Volume : 1 | Issue : 4 | April 2012 ISSN - 2250-1991

Research Paper Engineering

Implementation of Digital Watermarking by Combined Transform Domain Algorithm for Copyright Authentication using Matlab

* Raval Keta J. ** Mrs. Sameena Zafar

* PG Student, Patel College of Engineering and Science, RGPV, Bhopal, M.P., India

** Assistant Professor, Patel College of Engineering and Science, RGPV, Bhopal, M.P., India

ABSTRACT

The advancing world of communication is faces with challenging problems related to security and authenticity. In the context of multimedia communication, digital images and videos have endangered with spatio-temporal manipulations. Uncompressed digital images require considerable storage capacity and transmission bandwidth efficient image compression solutions are becoming more critical with the recent growth of data intensive, multimedia-based web applications. Digital Watermarking and data hiding has become an important tool for protecting digital images from theft, illegal copying and unlawful reproduction. We propose a blind watermarking algorithm combination of Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT). The proposed algorithm is more secure, robust and efficient because of use of DWT and DCT.

Keywords : component; formatting; style; styling; insert

I. Introduction

In the world of digital media aspect of secured media, communication has increasing now days. The information hiding techniques are widely used to camouflage one form of information into another. Digital watermarking is an embedding technique, which inserts the hidden information into multimedia data (also called original media or cover-media). The hidden information (known as the watermark) may be in text, image, audio or video form. After inserting or embedding the watermark by specific algorithms, the original media will be slight modified [1]. These watermarked images transmitted over a channel via a communication media. When transmitted the watermarked image over the channel, signal noise introduced and cause embedded watermark and watermarked image to be corrupted. Most watermarking algorithm based on the concept of the spread spectrum communication by embedding a pseudorandom watermark into the image content and detected it by using the correlation method. To archive the high reliability of watermark detection, the watermark detection process has to be robust to the alterations in the host image caused from both unintentional and intentional distortions (Called “attacks”) [2]. The aim of attacks is not always to completely remove or destroy the watermark but usually to disable its detection. Distortions are limited to those not producing excessive degradations. Otherwise, the transformed watermarked object would be unusable. These distortions could also introduce degradation to the performance of the system. The use of digitally formatted image and video information is rapidly increasing with the development of multimedia broadcasting, network databases and electronic publishing. This evolution provides many advantages such as easy, fast and inexpensive duplication of products. However, it also increases the potential for unauthorized distribution of such information, and significantly increases the problems associated with enforcing copyright protection. The rapid evolution of digital technology makes the development of reliable and robust schemes for protecting digital still images, audio and video from piracy a matter of urgency. Piracy attacks include illegal access to transmitted data in networks, data content modification, production and retransmission of illegitimate copies. The impact of such attacks might be very large, booth in financial and security terms [2].

Robust image watermarks are watermarks designed to survive attacks including signal processing operations and spatial transformations. To evaluate robust watermarks, we need to evaluate how attacks affect the watermark of an image. The mean square error (MSE) and peak signal to noise ratio (PSNR) are the most popular metric to measure fidelity [5].

II. Basic Theory of Watermarking

The objective of digital watermarking is to embed or insert a message into a signal in a secure and imperceptible manner and to detect the embedded information from a watermarked signal [1][2]. A watermarked image may be attack or distorted before it is available to the watermark detector. A block diagram of a typical watermarking system is shown in Figure 1. In the following, we show watermarking. The original image and the desired watermark are embedded using one of the various schemes that are currently available. The obtained watermarked image is passes through a decoder in which usually a reverse process to that employed during the embedding stage is applied to retrieve the watermark. The different techniques differ in the way in which it embeds the watermark on to the cover object. A secret key is use during the embedding and the extraction process in order to prevent illegal access to the watermark.

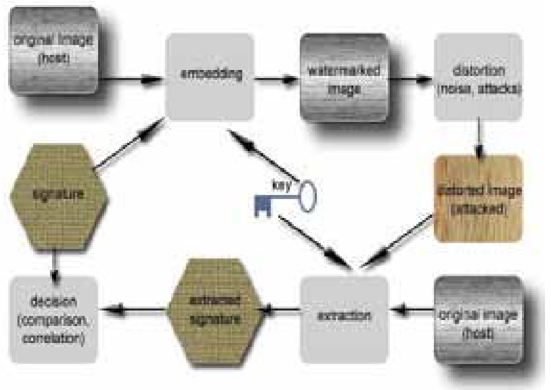


Figure 1. Typical Watermarking block diagram

III. Types of Watermarking

A digital watermark is a distinguishing piece of information that is assign to the data to be protect. One important requirement by this is that the watermark cannot easily extract or removed from the watermarked object. Watermarks and watermarking techniques can classify into several categories taking into account by this various criteria (see Figure 2 in which the types of Watermarks are present). As it can note, one of the criteria is embedding domain in which the watermarking is implement [3]. For example, watermarking can do in the spatial domain. An alternative possibility is the watermarking in the frequency domain.

