2011 International Conference on Computer Communication and Management
Proc .of CSIT vol.5 (2011) © (2011) IACSIT Press, Singapore

A Robust Digital Image Watermarking Approach against JPEG Compression Attack Based on Hybrid Fractal-Wavelet

Sanaz Shahraeini [1] and Mahdi Yaghoobi [2]

[1] Artificial Intelligence Dept, Islamic Azad University Mashhad Branch, Mashhad, Iran
[2] Electrical Engineering Dept, Islamic Azad University Mashhad Branch, Mashhad, Iran

Abstract. The recent progress in the digital multimedia technologies has offered many facilities in the transmission, reproduction and manipulation of data. However, this advance has also brought the problem such as copyright protection for content providers. Digital watermarking is one of the proposed solutions for copyright protection of multimedia. This paper proposes a blind watermarking algorithm based on fractal model in discrete wavelet domain for copyright protection. The idea of the presented scheme is to hide a binary image as a watermark with fractal parameters in wavelet domain of host image. Fractal compression technique is used to encode a gray image and fractal codes are embedded into the wavelet coefficients of the gray image according to well-connected watermark algorithm. The experimental results show that the algorithm is robust against JPEG compression attacks.

Keywords: Blind, Copyright protection, Fractal, Watermark, Wavelet

1. Introduction

The rapid evolution of the Internet makes easier the transmission of digital multimedia content such as text, audio, images and video. Digital media can be accessed or distributed through the network. As a result, replications of digital media are simple with no loss of fidelity, that is, the copy of a digital medium is identical to the original one. An unlimited number of identical copies of digital media can be illegally produced; this is a serious threat to the copyright of the media owner. Therefore, to protect and enforce intellectual property rights of the media owner is an important issue in the digital world [1].

Digital Watermarking is an important issue in the field of multimedia security protection. The digitization of our world has expanded the concept of watermarking in order to be used in authenticating ownership claims and protecting proprietary interests. Digital watermarking can be applied to various digital products such as images, audio, text, graphics and certificates. Especially in the image security concerns, it is a widely used method. Within several techniques this watermark can be recovered from the processed image in order to determine the copyright owner of the image. In digital watermarking, the actual bits are scattered in the image in such a way that they cannot be identified and show resilience against attempts to remove the hidden data.

An ideal watermarking system, however, would embed an amount of information that could not be removed or altered without making the cover object entirely unusable. As discussed in [2] this may deter people from illegal copying by allowing the determination of the legitimate owner of the protected digital media and corresponding copyright. As a side effect of these different requirements, a watermarking system will often trade capacity and perhaps even some security for additional robustness. There are two main categories that a watermark can fall under, namely visible and invisible watermarks. Most of the literature has focused on the invisible digital watermarking as it has more applications in today's digital world. Visible digital watermarks are strongly linked to the original paper watermarks that have been traced back to the end of 13th century.

Thus, Digital watermarks serve and important role in providing evidence of copyright infringements and thus making the misuse of protected multimedia traceable.

1.1. Watermark applications

The requirements that a watermarking system needs to comply with depends upon the specific type of application. A few most common applications involve: owner identification, transaction tracking (fingerprinting), copy protection, broadcast monitoring, medical applications, media bridging, data authentication and covert communication.

1.2. Watermark requirements

There are many different protocols and embedding techniques that enable us to hide data in a given object. However, all of the protocols and techniques must satisfy a number of requirements so that watermarking can be applied correctly. The main requirements that watermarking techniques must satisfy, involve: robustness, imperceptible, undeletable, unambiguous, quality of the image, payload capacity of the image, reliability of the watermark, fidelity and computational cost.

In this paper, we introduce a robust digital image watermarking algorithm. Our digital image watermarking approach is using fractal model in DWT domain. A binary image has chosen as a watermark. To verify the effectiveness of the proposed scheme, a series of simulations and experiments are conducted. Simulation results show that the proposed scheme is more robust than existing methods.

This paper is organized as follows. Section II describes previous works on image watermarking methods. In section III a fractal model that used in our watermarking approach is described. Section IV reviews some necessary background on wavelets. The proposed algorithm for watermark embedding and extraction is described in section V. In section VI we present experimental results and finally in section VII summaries of results and future research to continue this work is provided.

2. Previous works

Digital image watermarking has been the scope of heavy research since mid 1980's and a variety of watermarking techniques has been proposed in recent years.

