**A COMPARATIVE STUDY OF DWT AND DCT BASED IMAGE WATERMARKING TECHNIQUES**

SUBMITTED BY

**PRATIK SENGUPTA**

EXAMINATION ROLL NUMBER: M1TCS12-17

CLASS ROLL NUMBER: 001111003018

REGISTRATION NUMBER: 92373 of 2004-05

A THESIS SUBMITTED TO

THE FACULTY OF ENGINEERING & TECHNOLOGY OF JADAVPUR UNIVERSITY

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

**MASTER OF ENGINEERING**

IN

**SOFTWARE ENGINEERING**

UNDER THE SUPERVISION

OF

DR. BIBHAS CHANDRA DHARA

ASSISTANT PROFESSOR

DEPARTMENT OF INFORMATION TECHNOLOGY

JADAVPUR UNIVERSITY

2014

DEPARTMENT OF INFORMATION TECHNOLOGY

FACULTY OF ENGINEERING & TECHNOLOGY

**JADAVPUR UNIVERSITY**

CERTIFICATE OF SUBMISSION

I hereby recommend the thesis, entitled “**A Comparative Study of DWT and DCT based Image Watermarking Techniques**”, prepared under my guidance by Pratik Sengupta, be accepted in partial fulfilment of the requirements for the degree of Master of Engineering in Software Engineering of Jadavpur University.

-----------------------------------

Dr.Bibhas Chandra Dhara,

Assistant Professor,

Department of Information Technology,

Jadavpur University

Countersigned:

--------------------------------------

Head of the Department,

Department of Information Technology,

Jadavpur University

J**ADAVPUR UNIVERSITY**

DEPARTMENT OF INFORMATION TECHNOLOGY

FACULTY OF ENGINEERING & TECHNOLOGY

**CERTIFICATE OF APPROVAL**

The thesis at instance is hereby approved as a creditable study of an Engineering subject carried out and presented in a manner satisfactory to warrant its acceptance as a prerequisite to the degree for which it has been submitted. It is understood that by this approval the undersigned do not necessarily endorse or approve any statement made, opinion expressed or conclusion drawn therein, but approve this thesis for the purpose for which it is submitted.

Examiners:

............................................... ......................................... .........

(Signature of the examiner) (Signature of the supervisor)

**JADAVPUR UNIVERSITY**

**FACULTY OF ENGINEERING AND TECHNOLOGY**

**Declaration of Originality and Compliance of Academic Ethics**

I hereby declare that this thesis contains literature survey and original research work by the undersigned candidate, as a part of my Master of Software Engineering studies.

All information in this document have been obtained and presented in accordance with academic rules and ethical conduct.

I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Signature with Date

.............................................

Name : Pratik Sengupta

Roll Number : 001111003018

Thesis Title : A Comparative Study of DWT AND DCT Based Image Watermarking Techniques

**ACKNOWLEDGEMENT**

It has been a long journey by writing this thesis and the related work. I would like to thank a lot of people who gave me unending support and inspiration from the first day till the finishing of the thesis.

With my most sincere respect and gratitude, I would like to thank Dr. Bibhas Chandra Dhara, my guide, for the interesting subject he issued for this work and for his overwhelming support throughout the duration of this project. I would like to thank him for his valuable suggestions, guidance and encouragement which have helped me immensely in understanding the subject. His motivation always gave me the required inputs and momentum to continue my work, without which the project work would not have taken its current shape. His valuable suggestions and numerous discussions have always inspired new ways of thinking. I am highly grateful and I feel deeply honoured that I have got this opportunity to work with him.

I would like to thank all faculty members of the Department of Information Technology for their continuous support.

I would also like to thank my family, all my classmates and friends in Jadavpur University for the constant support and help they provided me all the time.

Regards,

Location: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: **Pratik Sengupta**

M.E. in Software Engineering

Class Roll No: **001111003018**

Exam Roll No: **M1TCS12-17**

Registration No: **92373 of 2004-05**

**ABSTRACT**

Image watermarking with both insensible detection and high robustness capabilities is still a challenging problem for copyright protection up to now. Many proposed methods are already there which are more efficient against certain type of attacks. This paper compares between two major Frequency Transform Watermarking approaches - Discrete Cosine Transform and Discrete Wavelet Transform based Watermarking in colored still image which are inherently collusion attack resistant.

Our DCT based Watermarking scheme for comparision is based on averaging of middle frequency coefficients of block DCT coefficients of an image which introduces high redundancy and can sustain malicious attacks. Experimental results show the robustness of the proposed scheme against the JPEG compression and other common image manipulations.

