ROBUSTNESS OF FREQUENCY DOMAIN IMAGE WATERMARKING AGAINST IMAGE PROCESSING ATTACKS

Chai Jee Sing

Degree of Master of Advanced Information Technology
2008
ROBUSTNESS OF FREQUENCY DOMAIN IMAGE WATERMARKING AGAINST IMAGE PROCESSING ATTACKS

CHAI JEE SING

A dissertation submitted
in partial fulfillment of the requirements for the degree of
Master of Advanced Information Technology

Faculty of Computer Science and Information Technology
UNIVERSITI MALAYSIA SARAWAK
2008
Abstract

Since there is an issue about none of robust digital watermarking uses the same robustness criteria, and consequently causes a non-practical comparison as well as slow down progress in this area. Generally, the schemes in spatial domain are usually less robust to attacks; while the schemes in frequency/transform domain are more robust to kinds of distortions. Synchronization errors can lead to significant performance loss of known image watermarking methods, which can be evidenced by the spurious effects that the suite of signal processing or transformation attacks contained in the benchmark software Stirmark. Thus, in order to provide a fair benchmark for image watermarking systems, a comparison technique using the most fundamental robust frequency domain schemes (DCT, DWT and FFT) are presented in this project. Experimental results provide the comparisons when two different sized watermarks are embedded into a grayscale image, and then show the watermark performance evaluation in such a way that fair comparisons between different frequency domain schemes are possible. Base on the performance of different watermarking schemes, a combination of watermarking scheme that is robust against both signal processing and transformation attacks is evaluated.
Abstrak

Kетидаan watermarking digital yang menggunakan kriteria ketahanan yang sama terhadap operasi pemprosesan digital, telah menyebabkan perbandingan yang tidak praktikal, dan juga memperlambankan perkembangan dalam bidang ini. Secara umumnya, skim watermarking dalam bidang ruangan (spatial) adalah kurang tahan terhadap serangan; sementara skim dalam bidang frekuensi adalah lebih tahan terhadap pelbagai jenis serangan. Kesan-kesan serangan pemprosesan isyarat dan transformasi dalam perisian Stirmark telah menyebabkan ralat dalam sinkronisasi yang boleh membawa kepada kehilangan prestasi bagi pelbagai kaedah watermarking bagi imej. Oleh itu, untuk memberikan perbandingan yang adil untuk sistem watermarking bagi imej, suatu teknik perbandingan dengan menggunakan skim bidang frekuensi yang tahan dan paling asas (DCT, DWT dan FFT) telah dipersyembahkan dalam projek ini. Keputusan eksperimen menunjukkan perbandingan dua jenis saiz watermark yang diselitkan dalam imej berwarna kelabu, dan kemudian menunjukkan penilaian watermark antara beberapa skim bidang frekuensi yang berlainan. Berdasarkan prestasi bagi skim watermarking yang berlainan, kombinasi skim watermarking yang tahan kepada kedua-dua jenis serangan pemprosesan isyarat dan serangan transformasi telah dinilaikan.
Acknowledgements

Hereby I extend my appreciation to many people who made this thesis possible. Special thanks are due to my supervisor Professor Dr. Wang Yin Chai. I would also like to acknowledge with much appreciation to Dr. Patrick Then Hang Hui. I am highly indebted to both of them for all the guidance, advices, helps and opinions for the research. Many thanks are due to Dr. Jane Labadin, and Dr. Wong Chee Weng, MAIT Programme Coordinator who always makes sure the proper running of this advance project. Many more persons including my family and friends who participated in various ways to ensure my research succeeded than those and I am thankful to them all.
Table of Contents

Abstract                                  ii
Abstrak                                   iii
Acknowledgements                          iv
Table of Contents                          v
List of Figures                            x
List of Tables                            xvii

Chapter 1  Introduction                   1
  1.1  Digital Watermarking                1
      1.1.1  Applications of Digital Watermarking  2
      1.1.2  Watermarking Requirements          3
  1.2  State-of-Art Watermarking Attacks   5
  1.3  Problem Statement                   6
  1.4  Research Motivation                 6
  1.5  Objective of Thesis                 7
  1.6  Scope of Thesis                     7
  1.7  Outline of Thesis                   8