The digital watermarking technologies can be divided into two categories by the embedding position, spatial domain and frequency domain watermark [3].In spatial domain techniques, the values at the image pixels are directly modified based on the watermark that has to be embedded. The simplest way is to modify the last significant bits (LSB) of the image's pixel data. In frequency domain the transform coefficients are modified instead of directly changing the pixel values. The inverse transform is finally applied to obtain watermarked image. The transforms commonly used for watermarking purposes are the discrete cosine transforms (DCT), discrete Fourier transforms (DFT) and discrete wavelet transforms (DWT) [4]. Spatial domain techniques are developed earlier and are easier to implement, but they are limited in robustness, while frequency domain techniques are more robust and compatible to popular image compression standards. . Digital wavelet transformation is adopted in this paper. The DWT is a mathematical transformation that takes a signal and transforms it from spatial domain into frequency domain. It efficiently decomposes an image into multi-resolution sub-bands and has the characteristics that energy compacts into a few low transform coefficients after the wavelet transform [5].

One of the earliest schemes for image watermarking using fractal coding was presented in 1996 by Puate and Jordan [6]. In their paper a fractal-based approach is proposed where the concept of fractal image compression is applied to binary image watermarking. In the approach, to embed a watermark fractal codes are skilfully divided into two subsets. Each subset represents a bit value, 0 or 1. To retrieve the embedded watermark, the fractal code of image block is found and the bit value of watermark is assigned according to the subset which the fractal code belongs to.

In 2000, Li and Wang utilized the isometric property to embed the watermark bit by two isometric kind of plane. Since then, there were few papers to investigate the digital watermarking based on fractal coding [7]. In this paper we applied fractal encoding technique as it identifies parts of the image that are most suited for data hiding.

Many image processing schemes that employ hybrid fractal and wavelet techniques have been proposed in the last few years [8]. In these schemes fractal image coding process is wavelet decomposition while the fractal decoding process is a successive interpolation of wavelet detail coefficients. The issues of these methods are related to robustness against image processing attacks and time of information processing.

3. Fractal image watermarking

Fractal encoding can be done in spatial domain [9] and frequency domain [10]. Paul Darven [11] suggested a fractal method that uses the information of range and domain region as key. Joan Paute and Fred Jordan [5] used key to generate coordinates of range blocks. Patrick Bas and Jean-Marc Chassery [12] used fractal scheme for watermarking. They find the transformation such that for each block D and R, a new range block R' is calculated [12]. Our approach used the collage theory that is developed by Jacquin [13] in fractal compression. This fractal code extracts the self-similarities of an image. It is generated by calculating an Iterated Function System (IFS) of the image. Here the entire image is not self similar, but parts of the image are self-similar with properly transformed parts of it. The use of fractal model in our approach is described in section 5.1.

4. Discrete wavelet transform

Discrete wavelet transform is a multi resolution decomposition of a signal. Considering an image, 1 level DWT involves applying a low pass and a high pass filters along the columns and then the rows respectively. The low pass filter applied along a certain direction extracts the low frequency (approximation) coefficients of a signal. On the other hand, the high pass filter extracts the high frequency (detail) coefficients of a signal [14].

In two dimensional applications, for each level of decomposition, we first perform the DWT in the vertical direction, followed by the DWT in the horizontal direction. After the first level of decomposition, there are 4 sub-bands: LL1, LH1, HL1, and HH1. For each successive level of decomposition, the LL sub-band of the previous level is used as the input. Each tile component undergoes three levels of decomposition. This results in 10 sub-bands per component. LH1, HL1, and HH1 contain the highest frequency bands present in the image tile, while LL3 contains the lowest frequency band.

The three-level DWT decomposition is shown in Fig.1.

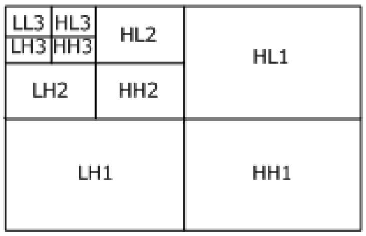


Fig.1: Three-level DWT decomposition

5. Proposed method

Our proposed method is approximately derived from [15]. But in our method a binary image is embedded in frequency domain of original image and algorithm searches similarities in frequency domain. Our embedding and extracting processes are shown in Fig.2 and Fig.3. The proposed scheme is based on fractal model in watermarking technique of image. The details are described in the following subsections.