Whereas, the DWT based scheme is based on hiding the watermark data in blocks of the block segmented image by embedding the watermark data in the low pass wavelet coefficients of each block. Due to low computational complexity of the proposed approach, this algorithm can be implemented in real time. Experimental results demonstrate the imperceptibility of the proposed method and its high robustness against various attacks such as filtering, JPEG compression, cropping, noise addition and geometric distortions.

Finally we compare the results from the two schemes.

**Chapter 1**

**Introduction**

Nowadays, digital images can be copied and stored easily and without loss in fidelity. Therefore, it is important to use some kind of property rights protection system. With digital multimedia distribution over World Wide Web, authentications are more threatened than ever due to the possibility of unlimited copying. So, watermarking techniques are proposed for copyright protection or authentication of digital media. Many watermarking methods for images have been proposed [1]- [4].

More and more researchers are joining this area and number of publications is increasing exponentially. Most of the work is based on ideas known from spread spectrum communication [5] which is additive embedding a pseudo- noise watermark pattern and watermark recovery by correlation [6]. Cox et al suggested using the DCT domain [6], which has been extensively studied because this is the transform used in JPEG compression. Further advantage of using DCT domain includes the fact that frequency transform is widely used in image and video compression and DCT

coefficients affected by compression are well known.

This paper proposes an efficient use of middle-band coefficients exchange to hide the watermark data. This paper uses the idea of Middle Band Coefficient Exchange which was discussed by Koch and Zhao [8] and further explained by Johnson and Katezenbeisser [9]. Later Hsu and Wu also used

the DCT based algorithm to implement the middle band embedding [10]. Further one more efficient collusion attack resistant scheme has been presented based on middle-band coefficients exchange [7]. Collusion attack is the severe problem for some applications of watermarking like fingerprinting which involve high financial implications. So while designing a watermark scheme we are taking this attack as a prime. [11]- [12] Our main motivation behind selecting middle-band

coefficients exchange scheme as a base is that this scheme has proven its robustness against those attacks which any how do not affect the perceptual quality of an image such as JPEG compression.

Section 2 discusses the background studies. Chapter 3 describes the proposed method and Chapter 4 discusses the results.

**Background**

The term "digital watermark" was first coined in 1992 by Andrew Tirkel and Charles Osborne. Watermarks are identification marks produced during the paper making process. The first watermarks appeared in Italy during the 13th century, but their use rapidly spread across Europe. They were used as a means to identify the papermaker or the trade guild that manufactured the paper. The marks often were created by a wire sewn onto the paper mold. Watermarks continue to be used today as manufacturer's marks and to prevent forgery.

The information to be embedded in a signal is called a digital watermark, although in some contexts the phrase digital watermark means the difference between the watermarked signal and the cover signal. The signal where the watermark is to be embedded is called the host signal. A watermarking system is usually divided into three distinct steps, embedding, attack, and detection. In embedding, an algorithm accepts the host and the data to be embedded, and produces a watermarked signal.

Then the watermarked digital signal is transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called an attack. While the modification may not be malicious, the term attack arises from copyright protection application, where third parties may attempt to remove the digital watermark through modification. There are many possible modifications, for example, lossy compression of the data (in which resolution is diminished), cropping an image or video, or intentionally adding noise.

Detection (often called extraction) is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was unmodified during transmission, then the watermark still is present and it may be extracted. In robust digital watermarking applications, the extraction algorithm should be able to produce the watermark correctly, even if the modifications were strong. In fragile digital watermarking, the extraction algorithm should fail if any change is made to the signal.

**Research Objective**

**Contributions**

Our research work has the following contributions:

• We proposed a new scheme which applies Discrete Dosine Transform and Discrete Wavelet Transform and a hybrid approach to watermark an image. The scheme is robust against JPEG compression, cropping, rotation and other image attacks (see Chapter 4 for detail).

• We have experimented on these image watermarking schemes to test and

show its performance.

• We compare our proposed schemes with the existing scheme in different

aspects and discuss the advantages and the disadvantages of that.

**The Structure of this Thesis**

This Thesis is organized as 5 chapters. The next chapter introduces the issues

related to multimedia security and different image watermarking

techniques, and a survey on current watermark techniques. The proposed image watermarking schemes

are described in chapter 3 and the experimental results in Chapter 4 are followed

by. Finally, a conclusion is given in chapter 5.

**Chapter 2**

**Literature Survey**

Over the past few years, there has been tremendous growth in computer networks

and more specifically, the World Wide Web. This phenomenon, coupled with the

exponential increase of computer performance, has facilitated the distribution of

multimedia data such as images. Publishers, artists, and photographers, however, may be

unwilling to distribute pictures over the Internet due to a lack of security; images can be

easily duplicated and distributed without the owner’s consent. Digital watermarks have

been proposed as a way to tackle this tough issue. This digital signature could discourage

copyright violation, and may help determine the authenticity and ownership of an image.

