International Journal of Scientific Engineering and Applied Science (IJSEAS) - Volume-1, Issue-4,July 2015
ISSN: 2395-3470
www.ijseas.com

Performance of DWT based watermarking in presence of different attacks

Sweety Jangra[1], Pooja Ahlawat[2]
M.Tech student, Department of CSE, R.N College of Engineering & Management
Assistant Professor, Department of CSE, R.N College of Engineering & Management

ABSTRACT
Nowadays; with the rapid development of information technology, the use of digital information is increasing day by day. And it is challenging to protect this information from piracy and other types of attacks. Digital watermarking techniques have been developed to protect the copy right of multimedia such as audio, video and images. The success of a digital watermarking technology depends on its robustness to deal with different attacks that are aimed at removing or destroying the watermark from its host data. Watermarked images are affected by various attacks such as salt & pepper noise, Gaussian noise, blurring and rotation etc. These attacks destroy the inserted watermark, so that the copyright problem may arise. In this paper, DWT based watermarking using alpha blending is introduced. And we test the image watermarking methods by using statistical parameters such as peak-signal-to-noise-ratio (PSNR) and mean square error (MSE).

Keywords— Watermark, Cropping, Salt & Pepper Noise, Rotation, MSE, PSNR, DWT.

1 INTRODUCTION

Due to the rapid and massive development of multimedia and the widespread use of the Internet, there is a need for efficient, powerful and effective copyright protection techniques. A variety of image watermarking methods have been proposed, where most of them are based on the spatial domain or the transform domain. However, in recent years, several image watermarking techniques based on the transform domain are developed [1]. Digital watermarking is a branch of information hiding which is used to hide proprietary information in digital media like photographs, digital music, or digital video. The ease with which digital content can be exchanged over the Internet has created copyright infringement issues. Copyrighted material can be easily exchanged over peer-to-peer networks, and this has caused major concerns to those content providers who produce these digital contents. For an efficient watermarking method, it should be robust to compression, filtering, rotation, scaling cropping, and collusion attacks among many other digital processing operations. The existing digital image watermarking techniques can be grouped into two major classes' namely spatial domain Watermarking and Transform Domain Watermarking techniques. In this paper performance of 3-level DWT based watermarking using alpha blending is tested against different attacks. The rest of the paper is organized as follows: Section 2, focuses on overview of DWT based watermarking. Section 3, watermarking embedding and extraction process algorithms. In section 4, discuss about different attacks .in section 5, gives

experimental results and compares. In section 6, conclusion is drawn.

2 DWT BASED WATERMARKING

Discrete wavelet transform (DWT) of the image produces multi resolution representation of an image. The multi resolution representation provides a simple framework for interpreting the image information. The DWT analyses the signal at multiple resolution. Discrete Wavelet transform (DWT) is a mathematical tool for hierarchically decomposing an image. It gained widespread acceptance in signal processing, image compression & watermarking. It decomposes a signal into a set of basic functions, called wavelets. Wavelets are created by translations and dilations of a fixed function called mother wavelet [5].

2.1 DWT BASED WATERMARKING EMBEDING AND EXTRACTION PROCESS

2.1.1 Concept of Watermark Embedding process

For this process firstly the colour image is read and converts it into a gray scale host image and 2-D, 3-level DWT (Discrete Wavelet Transform) is applied to the image. In case of two-dimensional image, after a DWT transform, the image is divided into four corners, upper left corner of the original image, lower left corner of the vertical details, upper right corner of the horizontal details, lower right corner of the component of the original image detail (high frequency). You can then continue to the low frequency components of the same upper left corner of the 2nd, 3rd inferior wavelet transform. In the same manner 2-D, 3-level DWT is also applied to the watermark image which is to be embedded in the host image. For this Haar wavelet is used. Then technique alpha blending is used to insert the watermark in the host image. In this technique the decomposed components of the host image and the watermark are multiplied by a scaling factor and are added. Since the watermark embedded in low frequency approximation Component of the host image so it is perceptible in nature or visible. Alpha blending: formula of the alpha blending the watermarked image is given by

WMI=k*(LL3) +q*(WM3)

WM3 = low frequency approximation of Watermark, LL3 = low frequency approximation of the original image, WMI=Watermarked image, k, q-Scaling factors.

