}} \\ \mathrm{F_k\ (u,v)} & \mathrm{u,v} \notin \mathrm{H_k} & 1 \leq \mathrm{k} \leq \mathrm{N_{HB}} \end{pmatrix}$$

Where $1 \leq u, v \leq 8$, and Qe is the quantization to the nearest even number and Qo is the quantization to the nearest odd number, Δ is a scaling quantity and it is also the quantization step used to quantize either to the even or odd number. The 4x4 block is converted back to the spatial domain 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 represents a graphical presentation for the embedding steps.

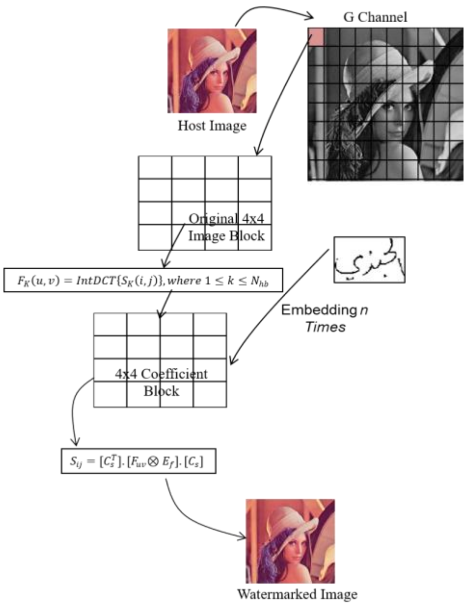

G Channel
Host Image
Original 4x4
Image Block
$F_K(u,v) = IntDCT\{S_K(i,j)\}, where\ 1 \leq k \leq N_{hb}$
الجندي
Embedding *n*
Times
4x4 Coefficient
Block
$S_{ij} = [C_s^T].[F_{uv} \otimes E_f].[C_s]$
Watermarked Image

Fig. 1. Graphical Presentation for Embedding Steps using IntDCT

The embedded information $w(i,j)$ can be extracted by performing block-based IntDCT transform for the watermarked host image and indicate the same coefficients of the host image that carries the 8 bits of the embedded watermarks using the same secret key in the initial scrambling operation. The Green component is divided into 4 × 4 blocks and IntDCT transformed for the recovery process. The process is inverse of the embedding process where each predefined frequency coefficient is quantized by Δ and rounded to the nearest integer. The extracted formula is defined as follows:

$$If\ Q\left(\frac{F_k(u,v)}{\Delta}\right)\ is\ odd\ then\ w(i,j) = 0$$

$$If\ Q\left(\frac{F_k(u,v)}{\Delta}\right)\ is\ even\ then\ w(i,j) = 1 \quad \text{.....(3)}$$

Where Q is rounded to the nearest integer. Δ the scaling quantity is the same as the one used in the embedding process. The inverse intDCT converts a frequency domain signal back to special domain [13]. Mathematically, It can also be described as:

$$S_{ij} = [C_s^T].[F_{uv} \otimes E_f].[C_s]$$

$$C_s = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1/2 & -1/2 & -1 \\ 1 & -1 & -1 & 1 \\ 1/2 & -1 & 1 & -1/2 \end{bmatrix}$$

$$E_s = \begin{bmatrix} p & q & p & q \\ q & r & q & r \\ p & q & p & q \\ q & r & q & r \end{bmatrix}$$

$$And\ \ p = 1/4, \quad q = \frac{1}{\sqrt{10}}, \quad r = 2/5$$

4 SIMULATION AND RESULTS

The watermarked image imperceptibility has been evaluated among different images, the Peak Signal to Noise Ratio (PSNR) and Structural Similarity Index measurement (SSIM) have been calculated between the original image and the watermarked image. Table 1 lists the results for the imperceptibility quality for the proposed algorithm at embedding strength of Δ = 16. While, Table 2 lists the results for the imperceptibility quality for the proposed algorithm at embedding strength of Δ = 24.