In general, a digital watermark is a code that is embedded inside an image. It acts

as a digital signature, giving the image a sense of ownership or authenticity. Ideal

properties of a digital watermark have been stated in many articles and papers [13-15].

These properties include:

1. A digital watermark should be perceptually invisible to prevent obstruction of the
2. original image.
3. A digital watermark should be statistically invisible so it cannot be detected or erased.

Watermark extraction should be fairly simple. Otherwise, the detection process

requires too much time or computation.

1. Watermark detection should be accurate. False positives, the detection of a non-

marked image, and false negatives, the non-detection of a marked image, should be

few.

1. Numerous watermarks can be produced. Otherwise, only a limited number of images

may be marked.

1. Watermarks should be robust to filtering, additive noise, compression, and other

forms of image manipulation.

1. The watermark should be able to determine the true owner of the image.

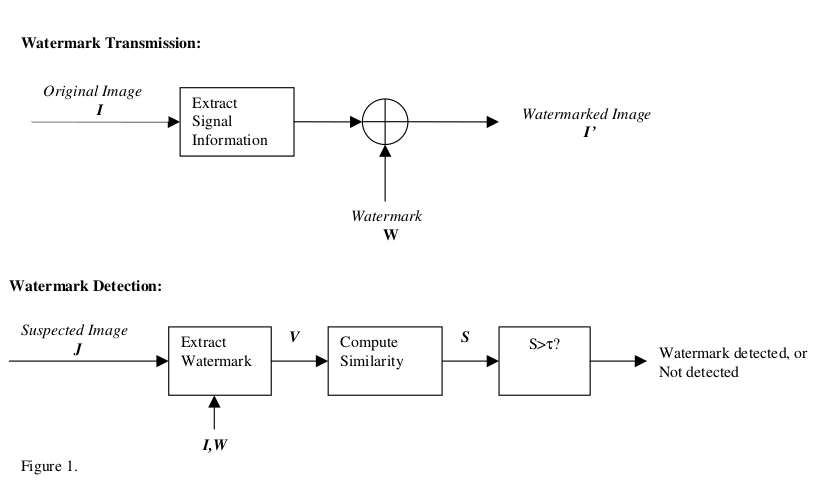


Figure 1 shows a general watermarking scheme. For transmission, the watermark

W is generated as a pseudo-random sequence to ensure statistical invisibility. Signal

information, such as DCT coefficients, are extracted from the original image I and

embedded into the information. The watermarked image I’ is formed with no visible

differences between I and I’.

For watermark detection, a suspected image J is taken and its signal information is

obtained. A suspected watermark V is extracted based on knowledge of the original

image I and the watermark W. A similarity measure S is performed on V and W.

Popular measures include the cross-correlation and correlation coefficient. Finally, S is

compared to a threshold τ. If S is larger than the threshold, then the watermark W is

detected. Otherwise, no watermark is detected.

**Security in Multimedia Communications**

**Steganography**

Steganography is the science of hiding information. Whereas the goal of cryptography is to make data unreadable by a third party, the goal of steganography is to hide the data from a third party.

There are a large number of steganographic methods that most of us are familiar with, ranging from invisible ink and microdots to secreting a hidden message in the second letter of each word of a large body of text and spread spectrum radio communication. With computers and networks, there are many other ways of hiding information, such as:

Covert channels (e.g., Loki and some distributed denial-of-service tools use the Internet Control Message Protocol, or ICMP, as the communications channel between the "bad guy" and a compromised system)

Hidden text within Web pages

Hiding files in "plain sight" (e.g., what better place to "hide" a file than with an important sounding name in the c:\winnt\system32 directory?)

Null ciphers (e.g., using the first letter of each word to form a hidden message in an otherwise innocuous text)

Steganography today, however, is significantly more sophisticated than the examples above suggest, allowing a user to hide large amounts of information within image and audio files. These forms of steganography often are used in conjunction with cryptography so that the information is doubly protected; first it is encrypted and then hidden so that an adversary has to first find the information (an often difficult task in and of itself) and then decrypt it.

**Digital Watermarking**

**Image Watermarking**

**Fidelity**

**Robustness**

**Statistical Imperceptibility**

**Low Error Probability**

**Real-time Detector Complexity**

**Reviews on Image Watermarking Techniques**

**Spatial Domain Watermarks**

**Modification of the Less-Significant-Bit**

**(LSB)**

: It is a simple approach to superimpose the watermark logo on the Least Significant Bit of the host image. It involves replacing **n** LSB of host image with data of the message to hide.

**Statistical Approximation:** It deals with the modification of some

statistics of the image to keep information. A simple

example would be the increase and decrease of

brightness of certain pixels of the image. The pixel

selection is determined by a pseudorandom number

generator. In this way, the statistic of the difference

between two pixels from the image taken randomly is

altered.