After embedding the cover image with watermark image, 3-level Inverse discrete wavelet transform is applied to the watermarked image coefficient to generate the final secure watermarked image..

2.2.2 Concept of Watermark Extraction process

The extraction algorithm process is the inverse of the embedding process. In this process firstly 3-level DWT is applied to watermarked image and cover image which decomposed the image in sub-bands. After that the watermark is recovered from the watermarked image by using the formula of the alpha blending. According to the formula of the alpha blending the recovered image is given by

RW = (WMI - k * LL3) (2)

Where RW= Low frequency approximation of Recovered watermark, LL3= Low frequency approximation of the original image, and WMI= Low frequency approximation of watermarked image. After extraction process, 3-level Inverse discrete wavelet transform is applied to the watermark image coefficient to generate the final watermark extracted image.

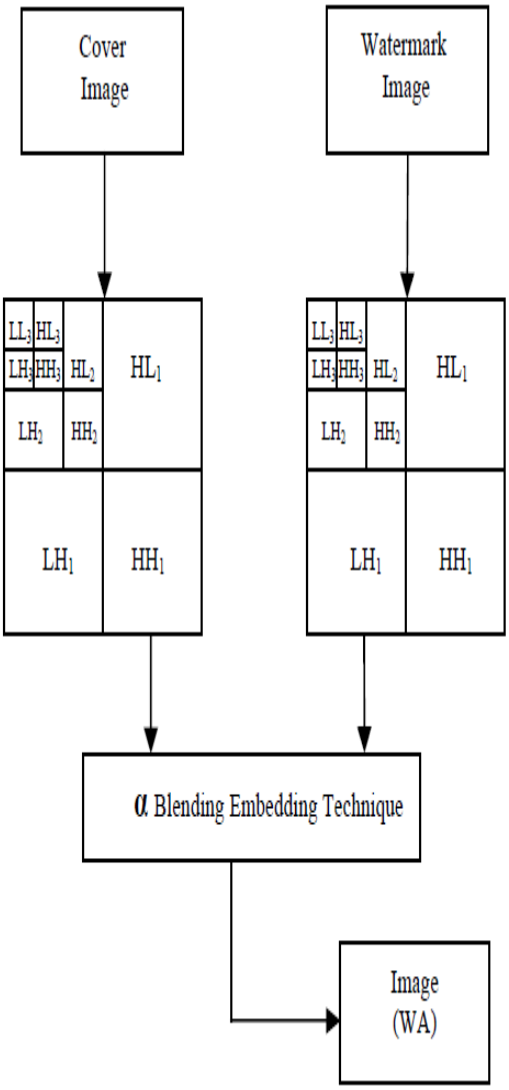

Fig -2.1 Watermark embedding technique

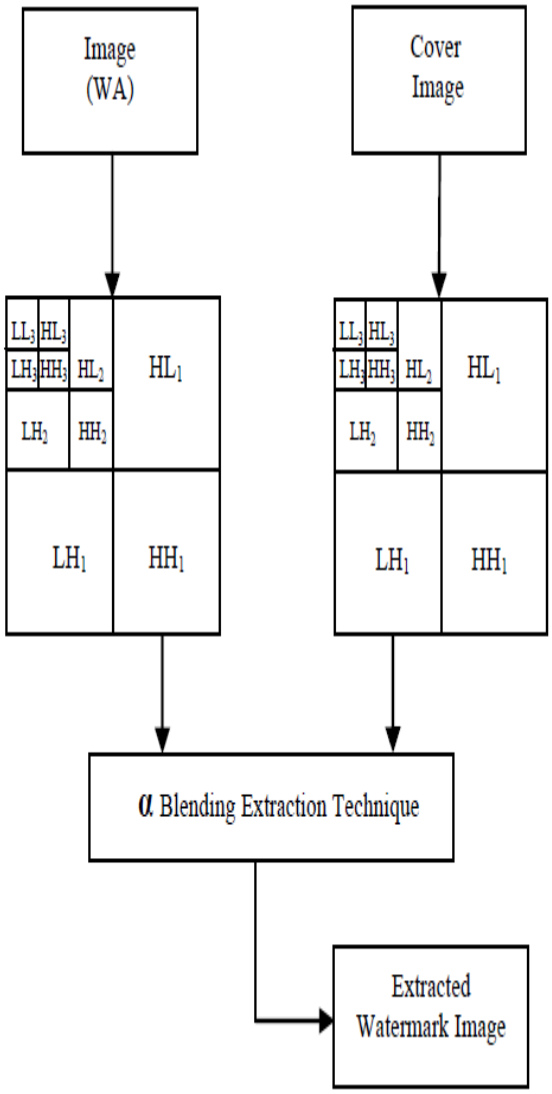

Fig -2.2 Watermark extraction technique

3 WATERMARK ATTACKS

Additive Noise: This may be from the use of D/A and A/D converters or from transmission errors. However, an attacker may introduce perceptually shaped noise (thus, imperceptible) with the maximum unnoticeable power. This will increase the threshold at which the correlation doctor works.

Filtering: Low pass filtering, for instance, does not introduce considerable degradation in watermarked images or audio, but can dramatically affect the performance, since spread spectrum like watermarks have a non-negligible high frequency spectral content.

Cropping: This is very common attack in many cases the attacker is interested in a small portion of the watermarked object, such as parts of a certain picture or frames of a video sequence. With this in mind, the watermark needs to be spread over the dimensions where this attack takes place.

Compression: This is an unintentional attach which appears in multimedia applications. Al the audio, video and images that are currently being distributed via internet has been compressed. If the watermark is required to resist different levels of compression, it is advisable to perform the watermark insertion task in the same domain where the compression takes place. For instance, DCT domain image watermarking is more robust to JPEG compression than spatial domain watermarking.

