ISSN: 0976-9102 (ONLINE)
DOI: 10.21917/ijivp.2015.0154

AN EFFICIENT ROBUST IMAGE WATERMARKING BASED ON AC PREDICTION TECHNIQUE USING DCT TECHNIQUE

Gaurav Gupta[1], Amit Mahesh Joshi[2] and Kanika Sharma[3]
[1, 3]Department of Electronics and Communication Engineering, National Institute of Technical Teachers Training and Research, Chandigarh, India
E-mail: [1]gauravgupta110688@gmail.com, [3]kanikasharma80@gmail.com
[2]Department of Electronics and Communication Engineering, Malaviya National Institute of Technology, India
E-mail: [2]amjoshi.ece@mnit.ac.in

Abstract

The expansion of technology has made several simple ways to manipulate the original content. This has brought the concern for security of the content which is easily available in open network. Digital watermarking is the most suitable solution for the defined issue. Digital watermarking is the art of inserting the logo into multimedia object to have proof of ownership whenever it is required. The proposed algorithm is useful in authorized distribution and ownership verification. The algorithm uses the concept of AC prediction using DCT to embed the watermark in the image. The algorithm has excellent robustness against all the attacks and outperforms the similar work with admirable performance in terms of Normalized Correlation (NC), Peak Signal to Noise Ratio (PSNR) and Tamper Assessment Function (TAF).

Keywords:

Blind Retrieval, Digital Rights Management, Error Correction, Invisibility, Robustness

1. INTRODUCTION

The usage of internet has increased tremendously over the past decade. The multimedia content is transferred frequently over the network. The growth of the technology has simplified sharing of the digital images, videos or any other legal document. But at the same instance, the threat of unauthorized access and distribution of such multimedia content is raised. The problem of unauthorized access can be solved by adding digital signature with the document. By introducing the digital signature, the authorized user can only able to access the document. However, the authorized user may not have the ownership of the same. Thus, for this purpose, a watermark of the authorized distributor is added to the image. Watermarking may be of any type such as visible/invisible, blind/non-blind, fragile/robust/semi-fragile etc. The watermark may be any text, image or logo of the distributor which acts as the ownership information of the valid or authorized distributor. The watermark is embedded such that it should not distort the host image and should also be invisible to the observer. The watermark is extracted from the host image in order to identify the authorized distributor. If the extracted watermark correlates the original watermark within some acceptable tolerance limit then the image is authenticated otherwise it is not. The image has to withstand some potential attacks once it has been transmitted over the noisy channel. The several common attacks are JPEG compression, salt-pepper/gaussian noise and filtering. The watermarking algorithm should be designed to have substantial robustness against all forms of attacks. One application for watermarking algorithm is in military where communication takes place over highly noisy channel i.e. link may be temporary, low bandwidth radio set up etc. Sometimes, it may not be possible to exact the watermark it its original form. The error correcting codes are inserted in order to minimize the Bit Error Rate (BER). Another application of digital watermarking scheme is in Digital Rights Management (DRM) systems. It addresses the issue related to content identification, ownership, storage and distribution rights of digital content [4-6]. DRM systems also handles issues related to Intellectual Property Rights (IPR) management. The main objective of this research is to design robust image watermarking algorithm for ownership and distribution rights. The proposed scheme is based on modification of DCT coefficients and AC prediction of few AC coefficients [7].

The paper is organized as follows: Section 2 describes the literature study of the existing watermarking algorithm. Section 3 explains the steps for the proposed algorithm. Section 4 discusses the results which are compared with similar previous algorithms and Section 5 concludes the research work.