**Texture Block Encoding:** It consist on selecting and copying a portion

of the image determined by texture (herbs, asphalt, etc)

in other area of the image with similar characteristics.

In this way two zones with identical textures can be

obtained from the image. To detect these regions in a

watermarked image it will suffice to calculate the

image self-correlation to detect the position, and

subtract the image itself but shifted to the position

indicated by the self-correlation. After this process,

zones where the difference is 0 can be appreciated. The

geometrical form described by the profile of the copied

zone may be the watermark (industry name,

geometrical figure, etc). If the entire image suffers a

uniform transformation, both regions will be affected

in the same way and it will be possible to detect these

two equal parts. However, this method requires a

visual inspection to detect possible zones to copy, and

the visual impact that the process produces.

**Frequency Domain Watermarks**

These schemes hide information in

frequencies domain of the images, changing the value

of the spectral coefficients. Most of these approaches

are inspired in coding and compression methods (DCT,

DFT and DWT).

**Discrete Cosine Transform**

A discrete cosine transform (DCT) expresses a finite sequence of data points in terms of a sum of cosine functions oscillating at different frequencies. The most common variant of discrete cosine transform is the type-II DCT, which is often called simply "the DCT", its inverse, the type-III DCT, is correspondingly often called simply "the inverse DCT" or "the IDCT".

**Discrete Wavelet Transform**

**Discrete Fourier Transform**

**Chapter 3**

**Discrete Cosine Transform based schemes:**

**Discrete Wavelet Transform based schemes:**

In [15] a novel method is presented for audio watermarking.

In this method the host signal in transform domains is modified with respect to the binary watermark signal (0 or 1).

The embedding processes used in this method can be summarized as follows:

 Windowing the host signal.

 Applying the wavelet transform to each frame.

 Embedding the watermark bit of 1 or 0 to a number

of wavelet coefficients, W(i), of each frame based on

the following equations:

W'(i) = W(i).a For embedding 1 (1)

W'(i) = W(i)/a For embedding 0 (2)

where a is the strength factor.

 Inverse wavelet transforming the resulted coefficients of each frame.

In the detection process, the embedded data is detected by the following process:

 Windowing the original and received signal and Applying the wavelet transform to each frame of them.

 Calculating a compare vector by dividing the wavelet coefficients of the received signal to the original one.

 Detecting the embedded bit by comparing the vector which is calculated in the second step with a threshold level. If the majority of the vector components is larger than the threshold level, the embedded bit would be 1, otherwise 0 is detected It is proved in [16] that as the embedding process is symmetrical, the best threshold value is (a + 1/a). 1/2

**Watermark embedding**

The embedding processes used in this method can be summarized as:

 Segmenting the original image to small non-overlapping blocks and then applying the wavelet transforming to each block.

 In each block, the wavelet coefficients in the last

lowpass scale are modified for embedding 1 or 0 based on (1) and (2).

 Applying the inverse wavelet transform to the obtained wavelet coefficients.

**Watermark detection**

The detection process can be described as follows:

 Block segmenting of the received and the original image and applying the wavelet transform to each block for the both images.

 Calculating the comparing matrix by dividing the wavelet coefficients of the received image to the original one.

 Detecting the embedded bit by comparing the matrix which is calculated in the second step with a threshold level. If the majority of the matrix components is larger than the threshold level, the embedded bit would be 1, otherwise 0 is detected.

We use the threshold level of (a + 1/a). 1/2 , same as [16].

**Hybrid Watermarking Schemes**

In this proposed scheme we convert the image into DWT domain followed by a 1D – DCT. This watermarking scheme is blind in nature meaning that it doesnot require the original Cover Image or even the watermark logo to recover the watermark.

**Chapter 4**

**Experimental Results**

**Results of DWT Watermarking scheme:**

In this section we perform several experiments to test the proposed algorithms and evaluated its performance against various kinds of attacks. Throughout our experiments we choose the strength factor of a = 1.025. These factors are selected to maximize the robustness of this approach, while the modifications introduced by the watermarking process are imperceptible. We use Normalized Cross Correlation (NCC) to measure the performance of the watermarking scheme against attacks. A set of two common images were tested for our experiments. The images are illustrated in Figure 2a and 2b. Watermark Logo to embed is shown in Figure 2c.

|  |  |
| --- | --- |
| A description... | A description... |
| Figure 2a (Cover Image) | Figure 2b (Cover Image) |

|  |  |
| --- | --- |
| The Logo used for watermarking is shown here. It is a 32x32 pixel logo. | FA description...igure 2c |
| Logo scaled to 400% | Figure 2dA description... |