Chapter 2  Literature Review             9
  2.1  Watermarking as Stenography System  9
  2.2  Watermarking Techniques            10
      2.2.1  Spatial vs. Frequency Domain      10
      2.2.2  Spatial Domain                   11
      2.2.3  Frequency Domain                 12
  2.3  DCT Domain Scheme                   13
2.4 DWT Domain Scheme 16
2.5 FFT Domain Scheme 19
2.6 Spread Spectrum 21
2.7 Watermarking Attacks 22
  2.7.1 Geometric and Signal Processing Attacks 23
2.8 Benchmarking of Watermarking Systems and the Shortcoming 24
2.9 Summary 24

Chapter 3 Methodology 26
3.1 Requirements for Watermarking System 27
3.2 Important Parameters and Variables of Different Watermarking System 31
3.3 Attacks on Watermark 32
3.4 Performance Evaluation and Representation 33
  3.4.1 Bit-Error vs. Attack Strength Graph 35
  3.4.2 Bit-Error vs. Visual Quality Graph 35
3.5 Software 35
  3.5.1 MATLAB 36
  3.5.2 StirMark 36
  3.5.3 Microsoft Visual C++ 35
3.6 Watermark-Object 37
3.7 Summary 38

Chapter 4 Results, Analysis and Discussion 39
4.1 Data Compilation for Performance Evaluation 39
  4.1.1 Bit-Error vs. Attack Strength 40
  4.1.2 Bit-Error vs. Visual Quality 45
4.2 Result Analysis & Discussion

4.2.1 Bit-Error vs. Attack Strength Graph Analysis

4.2.2 Robustness vs. Visual Quality Graph Analysis

4.3 Stirmark Attacks against Reference Image

4.4 Comparison-based Correlation in the DCT mid-band

4.4.1 Small Watermark Embed for DCT Mid-band Domain

4.4.2 Signal Processing Attacks for DCT Domain with Small Watermark

4.4.3 Transformation Attacks for DCT Domain with Small Watermark

4.4.4 Big Watermark Embed for DCT Mid-band Domain

4.4.5 Signal Processing Attacks for DCT Domain with Big Watermark

4.4.6 Transformation Attacks for DCT Domain with Big Watermark

4.5 CDMA Spread-Spectrum in the Wavelet Domain

4.5.1 Small Watermark Embed for DWT Domain

4.5.2 Signal Processing Attacks for DWT Domain with Small Watermark

4.5.3 Transformation Attacks for DWT Domain with Small Watermark

4.5.4 Big Watermark Embed for DWT Domain

4.5.5 Signal Processing Attacks for DWT Domain with Big Watermark
4.5.6 Transformation Attacks for DWT Domain with Big Watermark

