Sample image watermarking study

K. B. Neelima, T. Saravanan

Abstract
Digital watermarking is the powerful solution to copyright protection of digital media. Digital watermarking is nothing but the process of embedding information as watermark, in to the digital content which is to be protected from unauthenticated copying. Digital watermarking is having some other applications as copyright protection, fingerprinting, owner identification etc. Application of watermarks is depending upon the types of watermarks classification such as fragile, robust, visible and invisible. The main requirements of digital watermarks are integrity, robustness and complexity. This paper presents the measure of recovered image quality in terms of signal to noise ratio and similarity ratio, two dimensional discrete cosines transform (DCT2) watermarking and two dimensional fast Fourier transform (FFT2) watermarking methods.

Keywords: Digital watermarking, discrete wavelet transform, discrete cosine transform, Fast Fourier transform

1. Introduction
Digital watermarking is a robust technique to overcome the shortcomings of various copyright laws for digital data. The specialty of watermark is that it remains with the cover image even if it is copied. It is very difficult for counterfeiters to remove or alter watermark to prove ownership or copyrights of data watermark even though if it is extracted and tested. As such the owner always has his data safe and secure. Our aim is to study different watermarking algorithms and comparing them to find the one which is the most reliable and resistant to all types of attack, such as scalar or geometric. Counterfeiters try attack the watermarked image results in degrade of the quality of watermarked image. Generally the attacks may be Gaussian and median filter, compression, scaling and rotation of watermarked image. Once watermarked is attacked it become very difficult to recover watermark from the watermarked image and even if it recovered it is not useful to prove the ownership and copyrights. So the main idea is to find those regions, which are known as patches, in the given image which are very stable and resistant to attacks.

2. Digital Image Watermarking
Watermarking is defined as, “the process of possibly irreversibly embedding information in a digital signal. The signal can be an image, audio, picture or video”. The embedded data will be detected or extracted from a multimedia application element. By the eighteenth century, in Europe paper watermarks are made and America more clearly utilizing. They were used as trademarks. Nowadays a number of companies are using watermarking technologies for a variety of applications [1].

A watermarking algorithm must be consistent over following properties and parameters: Transparency
The fundamental requirement for any Watermarking method is it should be transparent to the end user. Security: Watermark information shall only be accessible to the authorized parties.
Ease of embedding and retrieval: The computation need for the selected algorithm should be very less.
Robustness
Watermarking must be robust to all kinds for signal processing operations, attacks or unauthorized access.
Effect on bandwidth
Watermarking should be prepared in such a way that it should not increase the bandwidth required for transmission.
The sudden increase in watermarking interest is mostly due to the increase in concern over...
copyright protection of content. The first technology utilized by owners is cryptography. Cryptography is probably the common method of protecting digital data. The data is encrypted prior to transmission, and the extracted key is provided with the legitimate copies of the data. The encrypted file can then be made available via the Internet, but is useless to attacker without an appropriate key. Although copy prevention and copyright protection are the key factors behind research in the digital watermarking, there is a number of applications uses watermarking. These include broadcast monitoring, transaction tracking, authentication, copy control, and device control [1]. An effective authentication scheme must have the following features:

1. To be able to determine whether an image is altered or not.
2. To be locate the alteration on the image.
3. To be able to integrate authentication data with host image rather than as a separate format file.
4. The embedded authentication data should be invisible under normal viewing conditions.
5. To allow the watermarked image be stored in lossy-compression format [3].

3. Types of Watermarking
Some of the important types of watermarking based on different watermarks are given below.

Visible watermark
Visible watermarks are the extension of the concept of logos. That watermarks are applicable to images only. The watermarks cannot be removed by cropping. Visible watermarks degrade the quality of image. These watermarks have applications in areas like graphics, software interface and maps.

Invisible watermark
Watermark in this type is hidden in the image. The watermark can be extracted by authorized user only. These watermarks are used for content and/or author authentication and for detecting unauthorized copier.

Robust Watermark
In robust method, invisible watermarks are embedded and resist to image processing or attacks. These are using for copyright protection or ownership verification.

Fragile Watermark
Fragile watermarks are those watermarks which modified easily by any attempt to tamper with them. Fragile watermarks are attacked by data manipulation.

Semi Fragile Watermark
These are sensitive to signal modification. Feature of both robust & fragile watermark. These provides data authentication. Besides watermark robustness, the watermarking process can also be categorized into visible and invisible types, visible watermarks are perceptible to the user and invisible watermarks are imperceptible. In this paper, invisible watermarks are considered because they have a wide range of applications compared to visible watermarks [4].

4. Distortions and Attacks
First of all, the reasons or purposes for an attack against a watermark image are, to weaken, remove or alter the watermark, and attacks which occurs during image processing and not tampered the watermark. Lossy image compression is considered the common form of attack. Removal attacks attempt to remove or separate the watermark. The removing of the watermark from the data, this is known as a removal attack. The goal of attack is to add noise or distortion to the cover image in order to make the watermark undetectable [4]. The attack is successful if the watermark is not detected anymore. Some of these types of attacks are:

- Lossy image JPEG compression
- Gaussian noise Addition
- De-noising
- Filtering
- Median filtering and blurring
- Signal enhancement (sharpening, contrast enhancement)
- Geometrical attacks
- Cryptographic attacks
- Protocol attacks

In our work we use removal attacks, to compare the different techniques, image is compressed using JPEG compression; also we add Gaussian noise and salt and pepper noise to the watermarked image and then we filtering it using median filter.

