



AENSI Journals

Australian Journal of Basic and Applied Sciences

ISSN:1991-8178

Journal home page: www.ajbasweb.com

Content Based Watermarking Techniques using HSV and Fractal Dimension in Transform Domain

¹S. Radharani and ²Dr. M.L.Valarmathi¹Assistant Professor, Sree Narayana Guru College, Department of Computer Applications, S. Radharani, Coimbatore. India.²Associate Professor, Govt. College of Technology, Department. of Computer Science & Engineering, Dr. M.L. Valarmathi, Coimbatore. India.

ARTICLE INFO

Article history:

Received 12 January 2014

Received in revised form 20

March 2014

Accepted 25 March 2014

Available online 2 April 2014

Keywords:

Content based, DCT, DWT, Fractal Dimension, HSV

ABSTRACT

The central idea of the present paper is based on selecting the watermark information from the host image itself. For which, in this work, we select the fractal dimension as the feature of the host image. The proposed method uses three techniques namely DCT, DWT, combined DCT & DWT to embed the watermark by exploiting Fractal Dimension and Human Visual System (HVS), so that a trade-off between imperceptibility and robustness will be maintained. According to the experimentation results, in all the methods, the watermarked images could be recovered effectively. Our method is also useful to detect the tampered location in the watermarked image correctly.

© 2014 AENSI Publisher All rights reserved.

To Cite This Article: S. Radharani and Dr. M.L.Valarmathi., Content Based Watermarking Techniques using HSV and Fractal Dimension in Transform Domain. *Aust. J. Basic & Appl. Sci.*, 8(3): 112-119, 2014

INTRODUCTION

A digital watermarking is the process that can be used to hide a piece of information into a multimedia content, which is imperceptible to a human observer, but can be easily detected by a computer. The principle advantage is that the watermark is inseparable from the content.

Content based Digital Watermarking involves three major phases:

- (i) Watermark Creation,
- (ii) Watermark Embedding,
- (iii) Watermark Extraction.

Digital Watermarks may be a pseudo random sequence or a logo of a company or an image. Watermark embedding is done in the watermark carriers such as Discrete Cosine Transform (DCT) or Discrete Wavelet Transform (DWT), etc., of the original data resulting in watermarked data. The watermarked data can be compressed in order to reduce its size, corrupted by noise during its transmission through a noisy channel. It can be subjected to other common image processing operations such as filtering, histogram modification etc.

Digital watermark technology has developed extensively during the recent few years and is widely applied to protect the copyright of a digital image. A digital watermark is the information, embedded imperceptibly and robustly in the host data which cannot be removed. By adding a watermark signal to the host data the watermark signal is unobtrusive and secure in the signal mixture.

Background:

A new public content-based watermarking method for image authentication using ICA and DCT for gray scale images is proposed in (Dr. Latha Parameswaran and Dr. K. Anbumani, 2008). Based upon this paper, this project has been implemented for color images. Watermarks are embedded in the mid - frequency DCT coefficients. DCT is a widely used technique for watermarking (Francisco J. Gonzalez-Serrano, Harold Y. Molina-Bulla, and Juan J. Murillo-Fuentes, May 2001).

In (Dan Yu, Farook Sattar, and Kai-Kuang Ma, 2002) ICA is applied to the blocks of the host image and the watermark image. The least-energy independent components of the host are replaced by the high-energy independent components of the watermark image. For watermark extraction the demixing matrices of both the watermark and the host images are required.

Redundant DWT (RDWT) is used in (Stephane Bounkong, Boremi Toch, David Saad, and David Lowe, 2003). Many authors have worked on content-based watermarking for image authentication.

Corresponding Author: S. Radharani, Assistant Professor, Sree Narayana Guru College, Department of Computer Applications, S. Radharani, Coimbatore. India.

Choices of image features vary with techniques and directly influence the robustness of the method. Some techniques generate a random binary sequence to embed the watermark based on the features of the images (Eugene T. Lina, Christine I. Podilchuk, and Edward J. Delp, January 2000) and (Marc Schneider and Shih-Fu Chang, September 1996). In (Phen-Lan Lin, Po-Whei Huang, and An-Wei Peng, 2004), a localization based method has been presented to verify the integrity of the received image. In these techniques the host image is divided into a number of disjoint blocks and watermark is embedded in each of these blocks. To verify the authenticity of the received image, block wise authentication has been done.