4.6 Circular Symmetric Pattern in the 2-D Fourier Transform

4.6.1 Small Watermark Embed for FFT Domain

4.6.2 Signal Processing Attacks for FFT Domain with Small Watermark

4.6.3 Transformation Attacks for FFT Domain with Small Watermark

4.7 Robustness vs. Visual Quality

4.8 Processing Time

4.9 Robustness against Signal Processing and Geometrical Attacks

4.9.1 DWT-DFT Combination Watermarking

4.9.2 Result: DWT-FFT Domain against Signal Processing & Geometric Transformation

4.9.3 Discussion: DWT-FFT Domain Watermarking Scheme

4.9.4 Result: Bit-Error vs. Visual Quality for DWT-FFT Domain

4.9.5 Discussion: Robustness vs. Visual Quality for DWT-FFT Domain

4.9.6 Result: Robustness Result of DWT-FFT Domain with \( k = 3 \) and \( \alpha = 50000 \)

4.9.7 Discussion: DWT-FFT Domain Watermarking Scheme \( (K = 3 & \alpha = 50000) \)

4.9.8 Performance Comparison between DWT, FFT & DWT-FFT Combination Domain

4.10 Summary
4.11 Related Work

Chapter 5 Conclusions

5.1 Contribution

5.2 Future Research

References

Appendices

Appendix A: BER, Elapsed Time and PSNR for DCT Scheme

Appendix B: BER, Elapsed Time and PSNR for DWT Scheme

Appendix C: BER, Elapsed Time and PSNR for FFT Scheme

Appendix D: BER, Elapsed Time and PSNR with Fixed Attack for DCT Scheme

Appendix E: BER, Elapsed Time and PSNR with Fixed Attack for DWT Scheme

Appendix F: BER, Elapsed Time and PSNR with Fixed Attack for FFT Scheme

Appendix G: BER and PSNR for DWT-FFT Scheme

Appendix H: BER and PSNR with Fixed Attack for DWT-FFT Scheme

Appendix I: BER and PSNR for DWT-FFT Scheme (k=3 & alpha=50000)
List of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 1.1</td>
<td>Block Diagram of a Watermarking Algorithm</td>
<td>2</td>
</tr>
<tr>
<td>Figure 2.1</td>
<td>Illustration of a Steganographic System</td>
<td>9</td>
</tr>
<tr>
<td>Figure 2.2</td>
<td>Flowchart in spatial domain &amp; frequency domain</td>
<td>10</td>
</tr>
<tr>
<td>Figure 2.3</td>
<td>Definition of DCT Regions</td>
<td>13</td>
</tr>
<tr>
<td>Figure 2.4</td>
<td>DCT Flow Chart</td>
<td>16</td>
</tr>
<tr>
<td>Figure 2.5</td>
<td>2 Scale 2-Dimensional Discrete Wavelet Transform</td>
<td>17</td>
</tr>
<tr>
<td>Figure 2.6</td>
<td>DWT Flow Chart</td>
<td>19</td>
</tr>
<tr>
<td>Figure 2.7</td>
<td>Forming the Ring of Radius r</td>
<td>20</td>
</tr>
<tr>
<td>Figure 2.8</td>
<td>An Example of a Spread Spectrum Signal Used as a Digital Watermark</td>
<td>22</td>
</tr>
<tr>
<td>Figure 3.1</td>
<td>Criteria for Benchmarking Watermarking</td>
<td>26</td>
</tr>
<tr>
<td>Figure 3.2</td>
<td>35-digit &quot;key&quot; used as initial state of Matlab random number generator</td>
<td>30</td>
</tr>
<tr>
<td>Figure 3.3</td>
<td>Small Watermark (24 x 18 pixels) &amp; Big Watermark (50 x 20 pixels)</td>
<td>37</td>
</tr>
<tr>
<td>Figure 3.4</td>
<td>Lena Reference Image (512 x 512 pixels)</td>
<td>38</td>
</tr>
<tr>
<td>Figure 4.1</td>
<td>BER vs. JPEG Quality Graph for Small &amp; Big Watermark</td>
<td>41</td>
</tr>
<tr>
<td>Figure 4.2</td>
<td>BER vs. Noise Graph for Small &amp; Big Watermark</td>
<td>41</td>
</tr>
<tr>
<td>Figure 4.3</td>
<td>BER vs. Affine Graph for Small &amp; Big Watermark</td>
<td>41</td>
</tr>
<tr>
<td>Figure 4.4</td>
<td>BER vs. Flipping Graph for Small &amp; Big Watermark</td>
<td>42</td>
</tr>
<tr>
<td>Figure 4.5</td>
<td>BER vs. Convolution Filtering Graph for Small &amp; Big Watermark</td>
<td>42</td>
</tr>
<tr>
<td>Figure 4.6</td>
<td>BER vs. Cropping Graph for Small &amp; Big Watermark</td>
<td>42</td>
</tr>
<tr>
<td>Figure 4.7</td>
<td>BER vs. Median Filtering Graph for Small &amp; Big Watermark</td>
<td>43</td>
</tr>
<tr>
<td>Figure 4.8</td>
<td>BER vs. Rescaling Graph for Small &amp; Big Watermark</td>
<td>43</td>
</tr>
<tr>
<td>Figure 4.9</td>
<td>BER vs. Remove Lines Graph for Small &amp; Big Watermark</td>
<td>43</td>
</tr>
<tr>
<td>Figure 4.10</td>
<td>BER vs. Rotation Graph for Small &amp; Big Watermark</td>
<td>44</td>
</tr>
</tbody>
</table>
Figure 4.11: BER vs. Rotation-Crop Graph for Small & Big Watermark
Figure 4.12: BER vs. Rotation-Scale Graph for Small & Big Watermark
Figure 4.13: BER vs. PSNR_JPEG_15% Graph for Small & Big Watermark
Figure 4.14: BER vs. PSNR_Noise_20% Graph for Small & Big Watermark
Figure 4.15: BER vs. PSNR_HFlip Graph for Small & Big Watermark
Figure 4.16: BER vs. PSNR_VFlip Graph for Small & Big Watermark
Figure 4.17: BER vs. PSNR_Conv1(Gaussian) Graph for Small & Big Watermark