Table 1 Quality of the watermarked images at Δ = 16

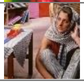
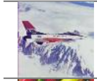
Image	**Description**	**PSNR at Δ = 16**	**SSIM at Δ = 16**
	Leena	57.5	0.9895
	Baboon	53.1	0.9815
	F16	51.1	0.9785
	Pepper	59.1	0.9925
	Barbara	50.2	0.9735

Table 2 Quality of the Watermarked Images at Δ = 24

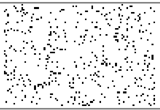
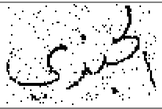
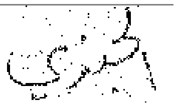
Image	**Description**	**PSNR at Δ = 24**	**SSIM at Δ = 24**
	Leena	53.5	0.9895
	Baboon	50.3	0.9815
	F16	48.5	0.9785
	Pepper	56.5	0.9925
	Barbara	47.5	0.9735

The handwritten signature watermark is embedded into Lena image at several watermarking strengths Δ. Normalized Cross-Correlation evaluation is used to measure similarities between original and extracted watermark images. In Table 3, Δ is set at 16 and 24 respectively. The robustness of the proposed method is evaluated using various types of attacks such as filters, geometric, and JPEG compression. In order to visually prove results, samples of simulation outputs depicted at Table 4 when the watermarking strength Δ=16 and Table 5 when the watermarking strength Δ=24.

Table 3 NC Values against Different Attacks

Attacks at Δ = 16		Attacks at Δ = 24	
Attacks	**NC**	**Attacks**	**NC**
JPEG 25	0.9404	JPEG 25	0.9870
JPEG 50	0.9682	JPEG 50	0.9914
JPEG 75	0.9909	JPEG 75	0.9988
S&P, 0.005	0.9721	S&P, 0.005	0.9766
S&P, 0.01	0.9216	S&P, 0.01	0.9363
Median [3×3]	0.9894	Median [3×3]	0.9975
Median [5×5]	0.9421	Median [5×5]	0.9668
Scale 0.5%	0.9928	Scale 0.5%	0.9989
Scale 2.0%	1	Scale 2.0%	1
Wiener [3×3]	0.9944	Wiener [3×3]	0.9996
Cropping Vertical 50%	0.9975	Cropping Vertical 50%	0.9979
Average [3×3]	0.9719	Average [3×3]	0.9955
Average [5x5]	0.9080	Average [5x5]	0.9455
S&P noise, *d*=0.02 + Median 3×3	0.9835	S&P noise, *d*=0.02 + Median 3×3	0.9977

Table 4 Extracted Watermarks after Different attacks at Δ = 16

Watermark Size 96 x 64 at Δ = 16		
		
JPEG 25	JPEG 50	JPEG 75

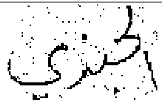
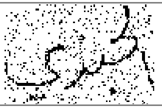
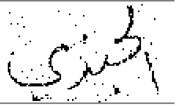
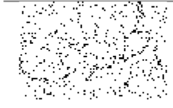
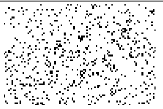
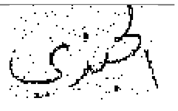
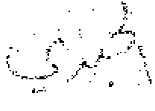
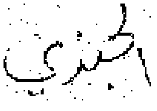
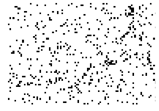
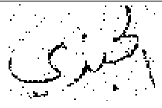
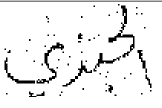
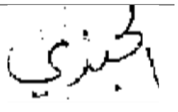
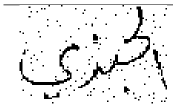
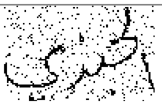
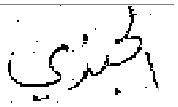
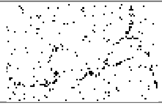
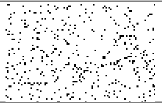
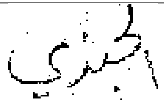
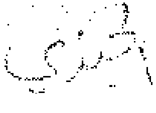
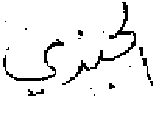
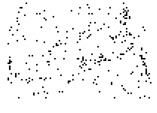
		
S&P, 0.005	S&P, 0.01	Median Filter
		
Median Filter [5×5]	Average Filter [5×5]	S&P noise, *d*=0.02+
		
Cropping50%	Scale down	Wiener Filter

Table 5 Extracted Watermarks after Different attacks at Δ = 24

Watermark Size 96 x 64 at Δ = 24		
		
JPEG 25	JPEG 50	JPEG 75
		
S&P, 0.005	S&P, 0.01	Median Filter
		
Median Filter [5x5]	Average Filter [5x5]	S&P noise, *d*=0.02+
		
Cropping50%	Scale down	Wiener Filter

Experimental results show that the proposed algorithm becomes more robust against attacks when higher water strengths are utilized. However, on the other hand this will reduce the invisibility qualities of the watermarked images.