These two are 512×512 standard images: Lena and Mandrill

Their watermarked versions are shown in Figures 2b and 2c. As we see the imperceptibility of the watermarked images are satisfied, the mean PSNR (peak-signal-to-noise-ratio) of

the watermarked images are 71.01 dB, 80.19 dB

and \_\_\_\_dB respectively.

|  |  |
| --- | --- |
| A description... | A description... |
| Figure 2c (After Watermarking) | Figure 2d (After Watermarking) |
| NCC: 1 mse=0, psnr=71.91, psnrMax=71.01, snr=66.01 ber: 0 | NCC: 1 mse=0, psnr=80.19, psnrMax=77.5, snr=74.1 ber: 0 |

In the second experiment, we test the robustness of theis watermarking methods against JPEG compression

attacks. Figure 2e shows the resulted NCC for different images. As we see, the DWT method is highly robust against JPEG attacks.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **JPEG Compression/Metrics** | **Image Name** | **NCC** | **MSE** | **PSNR** | **PSNR Max** | **SNR** | **BER** |
| **100%** | Lena | 1.0 | 0.0 | Infinity | Infinity | Infinity | 0.0 |
| **90%** | Lena | 1.0 | 0.0 | Infinity | Infinity | Infinity | 0.0 |
| **80%** | Lena | 0.98 | 889.9 | 18.64 | 17.93 | 14.61 | 0.02 |
| **70%** | Lena | 0.97 | 1686.13 | 15.86 | 15.15 | 11.83 | 0.04 |
| **60%** | Lena | 0.96 | 2154.5 | 14.8 | 14.09 | 10.77 | 0.04 |
| **50%** | Lena | 0.93 | 3372.26 | 12.85 | 12.14 | 8.82 | 0.07 |
| **40%** | Lena | 0.89 | 5292.57 | 10.89 | 10.18 | 6.86 | 0.11 |
| **30%** | Lena | 0.85 | 7306.56 | 9.49 | 8.78 | 5.46 | 0.15 |
| **20%** | Lena | 0.76 | 0866.16 | 7.77 | 7.06 | 3.74 | 0.23 |
| **10%** | Lena | 0.61 | 18594.25 | 5.44 | 4.73 | 1.41 | 0.39 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **JPEG Compression/Metrics** | **Image Name** | **NCC** | **MSE** | **PSNR** | **PSNR Max** | **SNR** | **BER** |
| **100%** | Mandrill | 1 | 46.84 | 31.42 | 30.72 | 27.39 | 0 |
| **90%** | Mandrill | 0.99 | 702.55 | 19.66 | 18.95 | 15.63 | 0.01 |
| **80%** | Mandrill | 0.97 | 1358.27 | 16.8 | 16.09 | 12.77 | 0.03 |
| **70%** | Mandrill | 0.92 | 3840.63 | 12.29 | 11.58 | 8.26 | 0.08 |
| **60%** | Mandrill | 0.91 | 4636.85 | 11.47 | 10.76 | 7.44 | 0.1 |
| **50%** | Mandrill | 0.88 | 5807.78 | 10.49 | 9.78 | 6.46 | 0.12 |
| **40%** | Mandrill | 0.84 | 7681.25 | 9.28 | 8.57 | 5.25 | 0.16 |
| **30%** | Mandrill | 0.84 | 7587.58 | 9.33 | 8.62 | 5.3 | 0.16 |
| **20%** | Mandrill | 0.77 | 10866.16 | 7.77 | 7.06 | 3.74 | 0.23 |
| **10%** | Mandrill | 0.63 | 16954.96 | 5.84 | 5.13 | 1.81 | 0.35 |

|  |  |
| --- | --- |
|  | |
| Figure 2e (Line Graph – JPEG Compression Level vs NCC and BER) | |
| NCC: Normalized Cross Correlation | BER: Bit Error Rate |

|  |  |  |
| --- | --- | --- |
| **JPEG Compression Level** | **JPEG Compressed Image** | **Extracted Watermark** |
| JPEG Compressed Image with quality factor of 100% | A description... | A description... |
| JPEG Compressed Image with quality factor of 90% | A description... | A description... |
| JPEG Compressed Image with quality factor of 80% | A description... | A description... |
| JPEG Compressed Image with quality factor of 70% | A description... | A description... |
| JPEG Compressed Image with quality factor of 60% | A description... | A description... |
| JPEG Compressed Image with quality factor of 50% | A description... | A description... |
| JPEG Compressed Image with quality factor of 40% | A description... | A description... |
| JPEG Compressed Image with quality factor of 30% | A description... | A description... |
| JPEG Compressed Image with quality factor of 20% | A description... | A description... |
| JPEG Compressed Image with quality factor of 10% | A description... | A description... |
|  |  |  |

In the third experiment, the watermarks are tested against

additive white Gaussian noise attack with different noise

levels. The NCC results are shown in Figure 2f. Again, we

see that the proposed watermarking schemes are robust

against even high variance noise attack.