Rotation and Scaling: Correlation based detection and extraction fail when rotation or scaling is performed on the watermarked image because the embedded watermark and the locally generated version do not share the same spatial pattern anymore.

Statistical Averaging: An attacker may try to estimate the watermark and then 'unwater mark' the object by subtracting the estimate. This is dangerous if the watermark does not depend substantially on the data. Note that with different watermarked objects it would be possible to improve the estimate by simple averaging. This is a good reason for using perceptual masks to create the watermark.

Multiple Watermarking: An attacker may watermark an already watermarked object and later make claims of ownership. The easiest solution is to timestamp the hidden information by a certification authority.

- **Attacks on Other Levels:** There are a number of attacks that are directed to the way the watermark is manipulated. For instance, it is possible to circumvent copy control mechanism discussed below by super scrambling data so that the watermark is lost or to deceive web crawlers searching for certain watermarks by creating a presentation layer that alters the way data are ordered. The latter is sometimes called 'mosaic attack'.

4. EXPERIMENTAL RESULTS AND COMPARES

Different types of attacks have been performed using MATLAB. It will be too huge to include all attacks within the scope of this Dissertation. Hence, some attacks have been selected to represent categories of attacks such as Gaussian noise attack, Salt and Pepper noise attack, image rotation, image flip, JPEG compression, image blur etc. The JPEG Compression is applied with quality factor where the quality means the amount of degradation in the image to indicate the robustness of the proposed schemes against JPEG compression. The Gaussian noise is applied over the watermarked image 0.05 variance, where the variance of the noise is a function of the image intensity values in the watermarked image. The salt and peppers noise is add with noise intensity of 0.5. Rotation applying a 90^{o} degree of rotation on the image will lead to a full damage to the watermark information. To blur the image we have been use motion blur effect. And a flip effect is also used as an attack.