In (Eugene T. Lina, Christine I. Podilchuk, and Edward J. Delp, January 2000), Image Authentication has been done using content-based watermarks. But these schemes do not embed the watermark in the image content; instead embed them in the image header. These techniques distort the host image before watermark embedding. In (Huijuan Yang and Alex C. Kot, December 2006) a watermarking technique based on the quad-tree is proposed. This scheme embeds a Gaussian sequence watermark into low-frequency band of the wavelet transform. In this technique, watermark is embedded into visually insensitive pixels in quad-trees.

In (Saeed K. Amirgholipour Ahmad R. Naghsh Nilchi, June 2009), a new robust digital image watermarking algorithm based on combined DWT-DCT Transformation is proposed. A binary watermarked logo is scrambled by Arnold cat map and embedded in certain coefficient sets of a 3-level DWT transformed of a host image.

Then, DCT transform of each selected DWT sub-band is computed and the PN-sequences of the watermark bits are embedded in the middle frequencies coefficients of the corresponding DCT block.

In extraction phase, the watermarked image, which maybe attacked, is pre-filtered by combination of sharpening and Laplacian or Gaussian filters, to increase the distinction between host image and watermark information. We describe an imperceptible and a robust combined DWT-DCT digital image watermarking algorithm.

The algorithm uses the combination of the DWT and the DCT to embed the watermark in digital image. Performance evaluation results show that combining the two transforms improved the performance of the watermarking algorithms that are based solely on the DWT transform (Ali Al-Haj, 2007). In (Emir Ganic Ahmet M. Eskicioglu Sep 2004) a hybrid scheme based on DWT and SVD (Singular Value Decomposition) is presented. (Rongrong Ni and Qiuqi Runa, 2006) proposes to determine the fractal dimension which specifically represents the content of the host image.

Most of the above authors supports in embedding a specified watermark. Mostly their aim is to give copyright protection and to require a lot of information about the host image for watermark extraction. Additional image mixtures are artificially created and then ICA is used as a blind source separation technique to separate the host image, the watermark, and the key.

In the method proposed here, fractal dimension represents the feature of the host image. No information about the host is required for watermark extraction. The proposed method aims in comparing on content-based watermarking techniques for color image. Generally this method uses Watermark generation procedure using Box-Counting method. The watermark embedding procedure uses three techniques namely DCT, DWT and Combined DCT & DWT. The same methods are used to extract the watermark values.

Objective:

This paper aims in proposing efficient comparison techniques to provide authentication for color image using human visual system based on fractal dimension watermarking. This is achieved by using techniques such as Box-Counting method for generating watermark value. The three techniques such as DCT, DWT and Combined DCT & DWT are used for embedding the watermark values and the same methods are used to extract the watermark values from the watermarked image.

The Fractal Dimension (FD) represents the feature of the host image. The spatial domain and frequency-domain watermarking techniques are used to embed the watermark values in various coefficients of the blocks. This authentication technique is robust against incidental image processing operations.

A. Watermark Generation using FD:

The following procedure is used to generate the watermark values for all the watermark techniques.

1. Segment the watermark image I of size $n \times n$ into blocks of size $m \times m$ resulting in K blocks.
2. Perform Box-counting method of each block treating each row of the block as a vector.
3. Compute the Fractal Dimension (FD) of the blocks using the formula shown below; this is the content-based feature watermark (w) of the block

$$FD = \frac{\log(\text{no. of self-similar pieces})}{\log(\text{magnification factor})}$$

4. Repeat steps 2 – 3 for computing the watermark for all the blocks. This set forms the watermark (W),
 $W = \{w_1, w_2, \dots, w_k\}$

B. Watermark Embedding:

Before applying embedding algorithm convert the host RGB image into HSV image.

Discrete Cosine Transform (DCT):

1. Compute DCT of each block of host image.
2. Select the mid-frequency coefficient at the chosen location (p, q) in each block.
3. Replace the chosen coefficient with the scaled watermark.
4. Perform inverse DCT.
5. Repeat steps 1–4 for all the blocks. The result is the watermarked image I^* .

Discrete Wavelet Transform (DWT):

1. Apply four times DWT (Haar wavelet) to decompose the host image and it will be segmented into four non-overlapping multi-resolution sub-bands: LL_4 , HL_4 , LH_4 , and HH_4 .
2. Replace mid component with scaled watermark of same sign.
3. Perform inverse DWT.
4. Repeat above steps for all the blocks. The result is the watermarked image I^* .