Figure 4.18: BER vs. PSNR_Conv2(Sharpening) Graph for Small & Big Watermark
Figure 4.19: BER vs. PSNR_Median(9x9) Graph for Small & Big Watermark
Figure 4.20: BER vs. PSNR_Rotation180 Graph for Small & Big Watermark
Figure 4.21: BER vs. PSNR_Affine8 Graph for Small & Big Watermark
Figure 4.22: BER vs. PSNR_Rescale50 Graph for Small & Big Watermark
Figure 4.23: BER vs. PSNR_Remove Lines100 Graph for Small & Big Watermark
Figure 4.24: BER vs. PSNR_Rotation-Crop0.25 Graph for Small & Big Watermark
Figure 4.25: BER vs. PSNR_Crop50 Graph for Small & Big Watermark
Figure 4.26: BER vs. PSNR_Rotation0.25 Graph for Small & Big Watermark
Figure 4.27: BER vs. PSNR_Rotation-Scale0.25 Graph for Small & Big Watermark
Figure 4.28: Reference Image and Watermark-Object without Any Processing
Figure 4.29: Stirmark Attacks against Reference Image
Figure 4.30: Watermarked Image & Recovered Small Watermark for DCT Domain
Figure 4.31: Noise & JPEG Compression for Small Watermark for DCT Domain
Figure 4.32: Median-Cut & Convolution filtering for Small Watermark for DCT Domain
Figure 4.33: Flipping for Small Watermark for DCT Domain
Figure 4.34: Remove Lines & Rotation for Small Watermark for DCT Domain
Figure 4.35: Rescaling & Affine for Small Watermark for DCT Domain
Figure 4.36: Cropping & Rotation-Crop for Small Watermark for DCT Domain
Figure 4.37: Rotation-Scale for Small Watermark for DCT Domain
Figure 4.38: Watermarked Image & Recovered Big Watermark for DCT Domain
Figure 4.39: Noise & JPEG Compression for Big Watermark for DCT Domain
Figure 4.40: Median-Cut & Convolution filtering for Big Watermark for DCT Domain
Figure 4.41: Flipping for Big Watermark for DCT Domain
Figure 4.42: Remove Lines & Rotation for Big Watermark for DCT Domain
Figure 4.43: Rescaling & Affine for Big Watermark for DCT Domain
Figure 4.44: Cropping & Rotation-Crop for Big Watermark for DCT Domain
Figure 4.45: Rotation-Scale for Big Watermark for DCT Domain
Figure 4.46: Watermarked Image & Recovered Small Watermark for DWT Domain
Figure 4.47: Noise & JPEG Compression for Small Watermark for DWT Domain
Figure 4.48: Median-Cut & Convolution filtering for Small Watermark for DWT Domain
Figure 4.49: Flipping for Small Watermark for DWT Domain
Figure 4.50: Remove Lines & Rotation for Small Watermark for DWT Domain
Figure 4.51: Rescaling & Affine for Small Watermark for DWT Domain
Figure 4.52: Cropping & Rotation-Crop for Small Watermark for DWT Domain
Figure 4.53: Rotation-Scale for Small Watermark for DWT Domain
Figure 4.54: Watermarked Image & Recovered Big Watermark for DWT Domain
Figure 4.55: Noise & JPEG Compression for Big Watermark for DWT Domain
Figure 4.56: Median-Cut & Convolution filtering for Big Watermark for DWT Domain
Figure 4.80: BER vs. Flipping Graph for DWT-FFT Domain 119
Figure 4.81: BER vs. Convolution Filtering Graph for DWT-FFT Domain 119
Figure 4.82: BER vs. Cropping Graph for DWT-FFT Domain 119
Figure 4.83: BER vs. Median Filtering Graph for DWT-FFT Domain 120
Figure 4.84: BER vs. Rescaling Graph for DWT-FFT Domain 120
Figure 4.85: BER vs. Remove Lines Graph for DWT-FFT Domain 120
Figure 4.86: BER vs. Rotation Graph for DWT-FFT Domain 120
Figure 4.87: BER vs. Rotation-Crop Graph for DWT-FFT Domain 120
Figure 4.88: BER vs. Rotation-Scale Graph for DWT-FFT Domain 120
Figure 4.89: Watermarked Image & Recovered Watermark for DWT-FFT Domain 121
Figure 4.90: Noise & JPEG Compression for DWT-FFT Domain 122
Figure 4.91: Median-Cut & Convolution filtering for DWT-FFT Domain 123
Figure 4.92: Flipping & Remove Lines for DWT-FFT Domain 124
Figure 4.93: Rotation & Rescaling for DWT-FFT Domain 125
Figure 4.94: Affine & Cropping for DWT-FFT Domain 126
Figure 4.95: Rotation-Crop & Rotation-Scale for DWT-FFT Domain 127
Figure 4.96: High-frequency drop-off at the edges of images 128
Figure 4.97: Fourier transform as deblurring function 129
Figure 4.98: BER vs. PSNR_JPEG_15% Graph for DWT-FFT Domain 130
Figure 4.99: BER vs. PSNR_Noise_20% Graph for DWT-FFT Domain 130
Figure 4.100: BER vs. PSNR_HFlip Graph for DWT-FFT Domain 130
Figure 4.101: BER vs. PSNR_VFlip Graph for DWT-FFT Domain 130
Figure 4.102: BER vs. PSNR_Conv1(Gaussian) Graph for DWT-FFT Domain 130
Figure 4.103: BER vs. PSNR_Conv2(Sharpening) Graph for DWT-FFT Domain 130
Figure 4.104: BER vs. PSNR_Median(9x9) Graph for DWT-FFT Domain 131
Figure 4.105: BER vs. PSNR_Rotation180 Graph for DWT-FFT Domain