2. LITERATURE SURVEY

The literature available contains various watermarking algorithms which are robust to various noise attacks and JPEG compression. The robustness of the algorithm is a measure of how accurately it is able to retrieve the watermark when the watermarked image is attacked by noise or JPEG compression. Factors like Normalized correlation (NC) and Tamper Assessment Function (TAF), discussed in Section 4, are used to measure the robustness of the algorithm. The frequency domain watermarking algorithms are based on orthogonal transforms like Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) or Singular Value Transform (SVD). Chinmayee et al. [8] utilized the correlation between the two DCT coefficients of the adjacent 8x8 blocks at the same position. The DCT coefficient is modified to bring the difference from the adjacent block coefficient in the specified range. Patra et al. [9] proposed a Chinese Remainder Theorem (CRT) based digital watermarking technique in DCT domain which has the robustness to various attacks. This technique is useful for copyright protection and authentication of multimedia data. The proposed technique works better than the SVD based watermarking technique in terms of TAF and Peak Signal to Noise Ratio (PSNR). The above algorithms involve modifying the DC or low frequency coefficients of the original image. Such process modifies the energy content of the image and this may result in the change in the perceptibility to the user. To cope with such a problem, a novel algorithm was proposed by Liu et al. [10] to embed the watermark in the high frequency coefficient after applying the Quadratic DCT transform. It leads to a little change in the energy content of the image which suggests less degradation in the perceptibility to the viewer. Local average moment is used by Wu and Ren which is used to modify the selected AC coefficients to embed the watermark. A pseudo random number and a secret key is used to select the AC coefficient whose value is to be modified. A robust hybrid SVD-DCT based watermarking algorithm was proposed by Li et al. [12]. SVD is applied to cover the image blocks and then DCT is applied on macro blocks comprised of the first singular values (SV) of each image block. The watermark bits are embedded into the high frequency band of SVD-DCT block by imposing a particular relationship between some pseudo-randomly selected pairs of the DCT coefficients. Joshi et al. [13] presented the dual domain watermarking scheme for image copy right application. The proposed method is used to embed the watermark in both spatial domain and frequency domain. It has advantages of low complexity as well as acceptable robustness against some standard attacks. The same author further developed for video watermarking algorithm which is suited to H.264 video standard [14]. It uses the concept of Integer Discrete Cosine Transform (Int-DCT) to have better speed with low complexity. The algorithm is implemented on VIRTEX-4 FPGA to verify the real time performance.

3. PROPOSED WATERMARKING ALGORITHM

The proposed scheme involves embedding the watermark payload into the DC coefficients of each block and modification of *AC*(1, 1) coefficient using AC prediction technique.

3.1 WATERMARK EMBEDDING

The following steps describe the working of algorithm for embedding the watermark bits in the original image.

1. Divide the original image *I*(*i*, *j*) into 8 × 8 pixels blocks $I\_B_q(x, y)$, where, $I\_B_q(x, y)$ represents the q^{th} block and *q* is in the range $1 \le q \le k$. The size of original image is $M \times N$ pixels. The number of pixel blocks is given by Eq.(1).

$$\text{no. of } 8 \times 8 \text{ blocks } (k) = \frac{M * N}{8 * 8} \tag{1}$$

2. Calculate the DCT transform of each block. The transformed 8 × 8 block of image is given by *I_BTq*(*u*, *v*).

$$I\_BT_q(u,v) = DCT(I\_B_q(x,y)) \tag{2}$$

where, $1 \le q \le k$, $1 \le x, y \le 8$ and $I\_BT_q(u, v)$ represents the DCT transform of q^{th} block $I\_BT_q(x, y)$.

3. The binary watermark image is converted into an array of single row. The $m \times n$ watermark image consists of $m * n$ bits. Replicate each watermark bit four times at every position. Suppose the watermark bits *W*(*n*) are 11001101. The first bit of the sequence is '1'. Now, replicate this bit four times '1111'. The second bit is '0'. Replicate this bit again four times '0000'. In this way, the resulting watermark sequence *W_R*(*q*) becomes '11111111000000001111111100001111'. Thus a single watermark image is embedded four times in the original image. In case, if one of the blocks is attacked then it is possible to recover the embedded bit from the other blocks. This increases the robustness of the algorithm, where, *W_R* represents the repeated watermark sequence.

4. Embed the repeated sequence of watermark bits into the DC coefficients according to the following rule.

If *W_R*(*q*) = 1,

$$I\_BT_q'(u,v) = \begin{cases} \alpha * F_0\left(\dfrac{I_{BT_q}(u,v)}{\alpha}\right) & \text{if } u,v=0 \\ I\_BT_q(u,v) & \text{if } u,v \ne 0 \end{cases} \tag{3}$$

Else,

$$I\_BT_q'(u,v) = \begin{cases} \alpha * F_1\left(\dfrac{I_{BT_q}(u,v)}{\alpha}\right) & \text{if } u,v=0 \\ I\_BT_q(u,v) & \text{if } u,v \ne 0 \end{cases} \tag{4}$$

where, $F_0(x)$ indicates converting the value of *x* to most approximate odd number and $F_1(x)$ indicates converting the value of *x* to most approximate even number. α is the parameter of quantization. This parameter plays a vital role in increasing the robustness of the algorithm. The value of α is selected in the range $15 < \alpha < 35$.

5. Predict the *AC*(1, 1) coefficient using AC prediction technique used employed in [7].

$$AC(1,1) = \lambda * (DC1 + DC9 - DC3 - DC7) \tag{5}$$

The value of λ is modified in our proposed algorithm. The value of λ is chosen to be 0.35.