5. Quality Measurements
In order to evaluate the quality of watermarked image, the signal to noise ratio (SNR) equation is used

\[
SNR = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} I(i,j)^2}{\sum_{i=1}^{M} \sum_{j=1}^{N} [I(i,j) - AW(i,j)]^2}
\]

OR,

\[
SNR_{dB} = 10 \times \log_{10} \left( \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} I(i,j)^2}{\sum_{i=1}^{M} \sum_{j=1}^{N} [I(i,j) - AW(i,j)]^2} \right)
\]

The number of mismatching data between inserted watermark and extracted watermark is represented as the similarity of watermarks. The similarity factor of extracted watermark and inserted watermark is computed by the following

\[
SF = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} (W(i,j)^2 - W^*(i,j)^2)}{\sqrt{\sum_{i=1}^{M} \sum_{j=1}^{N} W(i,j)^2 \times \sum_{i=1}^{M} \sum_{j=1}^{N} W^*(i,j)^2}}
\]

Where \( W \) and \( W^* \) represent the inserted watermark image and the extracted watermark image, respectively, \( M \) and \( N \) represent the image size. The range of SF in magnitude is [0, 1]. SF is near or equals to 1, the extracted watermark is effective extraction. In general, acceptable value of SF is 0.75 or above.

6. Sample Watermarking Techniques

DCT Domain Watermarking
The image can be represented as a sum of the sinusoids of varying magnitudes and frequencies. In DCT, the significant information of the image is concentrated in some coefficients of the DCT. Common problem with DCT watermarking algorithm is block by block scaling of watermark image results in visual discontinuity [9]. In this paper, a visible watermarking technique is proposed that modifies the DCT coefficients of the host image. We have also proposed a modification to make the watermark more robust.

FFT Domain watermarking
The Fourier Transform is an important image processing tool which decomposes an image into sine and cosine terms. The transformation output represents the image in the frequency or Fourier, where the input image is in spatial domain. In the Fourier domain image, each pixel represents a particular frequency contained in the spatial domain image [10]. The Fourier Transform is used in wide range of applications, as
7. Results
The visual quality is measured using the Signal to Noise Ratio (SNR); SNR measure is the estimation of the quality of the extracted image compared with an embedded image. Reconstructed image with higher metric are judged as having better quality. The visual quality of extracted visual watermarks is measured by the Similarity Factor (SF). The compression ratio (CR) is defined by compression Ratio=image bytes/compressed bytes. For JPEG compression attack, CR is measured.

Figure shows the Lena image of 512X512 gray scale cover image and 512X512 watermark copyright.

![Copy Right](image.html)

**Fig 1:** a) Host Image  b) Watermark

**Table 1:** SNR Comparison between DCT & FFT for different types of attack

| Type of attack               | DCT scheme | FFT scheme |
|-----------------------------|------------|------------|
| JPEG 75                     | 88.1841    | 88.5531    |
| salt & peppers noise        | 31.7002    | 31.4703    |
| Gaussian noise              | 11.1045    | 11.162     |
| Rotating 35°                | 0.8822     | 0.8801     |
| Blurring                    | 16.1210    | 30.4845    |

The value of SNR in the table indicates that FFT is robust to blurring attack more than DCT but for other attacks are the same. In Table 2 we compare these methods with different types of attacks using SF as visual quality.

**Table 2:** Comparison between extracted watermarks using SF.

| Type of attack    | DCT scheme | FFT scheme |
|-------------------|------------|------------|
| JPEG 75           | 0.9998     | 0.9996     |
| Salt & peppers noise | 0.5511    | 0.5546    |
| Gaussian noise    | 0.2859     | 0.2881     |
| Rotating 35°      | 0.0925     | 0.0925     |
| Blurring          | 0.6195     | 0.6195     |

8. Conclusion
In this paper initially, we have general definition of digital image watermarking and discuss watermarking process in two frequency domain DCT and FFT and noticed that the process is the same but applied different transformation. Also observed that the two methods have the same robust, for all types of attack except blurring in that FFT is more robust than DCT.

9. References
1. [Http://Www.Scribd.Com/Doc/37021026/Project-Report-On-Digital-Watermarking](http://Www.Scribd.Com/Doc/37021026/Project-Report-On-Digital-Watermarking)
2. Minwu Bede Liu, “Watermarking for Image Authentication”, Department of Electrical Engineering, Princeton University, Princeton.
3. [Http://Homepages.Vub.Ac.Be/~Andooms/Research.Htm](http://Homepages.Vub.Ac.Be/~Andooms/Research.Htm)
4. [Http://Www.Alpvision.Com/Watermarking.Html](http://Www.Alpvision.Com/Watermarking.Html)
5. Edinmaharemagic And Borkofurht, “Survey of Watermarking Techniques and Applications”, Department Of Computer Science And Engineering, Florida Atlantic University.
6. AndrejasamˇCovi´C, J’Antur´An, “Attacks On digital wavelet image watermarks”, Journal of Electrical Engineering.
7. R. Gonzales, R. Woods “Digital Image Processing”, Addison-Wesley Publishing Company.