Robustness against rotation is the concept of the fourth experiment. Using template matching the rotation attack can be compensated by identifying the rotation angle and then rotating the image back. Therefore, the introduced distortion only comes from the interpolation due to image rotation. The NCC results are shown in Table 1. As we see even for large rotation angles our watermarking methods are still robust.

|  |  |  |
| --- | --- | --- |
| A description... | A description... | A description... |
| Watermarked Image rotated 7 degrees to right with respect to center. | Recovered Image | Extracted Watermark |

**Results of Hybrid Watermarking scheme:**

In this section we perform the above set of experiments to test our proposed algorithm and evaluate its performance against various kinds of attacks. Throughout our experiments we choose the strength factor of a = 10. These factors are selected to maximize the robustness of this approach, while the modifications introduced by the watermarking process are imperceptible. We use Normalized Cross Correlation (NCC) to measure the performance of the watermarking scheme against attacks. A set of two common images were tested for our experiments. The images are illustrated in Figure 2a and 2b. Watermark Logo to embed is shown in Figure 2c.

|  |  |
| --- | --- |
| A description... | A description... |
| Figure 2a (Cover Image) | Figure 2b (Cover Image) |

|  |  |
| --- | --- |
| The Logo used for watermarking is shown here. It is a 64x32 pixel logo. | A description...  Figure 2c |
| Logo scaled to 400% | A description...  Figure 2d |

Here also we have used the same set of images standard images: Lena and Mandrill

Their watermarked versions are shown in Figures 2b and 2c. As we see the imperceptibility of the watermarked images are satisfied, the mean PSNR (peak-signal-to-noise-ratio) of

the watermarked images are 71.03 dB, 72.06 dB

|  |  |
| --- | --- |
| A description... | A description... |
| Figure 2c (After Watermarking) | Figure 2d (After Watermarking) |
| NCC: 1 mse=0.01, psnr=71.03, psnrMax=70.14, snr=65.14 ber: 0.01 | NCC: 1 mse=0, psnr=72.06, psnrMax=69.37, snr=65.96 ber: 0 |

In the second experiment, we test the robustness of theis watermarking methods against JPEG compression

attacks. Figure 2e shows the resulted NCC for different images. As we see, the DWT method is highly robust against JPEG attacks.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **JPEG Compression/Metrics** | **Image Name** | **NCC** | **MSE** | **PSNR** | **PSNR Max** | **SNR** | **BER** |
| **100%** | Lena | 1 | 0 | ∞ | ∞ | ∞ | 0 |
| **90%** | Lena | 1 | 46.84 | 31.42 | 30.72 | 26.28 | 0 |
| **80%** | Lena | 0.97 | 1264.6 | 17.11 | 16.4 | 11.96 | 0.03 |
| **70%** | Lena | 0.93 | 2177.92 | 14.75 | 14.04 | 9.6 | 0.05 |
| **60%** | Lena | 0.93 | 2599.45 | 13.98 | 13.27 | 8.83 | 0.05 |
| **50%** | Lena | 0.88 | 4145.07 | 11.96 | 11.25 | 6.81 | 0.09 |
| **40%** | Lena | 0.81 | 7142.63 | 9.59 | 8.88 | 4.44 | 0.15 |
| **30%** | Lena | 0.69 | 11802.9 | 7.41 | 6.7 | 2.26 | 0.25 |
| **20%** | Lena | 0.51 | 21591.82 | 4.79 | 4.08 | -0.36 | 0.45 |
| **10%** | Lena | 0.46 | 24308.36 | 4.27 | 3.56 | -0.87 | 0.51 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **JPEG Compression/Metrics** | **Image Name** | **NCC** | **MSE** | **PSNR** | **PSNR Max** | **SNR** | **BER** |
| **100%** | Mandrill | 1 | 0 | ∞ | ∞ | ∞ | 0 |
| **90%** | Mandrill | 1 | 23.42 | 34.44 | 33.73 | 29.29 | 0 |
| **80%** | Mandrill | 0.97 | 1358.27 | 16.8 | 16.09 | 11.65 | 0.03 |
| **70%** | Mandrill | 0.94 | 2295.01 | 14.52 | 13.81 | 9.38 | 0.05 |
| **60%** | Mandrill | 0.91 | 3395.68 | 12.82 | 12.11 | 7.67 | 0.07 |
| **50%** | Mandrill | 0.89 | 4472.93 | 11.62 | 10.92 | 6.48 | 0.09 |
| **40%** | Mandrill | 0.83 | 6463.49 | 10.03 | 9.32 | 4.88 | 0.13 |
| **30%** | Mandrill | 0.76 | 10468.05 | 7.93 | 7.22 | 2.78 | 0.22 |
| **20%** | Mandrill | 0.61 | 18383.49 | 5.49 | 4.78 | 0.34 | 0.38 |
| **10%** | Mandrill | 0.52 | 25081.17 | 4.14 | 3.43 | -1.01 | 0.52 |