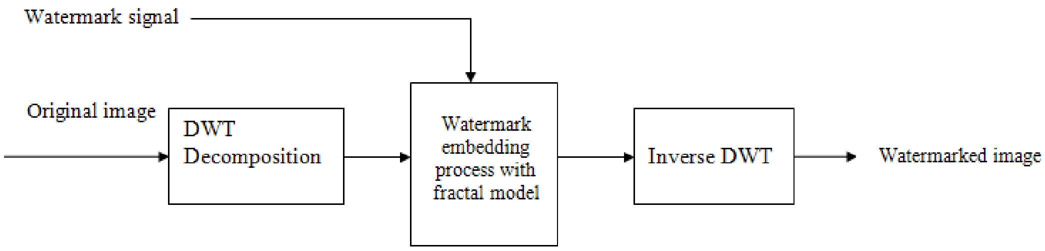


Fig.2: Block diagram of watermark embedding

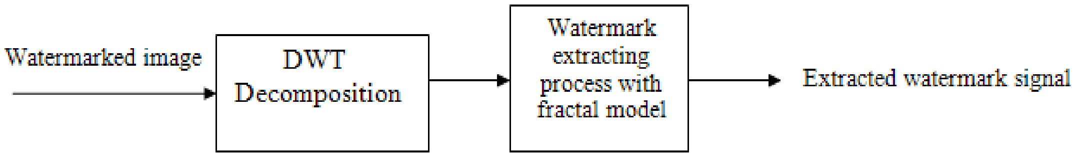

Watermarked image
DWT Decomposition
Watermark extracting process with fractal model
Extracted watermark signal

Fig3: Block diagram of watermark extracting

5.1. Watermark embedding

We can generalize the total watermark embedding process in the two steps: first extracting a set of features (host features) from the host image, and then by modifying them according to the watermark content. The choice of the host features and the definition of the embedding rule have implications on watermark robustness and imperceptibility, which are the main concerns and challenges of the watermark embedding process.

The most of the energy of the image concentrated in the low-frequency approximation of the carrier image after wavelet decomposition. It is the smooth part of the image and the human eye more sensitive to it. Although embedded watermark in this part can obtain a good robustness, but the watermark transparency will be significantly reduced. In normal circumstances, the watermark should be embedded in the second or third level of wavelet coefficients which has medium frequency characteristics in order to meet transparency and robustness requirements of the digital watermark. In our method we transform image into third level of discrete wavelet decomposition. In third level, The LH3 sub band is more significant than the HL3 sub band [16]. For this reason, it would be suitable to embed the watermark in the middle frequency band LH3 instead of HL3.

In this method image is partitioned in to 2 regions: domain region D and range region R. The sub images within the range region and domain region are called range blocks and domain blocks, respectively.

A domain pool is consisted of a set of blocks in the domain region. It is split into two halves D0 and D1. Fractal image compression theory is used to identify a series of range blocks and a corresponding series of matching domain blocks. The matching process produces the best matching domain block and a corresponding fractal transform for each range block.

The fractal transform basically involves multiplying a coefficient in the medium frequency of third level of DWT in the selected domain block by an average scaling factor (S) and adding an offset factor (O) to the result (R'=S.D+O) [13]. Thus the fractal transformation is applied to the domain block to produce a new range block that is visually similar to the original range block. This new block is written to the watermarked image in place of the old range block. If the current bit of watermarking data is 0, we search for a match in the first half of the domain pool otherwise we search the second half. For each bit of watermarking data a new range block is produced.

The embedding algorithm takes image I and binary watermarking image as input. It outputs a visually identical image Inew that has watermarking data hidden in it. First of all, image I is partitioned into four quadrants. First and fourth quadrants constitute the range region R and second and third quadrants constitute domain region D (Fig.4).

Each Range region is divided into square blocks {r0,r1,…,rl} of equal size (8×8). These blocks are non-overlapping. Also each D region is divided into square blocks of equal size (8×8). Each block in R region and D region is transformed to third level DWT coefficients and we consider the similarities between only the medium frequency coefficients of this level.

If the watermark bit is 0 we search for a best match in LL3 of each domain block in the D0 region otherwise we search for a best match in LL3 of each domain block in D1 region. For each bit of watermarking data a new LL3 of range block is chosen orderly. After fractal transformation new range block will be added in LH3 sub band of old range block.

R region	D_0 region
D_1 region	R region

Fig4: Image partitions

5.2. Watermark extracting

Extracting method is reverse of embedding. Range and domain regions remain same as in embedding process. First watermarked image‘s blocks are transformed into three-level DWT domain. To find a bit of watermark data in the image file, first we select a domain block from the domain region D0 in the same order as in the embedding process and search the range block r in two range regions which minimizes the quadratic error and matches it by a linear relationship. The linear relationship is that each coefficient in domain block is formed by multiplying corresponding coefficient in the range block by a scale factor and adding an offset factor. The match is successful if we can find this linear relationship between the two blocks. After match found in R regions, we set a bit of watermark data which corresponding to the place of R, to 0. These operations will continue in D1 domain same as last step but after match found in R regions, we set a bit of watermark data which corresponding to the place of R, to 1.