Combined DCT and DWT:

1. Apply four times DWT (Haar wavelet) to decompose the host image into four non-overlapping multi-resolution sub-bands: LL_4 , HL_4 , LH_4 , and HH_4 .
2. Compute DCT of sub band LH_4 .
3. Replace mid component with scaled watermark of same sign.
4. Perform inverse DCT and DWT.
5. Repeat above steps for all the blocks. The result is the watermarked image I^* .
Finally convert the watermarked image into RGB image.

C. Watermark Extraction and Authentication:**Discrete Cosine Transform (DCT):**

1. Perform watermark generation procedure of DCT on the received image and obtain the computed watermark.
2. Extract the embedded watermark from the chosen DCT coefficient.
3. This set forms the extracted watermark (W').
 $W' = \{w'_1, w'_2, \dots, w'_k\}$

Discrete Wavelet Transform (DWT):

1. Perform watermark generation procedure of DWT procedure on the received image and obtain the computed watermark.
2. Extract the embedded watermark from the chosen DWT sub band.
3. This set forms the extracted watermark (W').
 $W' = \{w'_1, w'_2, \dots, w'_k\}$

Combined DCT & DWT:

1. Perform watermark generation procedure of combined DCT & DWT procedure on the received image for all levels of DWT decomposition.
2. Extract the embedded watermark from the chosen DWT sub band and DCT coefficient.
3. This set forms the extracted watermark.

$$W' = \{w'_1, w'_2, \dots, w'_k\}$$

After extracting the watermark, calculate the block wise percentage difference (Δ) between the watermark values w^* and w' :

$$\Delta = (|W_i^* - W'_i| * 100 * \alpha) / \max \{W_i^*\}$$

where α is the embedding strength

In this method the percentage difference of the values corresponding to each block is used to detect any change in the block and thereby the authenticity of the image. If the difference is lesser than an experimentally chosen threshold value – then the entire image is considered authentic. If the difference of any block is greater than the threshold, then that block is identified as the tampered block and hence the image is unauthentic.

Results:**A. Selection of Parameters:**

Choosing a block size is based on the processing time and relevant features. After experimentation, a block size of 16 x 16 is chosen as it resulted in better PSNR value, computational time and better feature representation.

Selecting the suitable location to embed the watermark the proposed method uses the mid frequency coefficients, which ensures robustness.

To choose the appropriate value for the embedding strength (α), standard deviation (α_x) of the DCT coefficient values at that mid-diagonal location of all the blocks are obtained. Similarly the standard deviation α_w is obtained for the watermark. The value of embedding factor α is determined such that the watermark values are suitably scaled to have the same range of variation as that of the DCT coefficients.

$$\alpha = \alpha_x / \alpha_w$$

In this experimentation after computation the value is $\alpha = 0.517$.

The same method is applied for DWT and combined value of DCT & DWT methods to find out embedding strength (α). By experimentation, the value for embedding strength is 0.378 for both methods.

Threshold for the percentage difference Δ between the original and extracted watermarks has been determined as 15%. Lower thresholds resulted in false negatives; otherwise higher thresholds will make the technique to be fragile.

B. Experimentation and analysis of Results:

The proposed content-based watermarking method for image authentication has been implemented and tested using Matlab7.9.0 The method has been evaluated on a set of seven different sized images after changing their size into 256 x 256 color images. The system is tested with various standard images like Pepper, Lena, Baboon and House.

The original color images and its corresponding watermarked images obtained by embedding the watermark values (FD) with the images using DCT, DWT and Combined DCT & DWT techniques are shown in the Fig.1.



Fig. 1: a. Original Image b. Watermarked image using FD in DCT. c. Watermarked image using FD in DWT. d. Watermarked image using FD in combined DCT & DWT.

Fig.2. shows the watermarked color images after applying JPEG Compression obtained by embedding the watermark values (FD) with the images using DCT, DWT and Combined DCT & DWT techniques.



Fig. 2: a. Effect of watermarked Images after JPEG Compression Attack (JPEG 100, 80, 60, 40) using FD in DCT.



Fig. 2: b. Effect of watermarked Images after JPEG Compression Attack (JPEG 100, 80, 60, 40) using FD in DWT.



Fig. 2: c. Effect of watermarked Images after JPEG Compression Attack (JPEG 100, 80, 60, 40) using FD in combined DCT & DWT.

Fig.3. shows the watermarked color images after applying noise obtained by embedding the watermark values (FD) with the images using DCT, DWT and Combined DCT & DWT techniques.