Figure 4.106: BER vs. PSNR_Affine8 Graph for DWT-FFT Domain

Figure 4.107: BER vs. PSNR_Rescale50 Graph for DWT-FFT Domain

Figure 4.108: BER vs. PSNR_Remove Lines100 Graph for DWT-FFT Domain

Figure 4.109: BER vs. PSNR_Rotation-Crop0.25 Graph for DWT-FFT Domain

Figure 4.110: BER vs. PSNR_Crop50 Graph for DWT-FFT Domain

Figure 4.111: BER vs. PSNR_Rotation0.25 Graph for DWT-FFT Domain

Figure 4.112: BER vs. PSNR_Rotation-Scale0.25 Graph for DWT-FFT Domain

Figure 4.113: Watermarked Image with Maximum of Gain Factor/Alpha for DWT, FFT & DWT-FFT

Figure 4.114: Robustness vs. Visual Quality for DWT-FFT Domain

Figure 4.115: Watermarked Image & Recovered Watermark for DWR-FFT Domain

(alpha=50000 & k=3)

Figure 4.116: BER vs. JPEG Quality Graph for DWT-FFT Domain

(alpha=50000 & k=3)

Figure 4.117: BER vs. Noise Graph for DWT-FFT Domain

(alpha=50000 & k=3)

Figure 4.118: BER vs. Affine Graph for DWT-FFT Domain

(alpha=50000 & k=3)

Figure 4.119: BER vs. Flipping Graph for DWT-FFT Domain

(alpha=50000 & k=3)

Figure 4.120: BER vs. Convolution Filtering Graph for DWT-FFT Domain

(alpha=50000 & k=3)

Figure 4.121: BER vs. Cropping Graph for DWT-FFT Domain

(alpha=50000 & k=3)
Figure 4.122: BER vs. Median Filtering Graph for DWT-FFT Domain
(alpha=50000 & k=3) 139

Figure 4.123: BER vs. Rescaling Graph for DWT-FFT Domain
(alpha=50000 & k=3) 139

Figure 4.124: BER vs. Remove Lines Graph for DWT-FFT Domain
(alpha=50000 & k=3) 139

Figure 4.125: BER vs. Rotation Graph for DWT-FFT Domain
(alpha=50000 & k=3) 139

Figure 4.126: BER vs. Rotation-Crop Graph for DWT-FFT Domain
(alpha=50000 & k=3) 139