6. Experimental results

We use the peak signal-to-noise ratio (PSNR) to evaluate the quality between the attacked image and the original image. The PSNR formula is defined as follows [16]:

$$PSNR = 10 \times \log_{10} \frac{255 \times 255}{\frac{1}{H \times W} \sum_{x=0}^{H-1} \sum_{y=0}^{W-1} [f(x,y) - g(x,y)]^2} db \qquad (1)$$

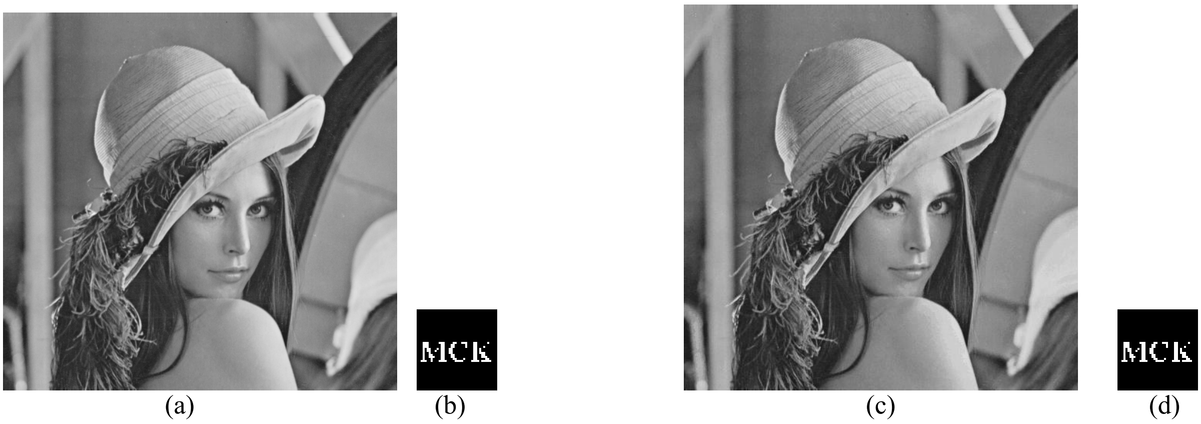
Where H and W are the height and width of the image, respectively; and f(x,y) and g(x,y) are the grey levels located at coordinate (x,y) of the original image and attacked image, respectively.

After extracting the watermark, the normalized correlation coefficient (NC) is computed using the original watermark and extracted watermark to judge the existence of watermark. It is defined as follows [16]:

$$NC = \frac{1}{w_h \times w_w} \sum_{i=0}^{w_h-1} \sum_{j=0}^{w_w-1} w(i,j) \times w'(i,j) \qquad (2)$$

We used 256×256×8 standard test images such as Lena.bmp, Airplane.bmp and Truck.bmp as original images which are obtained from[17], and the watermarking we used is the binary value image of 40×40 (Fig.5(a) and Fig.5(b)).

Fig.5(c) and Fig.5(d) shows the watermarked image and the extracted result.



(a) (b) (c) (d)

Fig.5: (a) Original Lena image of size 512×512 (b) Original binary watermark of size 40×40 (c) Watermarked Lena with PSNR=54.14 (d) Extracted watermark with NC=1

Table I,II and III show the NC values after attacks by JPEG compression with different quality factors on three watermarked images.

TABLE I. Normalized correlation coefficients(NC) after attacks by JPEG compression with the quality factors(QF) 10, 20, 30, 40, 50, 60, 70, 80, 90, and 100 in watermarked Lena image with PSNR=54.14

QF	10	20	30	40	50	60	70	80	90	100
NC	0.42	0.69	0.93	0.95	1	1	1	1	1	**1**
Extracted watermark										

TABLE II. Normalized correlation coefficients(NC) after attacks by JPEG compression with the quality factors(QF) 10, 20, 30, 40, 50, 60, 70, 80, 90, and 100 in watermarked Airplane image with PSNR=55.23

QF	10	20	30	40	50	60	70	80	90	100
NC	0.44	0.56	0.80	0.96	1	1	1	1	1	**1**
Extracted watermark										

TABLE III. Normalized correlation coefficients(NC) after attacks by JPEG compression with the quality factors(QF) 10, 20, 30, 40, 50, 60, 70, 80, 90, and 100 in watermarked Truck image with PSNR=53.31

QF	10	20	30	40	50	60	70	80	90	100
NC	0.39	0.53	0.76	0.92	0.95	1	1	1	1	**1**
Extracted watermark										

Compared to two existing recently published papers by Shu [8] and Li [16] based, the results are shown in that our proposed method is more robust against JPEG compression attack than the other 2 methods.