Fig. 3: a. Effect of watermarked Images after Noise Attack (Gaussian, Uniform noise) using FD in DCT.



Fig. 3: b. Effect of watermarked Images after Noise Attack (Gaussian, Uniform noise) using FD in DWT.



Fig. 3: c. Effect of watermarked Images after Noise Attack (FD) combined DCT and DWT.

Fig.4. shows the watermarked color images after applying low pass filter, sharpening and contrast stretching obtained by embedding the watermark values (FD) with the images using DCT, DWT and Combined DCT & DWT techniques.



Fig. 4: a. Effect of watermarked Images after filtering Attacks (Lowpass, Sharpening and Contrast Stretching) using FD in DCT.



Fig. 4: b. Effect of watermarked Images after filtering Attacks (Lowpass, Sharpening and Contrast Stretching) using FD in DWT.

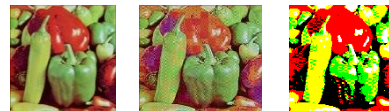


Fig. 4: c. Effect of watermarked Images after filtering Attacks (Lowpass, Sharpening and Contrast Stretching) using FD in combined DCT & DWT.

C. *Tamper Detection:*

Fig.5. shows the watermarked color images after tamper detection using DCT technique. For this purpose, we tamper some portion of watermarked image by randomly applied noise. Then we used our method to detect the tampered region.



Fig. 5: a. Tamper Detection (identifying tampered location from the tampered image) using FD in DCT.



Fig. 5: b. Tamper Detection (identifying tampered location from the tampered image) using FD in DWT.



Fig. 5: c. Tamper Detection (identifying tampered location from the tampered image) using FD in combined DCT & DWT.

The efficiency of the method in correctly extracting the watermark is given by the percentage difference between the computed and extracted fractal dimension of the received image blocks. Table 1 gives the highest percentage difference Δ for DCT, DWT, and combined DCT & DWT watermarking techniques for the test images. The values range from 39.9822 to 50.9442 in DCT method, the values range from 1.0969 to 9.1038 in DWT method and the values range from 24.5987 to 34.0755 in combined DCT & DWT method over all the test images. This indicates that the method extracts the embedded watermark accurately.

Table 1 gives the highest percentage difference Δ for various watermarking techniques for the test images. The values range from 1.0969 to 50.9442, over all the test images for various watermarking techniques using fractal dimension.

Table 1: Results after Watermarking Extraction without Attacks using FD.

S.NO		HIGHEST PERCENTAGE DIFFERENCE		
		DCT	DWT	Combined DCT and DWT
1	AVERAGE	48.25	4.9859	29.4833
2	MINIMUM	39.9822	1.0969	24.5987
3	MAXIMUM	50.9442	9.1038	34.0755

D. Quality of the Watermarked Image:

The proposed content-based watermarking method has been implemented on a different size of images. The metrics PSNR, Pearson Correlation Coefficient (PCC), Normalized Cross Correlation (NCC), and Image Fidelity (IF) are calculated between the host image and the watermarked image for various watermarking techniques. It can be observed that there is no perceptually noticeable difference in the images due to watermarking.

In Table 2, the quality metrics of the watermarked images using Fractal Dimension of different methods are compared. From the table DCT method produces better results than other observed techniques.

Table 2: Quality Metrics after Watermarking using FD.

EMBEDDING METHODS	PARAMETER	Baboon	Lena	Pepper
DCT	PCC	0.9943	0.9981	0.9968
	IF	1.0002	1.0001	1.0001
	NCC	1.0004	1.0001	1.0003
	PSNR	79.7356	79.2016	80.4821
	PCC	0.9870	0.9808	0.9829
DWT	IF	1.0004	1.0002	1.0002
	NCC	1.0005	1.0002	1.0003
	PSNR	76.9748	76.2806	76.4567
	PCC	0.9870	0.9809	0.9829
COMBINED DCT & DWT	IF	1.0004	1.0002	1.0002
	NCC	1.0005	1.0002	1.0003
	PSNR	76.9748	76.2806	76.4567

E. Robustness against Incidental Image Processing:

Robustness of the proposed method against normal signal processing operations such as jpeg compression, noise and filtering has been experimentally evaluated on all the test images.

For all these attacks, the values of highest percentage difference Δ using fractal dimension, ranges from 15.98987 to 51.55593 for various watermarking techniques as given in Fig.6.