Figure 4.127: BER vs. Rotation-Scale Graph for DWT-FFT Domain
(alpha=50000 & k=3) 139
List of Tables

Table 2.1: Quantization values used in JPEG compression scheme 14
Table 3.1: Summary of Possible Perceptibility Assurance Levels 27
Table 3.2: Basic Robustness Requirements 29
Table 3.3: Different graphs and corresponding variables and constants 35
Table 4.1: Processing Time 115
Table 4.2: Performance Comparison of Watermarking Scheme for DWT, FFT &
           DWT-FFT(k=2 & alpha=45000) 141
Table 4.3: Performance Comparison of Watermarking Scheme for DWT, FFT &
           DWT-FFT(k=3 & alpha=50000) 142
Table 4.4: Summary Table of Results in General 143
Chapter 1  Introduction

The rapid expansion of the Internet in the past years has rapidly increased the availability of digital data such as audio, images and videos to the public. Digital data can be stored efficiently and with very high quality and it can be manipulated easily using computers. Furthermore, digital data can be transmitted in a fast and inexpensive way through data communication networks.

However, the rapid evolution of digital networks, digital libraries and other World Wide Web services is obstructed by digital data piracy. Unauthorized copying and distribution of digital data is a severe problem in protecting intellectual property rights (IPR), where the easy transmission and manipulation of digital data constitutes a real threat for information creators and distributors. Copyright owners want to be compensated every time that their work is used and they want to be sure that their works are not used in an improper way, e.g. modified without their permission. However, copyright enforcement and content verification are very difficult tasks.

The embedding of digital watermarks into multimedia content has been proposed to tackle this problem, and many different schemes have been presented in the last years. More about digital watermark, watermarking attack and the overview of this research are described in the following sections.

1.1  Digital Watermarking

Watermark is a digital code unremovably, robustly, and imperceptibly embedded in the host data and typically contains information about origin, status, and/or destination of the data (Hartung & Kutter, 1999). The goal is to produce a media that looks exactly the same to a human eye but still allows its positive identification in comparison with the owner's key if necessary.
The process for watermarking is shown in Figure 1.1 (Wolfgang & Delp, 1997).

![Figure 1.1 - Block Diagram of a Watermarking Algorithm](image)

### 1.1.1 Applications of Digital Watermarking

Watermarking is not restricted to just retaining information of the author in the work, there are various other purposes for which watermarking may be incorporated into an object. Some of them are (Vallabha, 2003):

- **Copyright Protection**: For the protection of intellectual property, the data owner can embed a watermark representing the copyright information in his data.

- **Fingerprinting**: To trace the source of illegal copies, the owner can use a fingerprinting technique. This requires the owner to embed different information onto copied of the work provided to different customers. The information embedded can be a serial number, customer id etc.

- **Copy protection**: The watermark represents a single copy prohibit bit and the watermark detectors in the recording device determine whether the data offered to the recorder can be stored or not.

- **Broadcast Monitoring**: By embedding watermarks in the commercials, an automated monitoring system can determine whether the commercial was broadcasted or not. Also other TV programs which might represent significant intellectual property such as the News.

- **Data Authentication**: Introducing fragile watermarks into the data can help ensure that the data is not processed or modified in anyway by the user.
• **Indexing**: Introducing watermarks in video mail, movies, news items can be used to index the data.

• **Data Hiding**: Watermarking may be used to embed longer bits of information in the data. The earliest form of this is was in ancient Greece, where an author could hide his name in the text of the literary work. The term used to describe data hiding, "Steganography" originated in Greece.

• **Medical Safety**: Watermarks containing the name of the patient can be embedded onto the X-Rays, MRI Scans & other test results help in instant identification of the result as belonging to a patient and thus avoid mix-ups which can lead to catastrophic consequences.

### 1.1.2 Watermarking Requirements

Below is list of requirements which discussing the difficulties of watermarking system (Vallabha, 2003):

- **Perceptual Transparency**: In most applications, the watermark inserted should not affect the quality of the cover image or data and hence remain undetectable. The watermark should go unnoticed as long as the data is not compared with the original data. This requirement also arises from the fact that perceptible signals are much easier to remove and also do not have the built in advantage of stealth.