|  |  |  |
| --- | --- | --- |
| **JPEG Compression Level** | **JPEG Compressed Image** | **Extracted Watermark** |
| JPEG Compressed Image with quality factor of 100% | A description... | A description... |
| JPEG Compressed Image with quality factor of 90% | A description... | A description... |
| JPEG Compressed Image with quality factor of 80% | A description... | A description... |
| JPEG Compressed Image with quality factor of 70% | A description... | A description... |
| JPEG Compressed Image with quality factor of 60% | A description... | A description... |
| JPEG Compressed Image with quality factor of 50% | A description... | A description... |
| JPEG Compressed Image with quality factor of 40% | A description... | A description... |
| JPEG Compressed Image with quality factor of 30% | A description... | A description... |
| JPEG Compressed Image with quality factor of 20% | A description... | A description... |
| JPEG Compressed Image with quality factor of 10% | A description... | A description... |
|  |  |  |

The third experiment is on Blurring attack.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Gaussian Blur Radius/Metrics** | **Image Name** | **NCC** | **MSE** | **PSNR** | **PSNR Max** | **SNR** | **BER** | **Recovered Watermark** |
| **1** | Lena | 0.95 | 1967.15 | 15.19 | 14.48 | 10.04 | 0.04 | A description... |
| **2** | Lena | 0.91 | 2880.47 | 13.54 | 12.83 | 8.39 | 0.06 | A description... |
| **3** | Lena | 0.87 | 4168.49 | 11.93 | 11.22 | 6.78 | 0.09 | A description... |
| **4** | Lena | 0.81 | 6205.89 | 10.2 | 9.49 | 5.06 | 0.13 | A description... |
| **5** | Lena | 0.75 | 8009.11 | 9.09 | 8.39 | 3.95 | 0.17 | A description... |
| **1** | Mandrill | 0.95 | 1896.9 | 15.35 | 14.64 | 10.2 | 0.04 | A description... |
| **2** | Mandrill | 0.9 | 3302 | 12.94 | 12.23 | 7.8 | 0.07 | A description... |
| **3** | Mandrill | 0.84 | 4941.29 | 11.19 | 10.48 | 6.04 | 0.1 | A description... |
| **4** | Mandrill | 0.79 | 6510.33 | 9.99 | 9.29 | 4.85 | 0.14 | A description... |
| **5** | Mandrill | 0.74 | 8641.41 | 8.76 | 8.06 | 3.62 | 0.18 | A description... |

|  |
| --- |
|  |
| Figure showing results of NCC and BER on Gaussian Blur |

The fourth experiment is on Image Rotation.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Rotation Angle | Image Name | NCC | MSE | PSNR | PSNR Max | SNR | BER | **Recovered Watermark** |
| -7 | Lena | 0.88 | 4074.81 | 12.03 | 11.32 | 6.88 | 0.08 | A description... |
| -5 | Lena | 0.89 | 3302 | 12.94 | 12.23 | 7.8 | 0.07 | A description... |
| -3 | Lena | 0.91 | 3091.24 | 13.23 | 12.52 | 8.08 | 0.06 | A description... |
| -1 | Lena | 0.92 | 2927.31 | 13.47 | 12.76 | 8.32 | 0.06 | A description... |
| 1 | Lena | 0.91 | 2927.31 | 13.47 | 12.76 | 8.32 | 0.06 | A description... |
| 3 | Lena | 0.91 | 3419.09 | 12.79 | 12.08 | 7.64 | 0.07 | A description... |
| 5 | Lena | 0.9 | 3770.37 | 12.37 | 11.66 | 7.22 | 0.08 | A description... |
| 7 | Lena | 0.87 | 4355.83 | 11.74 | 11.03 | 6.59 | 0.09 | A description... |
| -7 | Mandrill | 0.9 | 3559.61 | 12.62 | 11.91 | 7.47 | 0.07 | A description... |
| -5 | Mandrill | 0.91 | 3700.12 | 12.45 | 11.74 | 7.3 | 0.08 | A description... |
| -3 | Mandrill | 0.9 | 3208.33 | 13.07 | 12.36 | 7.92 | 0.07 | A description... |
| -1 | Mandrill | 0.92 | 2903.89 | 13.5 | 12.79 | 8.35 | 0.06 | A description... |
| 1 | Mandrill | 0.92 | 2997.56 | 13.36 | 12.65 | 8.22 | 0.06 | A description... |
| 3 | Mandrill | 0.9 | 4262.16 | 11.83 | 11.13 | 6.69 | 0.09 | A description... |
| 5 | Mandrill | 0.89 | 3746.95 | 12.39 | 11.68 | 7.25 | 0.08 | A description... |
| 7 | Mandrill | 0.89 | 4379.25 | 11.72 | 11.01 | 6.57 | 0.09 | A description... |

|  |
| --- |
|  |
| Figure showing results of NCC and BER on Rotation Angle |

**Tests on Robustness**

**Experiment with Lossy Compression**

**Tests on Fidelity**

**Chapter 5**

**Conclusion**

In the previous chapters, we provided 3 watermarking schemes for watermarking still images.

