International Journal of Emerging Engineering Research and Technology
Volume 3, Issue 4, April 2015, PP 75-80
ISSN 2349-4395 (Print) & ISSN 2349-4409 (Online)

Wavelet-Based Semi Fragile Watermark for Digital Images

Taha Basheer Taha, Mohamad T. Sultan

Department of Computer Science, Cihan University, Erbil, Iraq

ABSTRACT

With the rapid development of the Internet and multimedia systems, access to multimedia data becomes easier, since the most commonly used multimedia files are digital images, the need to protect the content of these image and detect any simple alteration is very important issue.

In the same time the need to protect the copyright of these images becomes an important issue. Recently, digital watermarking techniques are utilized for copyright protection of digital images and for detecting alteration.

In this work, a wavelet-based digital watermarking algorithm has been proposed to detect any alteration in Images and to protect their copyrights. Semi-Fragile watermark has been used to allow the users to freely compress the images without any issues, in the same time any alteration in pixels' values will be detected by using non-blind wavelet-based algorithms.

A Graphical User Interface (GUI) has been designed and implemented to allow easily and efficiently choosing the host image, choosing and embedding the watermark, save the watermarked image in different formats, detect the alteration and mark their locations.

Keywords: Image Processing, Watermarking, Semi Fragile Watermark, DWT.

INTRODUCTION

With the rapid development of internet, digital media has been widely distributed on the network recently. It leads to an acute need for media authentication because such digital content can be easily edited or modified by certain software or tools. As a new solution for content authentication, digital watermarking, is drawing considerable attention and becomes an active research field [1].

Various types of watermarking schemes have been proposed to serve these purposes. The watermarks of the *robust* watermarking schemes for copyright protection are expected to survive different types of manipulations to some extent provided that the manipulated media are still valuable in terms of commercial importance or significant in terms of visual quality. Unlike robust schemes, the schemes for the purposes of authentication and content integrity verification are supposed to be *fragile*, i.e., we expect the watermark to be destroyed when attacks are mounted on its host media so that alarms can be raised when wrong watermark is extracted. Therefore, the emphasis of the fragile watermarking schemes is focused on the sensitivity to attacks or even incidental manipulations in some cases [2].

However the third type of watermarking is authentication based on semi-fragile watermarking(also called soft authentication), which allows accepting certain content modifying without going beyond predefined quality or semantic meaning level, such as JPEG compression. Semi-fragile watermarking is very useful for local bandwidth to transfer videos by suitable bit rate or resolution of original content. For example, suppose one encodes a standard definition video sequence with H.264 at 4 Mb/s and stores it in a network video server that will be accessed via a network. At a later time, if a client requests this video but he/she gets only bandwidth with 3Mb/s, hence, the server has to transfer the sequence to meet the new bandwidth requirement. However, in some scenarios, such as for law evidence and for military applications with high security requirements, it is necessary that any modifications of digital contents have to be detected. It is obvious that complete fragile watermarking is needed in these cases. Authentication based on complete fragile watermarking is called hard authentication, which not only can detect any modifications but also can locate the modified areas [3].

Address for correspondence

Comeng.taha987@yahoo.com

In this paper, an algorithm for embedding semi-fragile watermark is proposed. Depending on Discrete Wavelet Transformation (DWT), semi fragile watermark will be embedded inside host image and then extracted and checked using non-blind comparisons. However, the watermark will still robust if normal ways of compression are being used without internal modifications.

WATERMARKING AND DIGITAL WATERMARKS

Paper watermarks appeared in the art of handmade papermaking nearly 700 years ago. The oldest watermarked paper found in archives dates back to 1292 and has its origin in the town of Fabriano in Italy which has played a major role in the evolution of the papermaking industry. At the end of the 13th century about 40 paper mills were sharing the paper market in Fabriano and producing paper with different format, quality, and price [12].

After their invention, watermarks quickly spread in Italy and then over Europe and although initially used to indicate the paper brand or paper mill, they later served as indication for paper format, quality, and strength, and were also used as the basis for dating and authenticating paper. Years later, with the increasing importance and widespread distribution of digital media and imagery, the protection of the intellectual property rights of the owner for their media has become increasingly significant. One of the types of media is digital imagery, which can be copied and widely distributed without any significant loss of quality. Protecting the property rights of the owners of these images is therefore an increasingly important capability. A straightforward way to protect this is to completely encrypt the data and thereby require the end user to have the encryption key for the decoding. Another means to protect this data is to apply a digital watermark. Digital watermarking is the process by which an image is coded with an owner's watermark and can be done using either of two general approaches. One approach is to transform the host image into its frequency domain representation and embed the watermark data therein. The second is to directly treat the spatial domain data of the host image to embed the watermark [4].