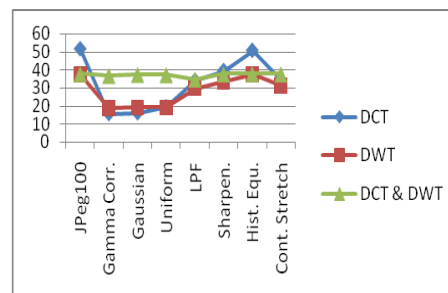


Fig. 6: Robustness of the FD technique after incidental image processing operations

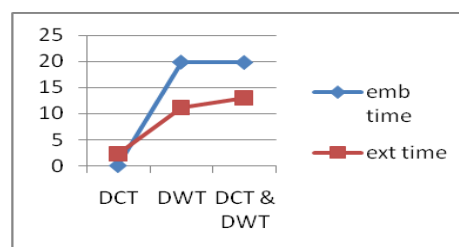


Fig.7: Time Complexity for embedding and extraction using FD.

From Fig.7, Embedding and Extraction time is too minimum for DCT based fractal dimension watermarking.

F. Limitations:

An important limitation of Fractal Dimension (FD) is the choice of the box size (R. Lopes and N. Betrouni, 2009) (it is sensitive to its box size). This method is not theoretically well founded and it is valid only for statistically self-similar signals.

Conclusion:

In this paper various content based watermarking techniques are implemented. Here the content of image is Fractal Dimension and it is obtained by using box-counting method. No information about the host is required for watermark extraction. The proposed method aims at comparing the content-based watermarking techniques for color images using fractal dimension embedded by three techniques namely DCT, DWT and Combined DCT & DWT. The same methods are used to extract the watermark values successfully and the results are compared.

The proposed methods authenticate the image even under common image processing operations and identify the tampered location correctly. The comparison of three transformed techniques shows that DCT based watermarking application provides better result. The three methods discussed in this paper, robust against noise and filtering attacks. Our future work is to improve the robustness against JPEG, Histogram like image processing operations.

REFERENCES

- Ali Al-Haj, 2007. Combined DWT-DCT Digital Image Watermarking, 3(9): 740-746.
- Dr. Latha Parameswaran, Dr. K. Anbumani, 2008. Content-Based Watermarking for Image Authentication Using Independent Component Analysis, Informatica, pp: 299-306.
- Dan Yu, Farook Sattar, and Kai-Kuang Ma, 2002. Watermark detection and extraction using Independent component analysis method, EURASIP Journal on Applied Signal Processing, 1: 92-104.
- Eugene, T., Lina, Christine I. Podilchuk and Edward J. Delp, 2000. Detection of Image alterations using semi - fragile watermarks, Proceedings of SPIE International Conference on Security and watermarking of Multimedia contents.

Emir Ganic. Ahmet M. Eskicioglu, 2004. Robust DWT-SVD Domain Image Watermarking: Embedding Data in all Frequencies, 4: 20-28.

Francisco, J., Gonzalez-Serrano, Harold Y. Molina-Bulla and Juan J. Murillo-Fuentes, 2001. Independent component analysis applied to digital image Watermarking, International Conference on Acoustic, Speech and Signal Processing (ICASSP), 3: 1997-2000.

Huijuan Yang and Alex C. Kot, 2006. Binary image authentication with tampering localization by embedding cryptographic signature and block identifier, IEEE Signal Processing Letters, 13(12): 741-744.

Marc Schneider and Shih-Fu Chang, 1996. A robust content based Digital Signature for Image Authentication, Proceedings of International Conference on Image Processing, 3: 227-230.

Phen-Lan Lin, Po-Whei Huang, and An-Wei Peng, 2004. A Fragile Watermarking Scheme for Image Authentication with Localization and Recovery, Proceedings of the IEEE Sixth International Symposium on Multimedia Software Engineering (ISMSE'04).

Lopes, R., N. Betrouni, 2009. Fractal and Multifractal Analysis, Medical Image Analysis 13: 634-649.

Rongrong, Ni, Qiuqi Runa, 2006. Region of Interest Watermarking Based on Fractal Dimension, The 18th International Conference on Pattern recognition (ICPR'06).

Saeed, K., Amirgholipour Ahmad R. Naghsh Nilchi, 2009. Robust Digital Image Watermarking Based on Joint DWT-DCT, 3(2): 42-54.

Stephane Bounkong, Boremi Toch, David Saad, and David Lowe, 2003. ICA for watermarking digital images, Journal of Machine Learning Research, 4: 1471-1498.