- **Robustness**: Robustness is a measure of the ability of the embedding algorithm to introduce the watermark in such a way that it is retained in the image despite several stages of image processing. A good watermarking algorithm embeds the watermark in the spatial or frequency regions of the image, which would be least affected by such processing. Good correlation is possible between the recovered watermark and the original watermark in spite of noise errors introduced in it by
processing. There is a special class of watermarks called "fragile" watermarks, which are intentionally made non-robust. These are intended for authentication of original material rather than tracing it back to a source after being processed. A fragile watermark is lost with the slightest of image processing since such processing alters the image in a manner not intended for by the original owner of the material. "Semi-fragile" watermarks are able to survive standard unintentional image processing such as image compression for storage.

- **Security**: Security of a watermarking technique can be judged the same way as with encryption techniques. Assuming that unauthorized parties know the algorithm used for the embedding, the security of the algorithm lies in the selection of key. Thus the algorithm is truly secure if knowing the exact algorithm to embed and extract data does not help an unauthorized party in actually recovering the data from the watermarked image.

- **Payload of watermark**: The amount of information that can be stored in a watermark depends on the application. For example, in copy protection purposes, a payload of one bit is more than sufficient.

- **Oblivious vs. Non-oblivious**: In applications such as copyright protection and data monitoring the watermark extraction algorithms can use the original unwatermarked data to find the watermark. This is called non-oblivious watermarking. In other applications, such as copy protection and indexing the watermark extraction algorithms cannot access the unwatermarked image. This significantly raises the difficulty of extraction. Such methods are called oblivious, public or blind watermarking algorithms.
1.2 State-of-Art Watermarking Attacks

It is an open problem whether reliable and secure public watermarks can exist. Such public watermarks allow anyone to detect electronic watermarks, while the security and robustness are not affected by this public knowledge. By secure we mean that knowledge about how to detect a watermark does not reveal how the watermark can be removed or altered. We call the watermarking scheme reliable if it is robust to typical transmission and storage imperfections (such as lossy compression, noise addition, format conversion, bit errors) and signal processing artifacts (noise reduction, filtering), whether intentional or not.

One categorization of the wide class of existing attacks contains four classes of attacks: removal attacks, geometric attacks, cryptographic attacks, and protocol attacks (Kutter et al., 2000).

Removal attacks aim at the complete removal of the watermark information from the watermarked data without cracking the security of the watermarking algorithm, e.g., without the key used for watermark embedding.

Cryptographic attacks aim at cracking the security methods in watermarking schemes and thus finding a way to remove the embedded watermark information or to embed misleading watermarks. One such technique is the brute-force search for the embedded secret information. Another attack in this category is the so-called Oracle attack, which can be used to create a non-watermarked signal when a watermark detector device is available.

Protocol attacks aim at attacking the entire concept of the watermarking application. One type of protocol attack is based on the concept of invertible watermarks. The idea behind inversion is that the attacker subtracts his own watermark from the watermarked data and claims to be the owner of the watermarked data. This can create
ambiguity with respect to the true ownership of the data. Another protocol attack is the copy attack (Kutter et al., 2000). In this case, the goal is not to destroy the watermark or impair its detection, but to estimate a watermark from watermarked data and copy it to some other data, called target data.

1.3 Problem Statement

Digital images are a convenient media which has a rapid growth, with its benefits in Efficient Storage, Ease of Manipulation, and Transmission. However these features make digital image vulnerable to copyright infraction, tampering and unauthorized distribution. Thus copyright protection has been a key problem. In the early days, encryption and control access techniques were used to protect the ownership of digital image.

Recently, the watermark techniques are utilized to keep the copyright of digital image (Lee & Jung, 2001), but there is issue about none of robust digital watermarking uses the same robustness criteria. Thus, it consequently causes a non-practical comparison as well as slow down progress in this area (Kuttera & Petitcolas, 1999).

1.4 Research Motivation

The purpose of working with attacks is that still no standard and general purpose of benchmark, and still lack of robustness to attacks for certain watermarking techniques. We can say that almost anybody can break a watermark, by blind use of simple manipulations, or after study of the methods.

Thus, by working on attacks, it's able to develop better methods, as with cryptography, and at the same time define better benchmarks (Voloshynovskiy et al., 1999).