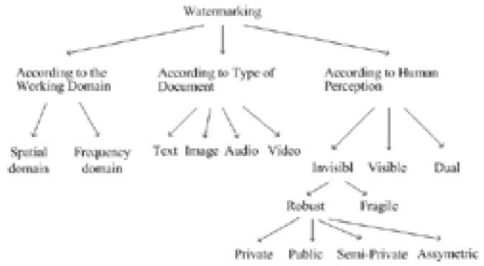


Figure 2. Types of watermarking methods

Watermarking techniques can classify into the following four categories according to the type of the multimedia document to watermark. According to the human perception, digital watermarks can classify into three different categories, like *Visible, Invisible-Robust watermark, Invisible-Fragile watermark, Dual watermark.*

IV. Transform Domain Watermarking

An advantage of the spatial techniques discussed above is that they can easily applied to any image; regardless of subsequent processing, (whether they survive this processing however is a different matter entirely). A possible disadvantage of spatial techniques is they do not allow for the exploitation of this subsequent processing in order to increase the robustness of the watermark.

Watermarking algorithm using transform domain techniques focus on embedding information in the frequency domain of the image as opposed to the spatial domain. The most popular transforms where the frequency domain watermarking algorithms work are Fourier Transform (FT), Discrete Cosine Transform (DCT) and Wavelet Transform (WT). These are applies to transform an image into the frequency domain where the coefficients of the digital image are separated into different priorities in accordance to the human perception system. The watermark bits embed by modulating the magnitude of these co-efficient.

A. Discrete Cosine Transform

Discrete cosine transformation (DCT) transforms a signal from the spatial into the frequency domain by using the cosine waveform [4]. DCT concentrates the information energy in the bands with low frequency, and therefore shows its popularity in data compression techniques such as JPEG and MPEG, and digital watermarking techniques.

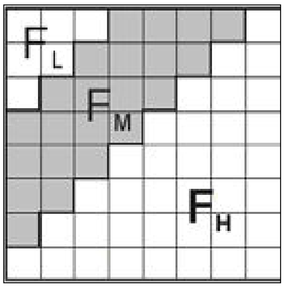


Figure 3. Discrete Cosine Transform region

Two-dimensional DCT of an image with size M x N and its inverse DCT (IDCT) is define in Equations (1) and (2), respectively.

$$F(jk) = a(j)a(k)\sum_{n=0}^{N-1}\sum_{m=0}^{N-1} f(mn) cos\frac{(2m+1)j\pi}{2N} \, cos\frac{(2n+1)j}{2N} \quad (1)$$

$$Where \; a(j) = \sqrt{\frac{1}{M}} \quad for \; m = 0$$

$$a(j) = \sqrt{\frac{2}{M}}$$

$$a(j) = \sqrt{\frac{2}{M}}$$

$$F(jk) = \sum_{n=0}^{N-1}\sum_{m=0}^{N-1} a(j)a(k)F(jk)\cos\frac{(2m+1)j\pi}{2N} \, co: \quad (2)$$

B. Discrete Wavelet Transform

The wavelet transform has been extensively use in the application of image processing and several other applications. Compression, signal analysis, digital watermarking and signal processing have been some of the applications made practical in this field of study in the past few decades. Figure 4 shows basics of DWT approach for image processing.

Figure 4. Discrete Wavelet Transform Based approach for image

To understand the basic idea of the DWT we focus on one-dimensional signal. A signal splits into two parts, usually high frequencies and low frequencies. The edge component of the signal is largely confine in the high frequency part. The low frequency part is splits again into two parts of high and low frequency (analysis). This process is continuing until the signal has been entirely decomposed or stopped before by the application at hand. For compression and watermarking applications, generally no more than five decomposition steps are computing [3][6]. Furthermore, from the DWT coefficients, the original signal can be reconstructing. The reconstruction process (synthesis) called the inverse DWT (IDWT).

$$I_{W_{u,v}} = \begin{cases} W_i + \alpha|W_i|x_i & u,v \in \\ wi & u,v \in \end{cases} \quad (3)$$

V. Our Utilisation approach

The wavelet transform based watermarking technique divides the image into four sidebands - a low-resolution approximation of the tile component and the component's horizontal, vertical and diagonal frequency characteristics. The process can repeated iteratively to produce N scale transform.

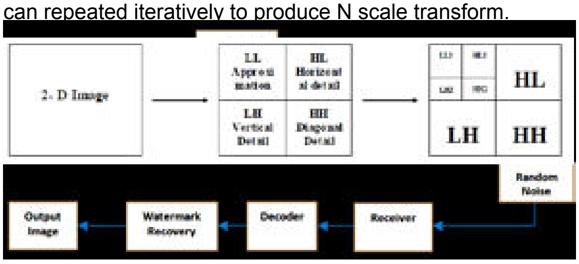


Figure 6. Embedding Approach

In the wavelet domain where *Wi* denotes the coefficient of the transformed image, *Xi* the bit of the watermark to be embedded, and α a scaling factor. To detect the watermark the same process as that used in DCT is implementing.