5 CONCLUSION

The H.264 video compression standard integer DCT has been implemented for image watermarking. The proposed technique takes advantage of the integer arithmetic operation, without loss of accuracy. The core part of the IntDCT transform is free from multiplications. It only requires additions and shifts. It does not need floating-point and fixed-point multiplications required by the traditional DCT method. The proposed algorithm survives several image processing attacks such as additive noise, rescaling, cropping and JPEG compression. For JPEG compression, the watermark was still recognizable even at the low-quality factor of 25 when the watermarking strength allocated at Δ=24. For future work, the proposed watermarking algorithm using the IntDCT transform can be extended to video watermarking based on the H.264 standard.

6 REFERENCES

[1] R G. van Scbyndel, A. 2. Tirkel, and C. F. Shamoon,"Secure spread specbum watermarking for multimedia,"IEEE Trans. Image Processing, vol. 6, pp. 1673-1687, Dec.1997.

[2] C.-W. Tang and EL-M. Hang "A feature-based robust digital image watermarking scheme," IEFE Transactions on Signal Processing, vol. 51, no. 4, pp. 950-959, Apr.2003.

[3] H. Zhang, L.Z. Cai, X.F. Meng, X.F. Xu, X.L. Yang, X.X. Shen and G.Y. Dong, "Image watermarking based on an iterative phase retrieval algorithm and sine–cosine modulation in the discrete-cosine-transform domain", Optics Communications, In Press, Uncorrected Proof, Available online 4 May 2007.

[4] Santa Agreste, Guido Andaloro, Daniela Prestipino and Luigia Puccio, "An image adaptive, wavelet-based watermarking of digital images", Journal of Computational and Applied Mathematics, In Press, Corrected Proof, Available online 1 February 2007.

[5] Al-Gindy, A., Al-Ahmad, H., Qahwaji, R., & Tawfik, A. (2008, August). A novel blind Image watermarking technique for colour RGB images in the DCT domain using green channel. In Communications, Computers and Applications, 2008. MIC-CCA 2008. Mosharaka International Conference on (pp. 26-31). IEEE.

[6] Taha Dawood Jasim, "Combined Robust And Fragile Watermarking Algorithms For Still Images", PhD Thesis, Faculty of Engineering and Informatics, 2014.

[7] S. Voloshynovskiy, S. Pereira, and T. Pun, "Attacks on Digital Watermarks: Classification, Estimation-Based Attacks, and Benchmarks",," in IEEE Communications Magazine, 2001, pp. 118-26.

[8] Ahmed Al-Gindy," Evaluation Tool for Generating Attacks on Watermarking Algorithms", in the IJCSNS International

Journal of Computer Science and Network Security, volume 16-No.6, 2016.

[9] Y. Muhammd K.E Khan, M.S Beg, “Performance Evaluation Of 4x4 DCT Algorithms for Low Power Wireless Applications” First International Conference On Emerging Trends In Engineering and Technology, 2008.

[10] Eugene Lai, Ching-Tang Hsieh and Kuo-Ming Hung, “Blind watermarking technique Based on Integer Discrete Cosine Transform and AC Prediction”, in the Proceedings of the 8th WSEAS International Conference on Automation and Information, Vancouver, Canada, June 19-21, 2007.

[11] Bian Yang, Martin Schmucker, Wolfgang Funk, Christoph Busch, Shenghe Sun, “Integer DCT-based Reversible Watermarking for Images Using Companding Technique”, in the Proceedings of SPIE - The International Society for Optical Engineering, 2004.

[12] A. Leest, M. Veen, and F. Bruekers, “Reversible image watermarking”, IEEE Proceedings of ICIP’03, vol.2, pp.731-734, September 2003.

[13] Saeed AL-Mansoori and Alavi Kunhu , “Robust Watermarking Technique based on DCT to Protect the Ownership of DubaiSat-1 Images against Attacks”, in the IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.6, 2012.

[14] Alavi Kunhu and Hussain Al-Ahmad , “Multi Watermarking Algorithm Based on DCT and Hash Functions for Color Satellite Images”, in the 9th IEEE International Conference on Innovations in Information Technology - Innovations, 2013.

[15] Z. Wei , J. Dai , J. Li, “Genetic Watermarking Based on DCT Domain

[16] Techniques”, Electrical and Computer Engineering, 2006. CCECE '06. Canadian Conference on, Canada, pp. 2365 – 2368, May, 2006.

[17] Delgado-Guillen, L. A., Garcia-Hernandez, J. J., & Torres-Huitzil, C. (2013, August). Digital watermarking of color images utilizing mobile platforms. InCircuits and Systems (MWSCAS), 2013 IEEE 56th International Midwest Symposium on (pp. 1363-1366). IEEE.