METHODOLOGY

Watermark Embedding

The process of embedding the watermark inside the host image is performed by applying DWT on the host image to be separated into four different frequencies LL HL LH and HH. L is stand for "Low" pass filtering, H for applying High Pass Filtering on the image, HH for example is for applying High pass filter for both rows and columns. Supposing the size of host image is 512* 512 pixels, each of DWT sub-frequencies has size of 256*565 pixel. The watermark which is binary image with size 64*64 bits will be embedded inside one of these DWT sub-frequencies after multiplying by certain factor for giving higher spread through image pixels. The experiments shows the best frequency to embed the watermark in is HH. Figure 1 shows different wavelet frequencies.

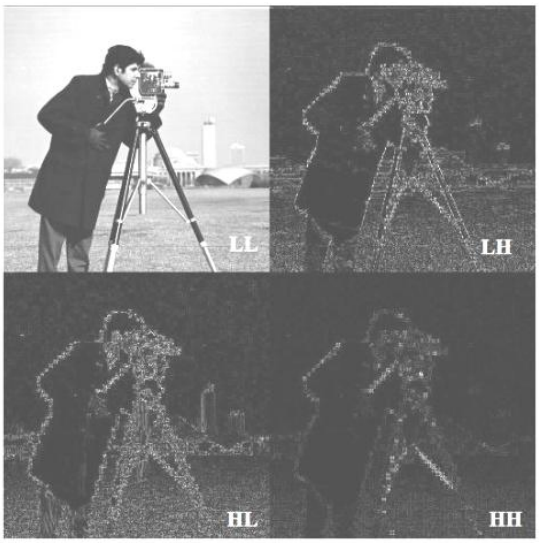

Figure1. *Different DWT frequency bands*

Watermark Extraction

The process of extracting watermark is to apply DWT on both source image and target image , subtract the HH part of the original image from HH of target image, the result will be the watermark vector which will be reconstructed to create it's equivalent two dimensional image.

Watermark Comparison

The process of comparing and find the alteration is non-blind, since the original image will be required to compare it with the target one. DWT will be applied on the original image which already has the original watermark and target image which contain the watermark which may be altered. Pixels will be compared one after one since any difference is considered as alteration and the equivalent location will be marked.

The process of embedding watermarking process, extracting and comparing is shown in figure 2.

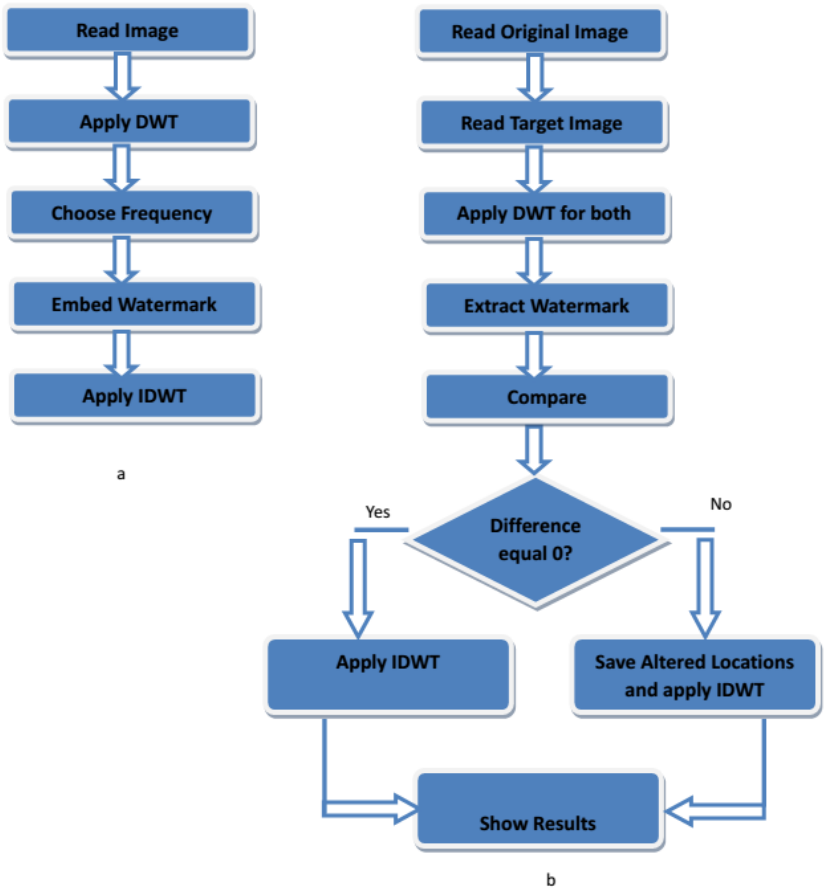

Figure2. *(a) Embedding Process, (b) Extracting Process*

RESULTS

Watermark Embedding

After applying DWT, original image has been separated into four different frequencies, LL, LH, HL, HH, embedding watermark with size of 64 bit within each of them will produce different result. Evaluating the perceptibility of the watermarks can be done either through subjective tests or a quality metric. Subjective test can be noticed by naked eye, and the most popular quantitative distortion measures in the field of image and video coding and compression are the *signal-to-noise ratio* (SNR), and the *peak signal-to-noise ratio* (PSNR). They are usually measured in *decibels* (dB): SNR (dB) = 10 log10 (SNR).