6. Apply the inverse DCT to each modified block *I_BTq*(*u*, *v*) to obtain the watermarked image *I_W*(*i*, *j*), where, *I_BTq*(*u*, *v*) represents the q^{th} block after *AC*(1, 1) modification.

The above mentioned procedure is shown in Fig.1.

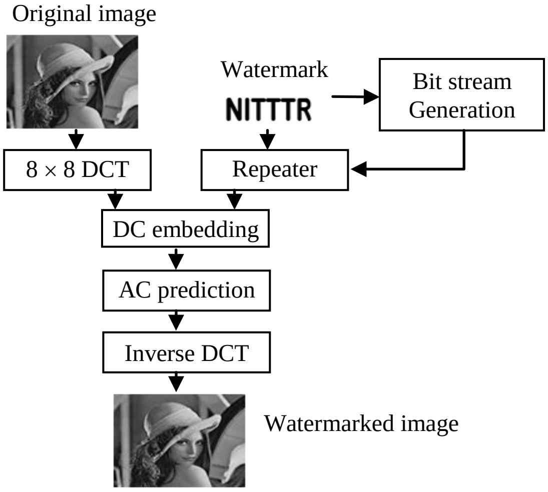

Fig.1. Procedure for watermark embedding

3.2 WATERMARK RETRIEVAL

The following steps describe the procedure for retrieving the watermark from the watermarked image:

1. The watermarked image *I_W*(*i*, *j*) is divided into k non-overlapping blocks of size 8 × 8. Each block is denoted by $I\_WB_q(x, y)$
2. Perform DCT transform of each 8 × 8 block. Each DCT transformed block is denoted by *I_WBq*(*u*, *v*)

$$I\_WBT_q(u,v) = DCT(I\_WB_q(x,y)) \quad (6)$$

3. Retrieve the repeated watermark bits sequence from the DC coefficients of each block as given by Eq.(7) and Eq.(8).

$$\text{if } F\left(\frac{I_{WBT_q}(0,0)}{\alpha}\right) = \text{even then } W\_R'(q) = 0 \quad (7)$$

$$\text{if } F\left(\frac{I_{WBT_q}(0,0)}{\alpha}\right) = \text{odd then } W\_R'(q) = 1 \quad (8)$$

   where, *F*(*x*) is a round function. In this way, calculate the complete bit sequence W_R'.
4. Calculate the *AC*(1,1) in every block according to Eq.(5). It is denoted by *AC*′(1, 1). Now, compare $I\_WBT_q(1, 1)$ with *AC*′(1, 1). If the difference of these two values occurs to be larger than a pre-determined threshold η, then the block is attacked otherwise not. The value of threshold η is given by Eq.(9).

$$\eta = abs(AC'(1,1) - I_{WBT_q}(1,1)) \quad (9)$$

5. To extract the original watermark bits sequence *W*′ from the repeated sequence *W_R*′, select one bit from *W_R*′ and copy to *W*′ and drop next three bits. In this way, carry out the same procedure for the entire bits sequence available in *W_R*′.
6. Convert the extracted original watermark series *W*′ into watermark image.

The Fig.2 shows the procedure of retrieving the watermark.

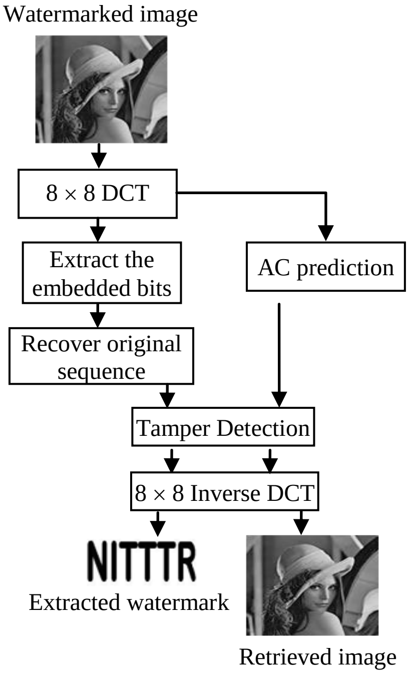

Fig.2. Procedure for extracting the watermark

4. RESULTS AND DISCUSSIONS

The original image is taken to be 512 × 512 in size and the watermark is a binary image of size 32 × 32. For testing this algorithm, images of Lena, Baboon, Cameraman and pepper are used. Fig.3 shows the watermark images and Fig.4 shows the host images.