7. Conclusion

Fractal image compression is a novel technique in the field of image compression. The main goal in fractal compression of images is to try to find self-similarity in an image and exploit this redundancy in the image coding. This paper proposed a novel blind watermarking algorithm based on fractal model in wavelet domain. The watermarking algorithm makes use of characteristic of multi resolution of DWT and fractal coding to assure the invisibility and robustness. The simulation experiments validate the effectiveness of the watermarking scheme. As a result, in the proposed method the values of the PSNR of the watermarked images are improved (PSNR is more than 50 dB) and it can effectively resist common image processing non geometric attacks, especially by JPEG compression (with a quality factor up to 20) .The extracted watermark for attack is clearly recognizable.

Further research should go towards improving the watermarking program and adding extra functionality. One of these is looking at having multiple watermarks for a single image, so that different parts of the image have a different watermark. We used fixed partitioning scheme. Instead of this, adaptive partitioning scheme can be used, which would yield better results if used as the basis for the data hiding method.

8. References

[1] L. Chang-Hsing and L. Yeuan-Kuen, "An adaptive digital image watermarking technique for copyright protection," Consumer Electronics, IEEE Transactions on, vol. 45, pp. 1005-1015, 1999.

[2] R.Oppliger, "Security Technologies for the World Wide Web," in Intellectual Property Protection, 2nd ed Noewood, MA: Artech House,2003,pp.347-357.

[3] Researches on Uniform Meaningful Watermark, Liu Quan, Jiang Xuemei, Proceedings of the 2002 6t International Conference on Signal Processing, 2002.

[4] M.S. Hsieh, and D.C. Tseng , “Hiding digital watermarks using multi-resolution wavelet transform”, IEEE Transactions on industrial electronics, vol. 48, No. 5, pp 875882, Oct, 2001.

[5] [4] Hua Lian; Bo-Ning Hu; Rui-Mei Zhao; Yan-Li Hou; , "Design of digital watermarking algorithm based on wavelet transform," Machine Learning and Cybernetics (ICMLC), 2010 International Conference on , vol.5, no.,

pp.2228-2231, 11-14 July 2010

[6] J. Puate and F. Jordan, “Using fractal compression scheme to embed a digital signature into image,” in Proc. SPIE Photonics East Symp., Boston, MA, Nov. 18–22, 1996.

[7] Aidan Mooney, John G. Keating, Ioannis Pitas, "A comparative study of chaotic and white soise signals in digital watennarking", Chaos, Solition and Fractal 35, p. 913-921, 2008.

[8] ShuGuo Yang; ChunXiaLi; ShengHeSun; RongSheng Xie; , "A Fractal Watermarking Scheme for Image in DWT Domain," Eighth ACIS International Conference on , vol.1, no., pp.364-368, July 30 2007-Aug. 1 2007

[9] J-M. Chassery P. Bas and B. Macq. Robust watermarking based on the warping of pre-defined triangular patterns. In Proc. SPIE, pages 99–109,2000.

[10] J.-M. Chassery P. Bas and F. Davoine. A geometrical and frequential watermarking scheme using similarities. SPIE Conference on Security and Watermarking of Multimedia Contents,San Jose, 3657:264–272, 1999.

[11] P. Davern and M. Scott. Fractal based image steganography. Information Hiding, First International Workshop, Lecture Notes in C omputer Science, pages 279–294, 1996

[12] J-M. Chassery P. Bas and F. Davoine. Self-similarity based image watermarking. IX European Signal Processing Conference, Island of Rhodes, Greece, pages 8–11, 1998

[13] A. E. Jacquin. Image coding based on a fractal theory of iterated contractive image transformation. IEEE Transactions on Image Processing, 1(1):18-30, January 1992.

[14] Davis, G. and Nosralinia, A., “Wavelet-Based Image Coding: An Overview,” IEEE Trans. on Image Proc., March 1996.

[15] Gulati Kamal, " Information Hiding Using Fractal Encoding,” Indian Institude of Technology Bombay,Jan.2003

[16] Wei-Hung Lin; Shi-Jinn Horng; Tzong-Wann Kao; Pingzhi Fan; Cheng-Ling Lee; Yi Pan; , "An Efficient Watermarking Method Based on Significant Difference of Wavelet Coefficient Quantization," Multimedia, IEEE Transactions on , vol.10, no.5, pp.746-757, Aug. 2008.

[17] F. A. P. Petitcolas, Weakness of Existing Watermark Scheme. Available: http://www.petitcolas.net/fabien/watermarking/stirmark/