Both of tests are considered when the right frequency had been chosen, the following results shows the Subjective and Objective (Quantitative) results when the watermark is hidden inside Cameraman JPG grayscale Image see table 1.

Table1. *Watermark Embedding in different DWT frequency bands*

Embedding Frequency Band	Subjective Test	PSNR
LL	VISIBLE	40.5020
LH	INVISIBLE	43.2037
HL	INVISIBLE	42.9338
HH	INVISIBLE	43.5243

From the results above we can figure that choosing the HH frequency is the best choice in this case, since it has the higher PSNR and Invisibility. However, hiding watermark in HH will make the watermark fragile but invisible, Since robustness of watermark is not considered in our work (we are tracking any alter in watermark), HH is the best place where we save our watermark without distorting the host image.

Comparison and Watermark Extraction

The process of comparison and alter detection is performed by non-blind suggested algorithm, where the original image is chosen with the watermark from graphical user interface (see figure 3a). next the target image which may has some modified pixels is loaded and the process of compare is established. One of the background buildings has been removed from the target image and the result of compare is shown in figure 3b where the modified pixels are marked.

Watermark can also be extracted from target image to protect copy rights of the author of the image from "Extract Watermark" selection.

However, saving the target image as other formats like GIF will not mark any alteration, since there are no modifications in any pixel. Figure 3c shows the result of comparing with GIF target image.

Figure3a

Figure3b

Figure3c

Figure3. *Graphical User Interface (a) Choosing Images. (b) Result after alteration (c) result for gif image format*

CONCLUSION

In this work, a wavelet-based semi -fragile watermarking algorithm has been proposed to discover any malicious changes in digital images.

The proposed algorithm shows:

- Discrete Wavelet Transform has been used to split the digital image into four different frequencies. By applying Low and High pass filters on both rows and columns of digital image. four frequency band are LL , LH , HL ,HH.
- By embedding a watermark within low frequencies, the water mark turned to be robust but visible to HVS in many cases, however embedding it inside high frequency will create invisible but fragile watermark.
- The size of the watermark and the binary format make it tiny and imperceptible to HVS.
- Watermark may be multiplied by certain factor to be distributed on all the embedding band.
- The Algorithm shows high sensitivity for content (malicious) altering and robust against safe altering like changing file format.
- Graphical User Interface is used to give more flexibility for the algorithm to be tested and used.

REFERENCES

[1] Raja' Alomari, Ahmed Ali Jaber. A fragile watermark algorithm for content authentication.King Abdullah II School for information security.Amman Jordan. 2004

[2] Wang, R. D., et al. "Fragile watermarking scheme suitable for the authentication of H. 264/AVC video content." *Journal of Information & Computational Science* 9.13 (2012): 3693-3706.

[3] Lim, Yusuk, Changsheng Xu, and David Dagan Feng. "Web based Image Authentication Using Invisible Fragile Watermark. Australian Computer Society." (2002).

[4] Hartung, Frank, and Martin Kutter. "Multimedia watermarking techniques."*Proceedings of the IEEE* 87.7 (1999): 1079-1107.

[5] *T. Y. Kuo, Y. C. Lo, Fragile video watermarking technique by motion field embedding with rate distortion minimization, Journal of Communication and Computer, 1 (2009), 16-22

[6] Johnson N., Duric Z., Jajoda S., "Information Hiding: Steganography and Watermarking-Attacks and Countermeasure", Kluwer Academic Publishers, 2000.

[7] Wang, Sha, et al. "Adaptive watermarking and tree structure based image quality estimation." *Multimedia, IEEE Transactions on* 16.2 (2014): 311-325.

[8] Karzenbeisser S., Perircolas F., "Information Hiding Techniques for Steganography and Digital Watermarking", Artech House, 2000.

[9] Ren, Na, Qi-sheng Wang, and Chang-qing Zhu. "Selective authentication algorithm based on semi-fragile watermarking for vector geographical data." *Geoinformatics (GeoInformatics), 2014 22nd International Conference on*. IEEE, 2014.

[10] Meerwald P., "Digital Image Watermarking in the Wavelet Transform Domain", M. Sc. Thesis, Salzburg University, Germany, 2001.

[11] Gonzalez R., Woods R., "Digital Image Processing", Prentice-Hall, 2002.

[12] Jain, Jaishree, and Vijendra Rai. *Robust Multiple Image Watermarking Based on Spread Transform*. INTECH Open Access Publisher, 2012.