(a) (b)

Fig.3. (a) & (b) Watermark payload

(a) Cameraman (b) Baboon (c) Peppers (d) Lena

Fig.4. Host images

The PSNR, MSE and SF values are calculated and are shown in Table.1 in order to verify the proposed watermarking algorithm. The value of PSNR is coming to be more than 40dB in every case which implies the validity of the proposed algorithm. The value of SF is coming nearly 1 in every case which shows that watermark is successfully retrieved in each case without distortion.

The value of the parameter of quantization α is taken in the range $20 \le \alpha \le 30$. This parameter affects the PSNR values. This parameter also plays a vital role in increasing the robustness of the algorithm. Increasing the value of α decreases the PSNR but increases the SF when the image is attacked or JPEG compressed. Optimizing this value according to our need is an important task. The value of λ used in AC prediction is another factor affecting the PSNR values of the algorithm. After examining the effect of different values of λ on the PSNR values, it is observed that for $\lambda = 0.35$, maximum PSNR is calculated. The value of threshold η varies with the requirement of every application. If every minor attack is to be detected, then the value of η is taken in the range $5 \le \eta \le 10$ and if major attacked area is to be highlighted, then $11 \le \eta \le 30$.

The measure of distortion occurred to host image done due to watermarking process is given by MSE and Peak Signal to Noise Ratio (PSNR). MSE is defined by Eq.(10) and PSNR is defined by Eq.(11) for an 8-bit gray scale image.

$$MSE = \frac{1}{M*N}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}\left(f'(x,y) - f(x,y)\right)^2 \quad (10)$$

$$PSNR(dB) = 20\log_{10}\frac{255}{MSE} \quad (11)$$

where, *M* × *N* is the size of the host image. *f*(*x*, *y*) is the original host image and *f*′(*x*, *y*) is the watermarked image. Another parameter which shows how successfully watermark is retrieved from the watermarked image is Normalized Correlation (*NC*). This parameter is given by Eq.(12).

$$NC = \frac{\sum_{i=0}^{N-1} w * w'}{\sum_{i=0}^{N-1} w^2} \tag{12}$$

where, w is the original watermark and w' is the retrieved watermark. N is the size of the watermark. For two identical images, the value of SF and NC is nearly 1. However, the value of SF can be tolerated up to 0.80. Another parameter used to test the robustness of the algorithm is Tamper Assessment Function (TAF) which is given by Eq.(13).

$$TAF(\%) = \frac{1}{M * N}\left[\sum_{i=0}^{N-1} w \oplus w'\right] * 100 \tag{13}$$

where, ⊕ is XOR operation between $w(i)$ and $w'(i)$ bits. For two identical images, the value of TAF should be 0. The smaller the values of TAF, the more similar are the images. For testing the robustness of the proposed algorithm, following attacks are considered: JPEG compression, Median Filtering (3 × 3), Gaussian noise (mean = 0, variance = 0.001) and salt and pepper noise (density = 0.01). Table.2 and Table.3 give the comparative analysis of the experimental values of TAF and SF with the existing algorithms.

The experimental results of the proposed algorithm show an outstanding robustness against JPEG compression as compared to [8]-[12]. The proposed algorithm also shows improved robustness against median filtering and Gaussian noise attacks. But, there is slight degradation in robustness against salt & pepper noise attack. However, the NC and TAF are in acceptable range.

5. CONCLUSION

Proposed algorithm is based on the concept of repeating the sequence of watermark bits to improve the robustness. It is also used to detect the tampering with AC prediction technique. The performance of the algorithm is simulated on MATLAB platform. The obtained values of Table.1, Table.2 and Table.3 confirm the ability of algorithm against various channel attacks. The algorithm is also compared with previous work and shows the commendable achievement in performance.

Table.1. PSNR, MSE and SF for 512 × 512 original and watermarked images

Watermark image	**512 × 512 Host image**	**MSE**	**PSNR (dB)**	**Normalized Correlation (NC)**
NITTTR	Lena	5.0758	41.0758	1
MNIT	Lena	5.0963	41.0587	1
NITTTR	Cameraman	6.0643	40.3030	1
MNIT	Cameraman	5.9732	40.3688	1
NITTTR	Baboon	6.5348	40.0046	0.9927
MNIT	Baboon	6.5467	40.0097	0.9992
NITTTR	Peppers	4.2035	41.8946	1
MNIT	Peppers	4.1611	41.9387	1

Table.2. Comparative Analysis of NC under different attacks for different algorithms