The first scheme is DCT based semi-blind Watermarking scheme, second one is DWT based Watermarking scheme which requires the original cover image for watermark detection and the third one is a Hybrid Blind Watermarking scheme having a

DWT followed by a 1D DCT watermarking which does not require the original cover image or the logo. All these schemes are very robust especially

against JPEG compression and other common image manipulation and attacks. All the

schemes also achieve a very good balance in “Image-imperceptibility vs. Robustness”

trade-off and are ICAR in nature.

**Bibliography**

|  |  |
| --- | --- |
| [1] | F.Hartung, and M. Kutter, “Multimedia Watermarking techniques”,  Proceddings of IEEE, Vol. 87, No 7, July 1999, pp. 1079-1107. |
| [2] | M. Arnold, M. Schmucker, and S.D. Wolthusen, “Techniques and  application of Digital Watermarking and Content Protection”,  Eds.Northwood ,Artech House, 2003. |
| [3] | Saraju P. Mohanty , "Digital Watermarking: A Tutorial Review",  URL: http://www.csee.usf.edu/~smohanty/research/Reports/WMSurvey1999  Mohanty.pdf http://citeseer.ist.psu.edu/mohanty99digital.htm |
| [4] | W. Bender, D. Gruhl, N. Morimoto, and A. Lu. "Techniques for data  hiding". IBM Systems Journal, Vol. 35.(3/4), 1996, pp. 313-336. |
| [5] | P.G.Flikkema, “Spread Spectrum techniques for wireless  communication”, IEEE Signal Processing 14, pp. 26-36, May 1997. |
| [6] | I.J. Cox, J.Kilian, T.Leighton and T. Shamoon, “Secure Spread  Spectrum watermarking for Multimedia,” IEEE Tras. on Image  Processing , Vol. 6,No12, 1997, pp. 1673-1687. |
| [7] | Vikas Saxena, J.P. Gupta, “Collusion Attack Resistant Watermarking  Scheme for Images Using DCT” , (To be appear in the Proceedings of  IEEE 15th Signal Processing and Communication Applications  Conference, 11-13 June 2007, Turkey) |
| [8] | Z. Zhao, and E. koch, “Embedding Robust Labels Into Images For  Copyright Protection”, Proc. of International  Congress on  Intellectual Property Rights for Specialised Information, Knowledge  and New Technologies", Vienna, Austria, August 21-25,1995, pp. 242-  251. |
| [9] | N. Johnson, ,and S. Katezenbeisser, “A Survey of Steganographic  Techniques”, Eds.Northwood, MA:ArtecHouse,43, 1999. |
| [10] | C.T.Hsu, and J.L.Wu., “Hidden Singatures in Images”, Proc. IEEE  International Conf. on Image Processing, ICIP-96, Vol.3, pp.223-226. |
| [11] | Network Technology research Center, Nanyang Technological  University, Singapore, http://www.ntu.edu.sg/ntrc/research.htm |
| [12] | Collusion-resistant watermarking and fingerprinting,  US Patent Issued on June 13, 2006  http://www.patentstorm.us/patents/7062653.html |
| [13] | I. Cox, J. Kilian, F. Leighton, and T. Shamoon, “Secure Spread Spectrum  Watermarking for Multimedia,” IEEE Transactions on Image Processing, vol. 6,  no. 12, pp. 1673-1687, Dec. 1997. |
| [14] | M. Swanson, B. Zhu, and A. Tewfik, “Transparent Robust Image Watermarking,”  Proc. IEEE Int. Conf. on Image Processing, Sept. 1996, vol. III, pp. 211-214. |
| [15] | I. Pitas, “A Method for Signature Casting on Digital Images,” Proc. IEEE Int. Conf.  on Image Processing, Sept. 1996, vol. III, pp. 215-218. |
| [16] | M. A. Akhaee, S. GhaemMaghami, and N. Khademi, "A  Novel Technique for Audio Signals Watermarking in the Wavelet  and Walsh Transform Domains," in International Symposium on  Intelligent Signal Processing and Communication Systems  (ISPACS), Japan, Dec, 2006. |
|  |  |
|  |  |
|  |  |
|  |  |