Test images

Fig 4.1 Test images peppers, puppy, baboon and cherry

The algorithm of watermark embedding and extraction are implemented using MATLAB. Peppers.jpg image of size 256x256 is selected as the cover image. Cherry.jpg, baboon.jpg and puppy.jpg images of different sizes are used as the watermark image. The MSE and PSNR of the watermarked image and recovered image are calculated. The value of scaling factor k is 0.6 to 1.5 for embedding and k is in between 0.6 to 1.4 for extraction of image from watermarked image. Table 5.1 and Table 5.2 show the performance of 3-level DWT watermarking under different attacks.

EMBEEDING		
TYPE OF ATTACK	**MSE**	**PSNR**
No attack	0.084	25.29
Salt and pepper noise(0.5)	0.0125	47.10
Gaussian noise(0.05)	0.0015	66.60
Motion blur effect	0.0033	57.11
Flip effect	0.0146	43.06

Table 4.1 Performance of DWT watermarking Embedding Image using MSE and PSNR under different attacks

RECOVERED		
TYPE OF ATTACK	**MSE**	**PSNR**
No attack	42.22	4.53
Salt and pepper noise(0.5)	10.48	17.66
Gaussian noise(0.05)	13.36	10.71
Motion blur effect	7.15	21.90
Flip effect	7.33	21.62

Table 4.2 Performance of DWT watermarking Recovered Image using MSE and PSNR under different attacks.

It has been found that 3-level DWT algorithm is robust to different attacks. Under normal conditions, when there is no attack, provide best result with highest PSNR value. Which shows that the embedded watermark is imperceptible and do not degrade the quality of the image in which the watermark is embedded. And with noise attack (Salt and Pepper noise) extracted watermark and original watermarked image withstand the noise attack. But give worst PSNR value for Gaussian noise. The experimental results show that the algorithm is robust to flip attack which performs best among all with highest PSNR value.

5. CONCLUSION FUTURE WORK

In this paper, an image watermarking technique based on a 3-level discrete wavelet transform has been implemented. This technique can embed the watermark into the image using alpha blending technique. Experiment result shows that

the quality of the watermarked image and the recovered watermark depend only on the scaling factors k and q. The DWT watermarking is resilient to different attacks and least robust to Gaussian noise. This tested algorithm has a good embedding capacity without reducing the quality of watermarked image after embedding process i.e. imperceptible watermark.

This algorithm can also be implemented using neural network, fuzzy logic and by using other image blending techniques to improve the performance. This watermarking algorithm can be improved for the color images. And this watermarking algorithm can be extended for Digital Watermarks that are resistive to all available attacks and image manipulation as we tested only four attacks.

REFRENCES

[1] Nallagarla.Ramamurthy#1 and Dr.S.Varadarajan "Image Watermarking Using 3-Level Discrete Wavelet Transform (DWT)" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (2) , 2012,3582-3587

[2]Sanjay Rawat1, Balasubramanian Raman2. A New Robust Watermarking Scheme For Color Images, IEEE 2nd International Advance Computing Conference 2010.

[3]. 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.

[4]. Athanasios Nikolaidis and Ioannis Pitas. Region-Based Image Watermarking, Published in IEEE Transactions on Image Processing, Vol. 10, No. 11, November, 2001.

[5]. I. J. Cox, M. L. Miller, J. A. Bloom, "Digital Watermarking", Morgan Kaufmann Publishers, 2001.

[6]. Chandra Mohan B and Srinivas Kumar S. Robust Multiple Image Watermarking Scheme using Discrete Cosine Transform with Multiple Descriptions. Published in International Journal of Computer Theory and Engineering, Vol. 1, No. 5, December, 2009.

[7]. 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.

[8]. Y. Kim, Kwon, and R. Park, "Wavelet Based Watermarking Method for Digital Images Using the Human Visual System",