Algorithm	**JPEG compression (50%)**	**Median Filtering (3 × 3)**	**Gaussian noise (mean = 0, variance = 0.001)**	**salt and pepper noise (density = 0.01)**
Proposed algorithm	0.9949	0.9834	0.8978	0.7752
Chinmayee et al. [8]	0.8847	0.9118	0.8816	0.8112

Table.3. Comparative Analysis of TAF under different attacks for different algorithms

Algorithm	**JPEG compression**	**Median Filtering (3 × 3)**	**Gaussian noise (mean = 0, variance = 0.001)**	**salt and pepper noise (density = 0.01)**
Proposed algorithm	0.3926	1.4648	9.7656	22.8561
Chinmayee et al. [8]	17.21	8.8710	11.391	18.19
J. C. Patra et al. [9]	10	Not available	16.53	Not available

REFERENCES

[1] Thomas H. Crystal, Astrid Schmidt – Nielsen and Elaine Marsh, “Speech in noisy environments (SPINE) adds new dimension to speech recognition R&D”, *Proceeding of the Second International Conference on Human Language Technology Research*, pp. 212–216, 2002.

[2] Rita Singh, Michael L. Seltzer, Bhiksha Raj and Richard M. Stern, “Speech in noisy environments: robust automatic segmentation, feature extraction, and hypothesis combination”, *Proceedings of International Conference on Acoustics, Speech and Signal Processing*, 2001.

[3] R. Naskar and R. S. Chakraborty, “Performance of reversible digital image watermarking under error-prone data communication: a simulation-based study”, *IET Image Processing*, Vol. 6, No. 6, pp. 728-737, 2012.

[4] Sabu Emmanuel and Mohan Kankanhalli, “A digital rights management scheme for broadcast video”, *Multimedia Systems*, Vol. 8, No. 6, pp. 444–458, 2003.

[5] Deepa Kundur and Kannan Karthik, “Video fingerprinting and encryption principles for digital rights management”, *Proceedings of the IEEE*, Vol. 92, No. 6, pp. 918–932, 2004.

[6] S.P. Mohanty, E. Kougianos and N. Ranganathan, “VLSI architecture and chip for combined invisible robust and fragile watermarking”, *IET Computer and Digital Techniques*, Vol. 1, No. 5, pp. 600–611, 2007.

[7] C. A. Gonzales, L. Allman, T. Mccarthy, A. N. Akansu and P. Wendt, “DCT coding for motion video storage using adaptive arithmetic coding”, *Signal Processing: Image Communication*, Vol. 2, No. 2, pp. 145-154, 1990.

[8] Chinmayee Das, Swetalina Panigrahi, Vijay K. Sharma and Kamalakanta Mahapatra, “A novel blind robust image

watermarking in DCT domain using inter-block coefficient correlation", *International Journal of Electronics and Communications*, Vol. 68, No. 3, pp. 244-253, 2014.

[9] Jagdish C. Patra, Jiliang E. Phua and Cedric Bornand, "A novel DCT domain CRT-based watermarking scheme for image authentication surviving JPEG compression", *Digital Signal Processing*, Vol. 20, No. 6, pp. 1597–1611, 2010.

[10] Wei Liu, Shuiyuan Yu and Xuan Wang, "A Robust Digital Image Watermarking Algorithm Based On Quadratic DCT Transform", *Proceedings of 3rd International Conference on System Science, Engineering Design and Manufacturing Informatization*, Vol. 1, pp. 133-137, 2012.

[11] Wen-Chuan Wu and Guang-Ruei Ren, "A DCT-Based Robust Image Watermarking Using Local Moment", *Proceedings of 3rd International Conference on Data Mining and Intelligent Information Technology Applications*, pp. 122-126, 2011.

[12] Zhen Li, Kim-Hui Yap and Bai-Ying Lei, "A New Blind Robust Image Watermarking Scheme In SVD-DCT Composite Domain", *Proceedings of 18th IEEE International Conference on Image Processing*, pp. 2757-2760, 2011.

[13] A. M. Joshi and A. Darji, "Efficient dual domain watermarking scheme for secure images", *International Conference on Advances in Recent Technologies in Communication and Computing*, pp. 909-914, 2009.

[14] A. M. Joshi, R. M. Patrikar and V. Mishra, "Design of low complexity video watermarking algorithm based on Integer DCT", *International Conference on Signal Processing and Communications*, pp. 1-5, 2012.

[15] Amit Joshi, Vivekanand Mishra and R. M. Patrikar, "Real Time Implementation of Digital Watermarking Algorithm for Image and Video Application", *Watermarking*, Vol. 2, pp. 65-91, 2012.