The characteristics of this transform domain are well suited for masking consideration since it is well localized both in time and frequency. The other important aspect of the technique used here is the way to introduce a watermark in an image. A watermark should introduce in perceptually significant regions of the data in order to remain robust. However, by doing so, we risk to alter the image (i.e. perceivably). The technique described here follows to a certain degree this requirement but tries to make the introduced watermark as invisible as it can while showing good robustness [7]. As the reader will understand, we have chosen to ensure transparency of the watermark and, in the same time keep the robustness by embedding the information within only the high and medium frequencies while keeping third resolution low frequencies, for which the HVS is most sensitive, untouched.

Similarly, discrete wavelet transform is a multi-resolution description of image. Hence, an image can shows at different level of resolution and can sequentially process from low resolution to high resolution. DWT is closer to the human visual system than the DCT, since it splits the signal into individual bands, which process independently.

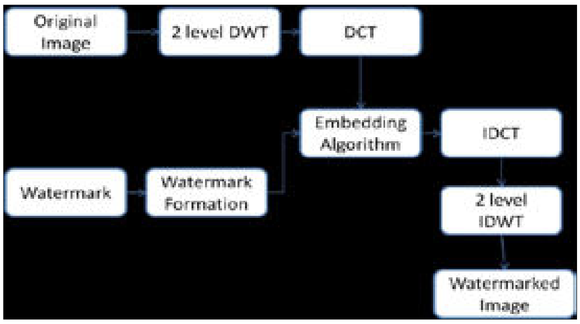


Figure 7. Extracting Approach

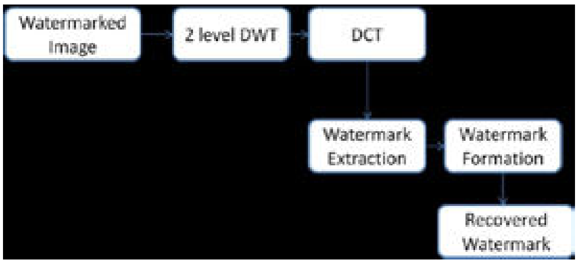
Watermarking schemes put more watermark energy into the large DWT coefficients, thus affecting mostly regions, like lines and texture on which the human visual system is not sensitive too [7]. DWT has spatial frequency locality, which means if the watermark is embedded into the DWT coefficients, it will affect the image locally. Hence, a wavelet transform provides both frequency and spatial description for an image [5].

According to properties and advantages of both DCT and DWT, an algorithm made to have advantages of both DCT as well as DWT. Our proposed block diagram of image watermarking technique using both DCT and DWT shows below.

VI. Results

Table 1 shows the simulated result of our utilization approach with different attacks in channel.

TABLE I. Simulation Result



Images	Parameters	
	PSNR	MSE
Watermarked Image	37.8815	10.5908
JPEG Comression Image	29.7529	68.8320
Blurring attack Image	26.2765	153.2597
Salt and Paper Noisy Image	23.7717	272.8389
Unsharp attack Image	18.6391	889.5409

VII. Conclusion

Experimental evaluation results show that combining the two transforms improved the performance of the watermarking algorithm. From the observation, we can say when we apply different attack on the channel peak signal to noise ratio decreases so the recovered result degraded but increase properties like robustness and concealing which very much affects in removal attacks like compression.

VIII. Future Work

Information is passes every day in our society. It is essential that interference in the communication of this information hiders the information from being received as little as possible. Error-correcting codes provide us with this ability. Error-correcting codes allow us to receive a piece of information, identify any errors, locate them, and correct them. Hamming code and cyclic codes are especially useful kind of error-correcting code. Error-correcting code theory has been use in areas outside of information communication.

REFERENCES

[1] Seitz J., Digital Watermarking For Digital Media, Information Science Publishing, United States of America, May 2005. [2] I. J. Cox, M. L. Miller, J. A. Bloom, "Digital Watermarking", Morgan Kaufmann Publishers, 2001. [3] Y. Kim, Kwon, and R. Park, "Wavelet Based Watermarking Method for Digital Images Using the Human Visual System", Proceeding of IEEE International symposium on circuits and systems,Vol. 4, pp. 80-83. July 1999. [4] Lin, S. and C. Chin, "A Robust DCT-based Watermarking for Copyright Protection," IEEE Trans.Consumer Electronics, 46(3): 415-421, 2000. [5] A.M.Kothari, A.C.Suthar, R.S.Gajre. Performance Analysis of Digital Image Watermarking Technique-Combined DWT-DCT over individual DWT, Published in International Journal of Advanced Engineering & Applications, Jan. 2010. [6] Shital Gupta, Dr Sanjeev Jain A Robust Algorithm of Digital Image Watermarking Based on Discrete Wavelet Transform. Published in Special Issue of IJCCT Vol.1 Issue 2, 3, 4; 2010 for International Conference [ACCTA-2010], 3-5 August 2010. [7] Suthar A.C., Patel C.B. and Kulkarni G.R., "Implementation Of Image Security Issues Using Mixed Frequency Domain Scheme" in International Transactions on Electrical, Electronics and Communication Engineering, ISSN: 2249- 8923, November '11 - June '11, Volume 1, No 5, pp.18-23.