A COMPARATIVE STUDY OF DIGITAL WATERMARKING TECHNIQUES ON STILL IMAGES

MIRZA REHENUMA TABASSUM
BIT0129

A Thesis
Submitted to the Bachelor of Information Technology Program Office
of the Institute of Information Technology, University of Dhaka
in Partial Fulfillment of the
Requirements for the Degree

BACHELOR OF INFORMATION TECHNOLOGY
(SOFTWARE ENGINEERING)

Institute of Information Technology
University of Dhaka
DHAKA, BANGLADESH

A COMPARATIVE STUDY OF DIGITAL WATERMARKING TECHNIQUES ON STILL IMAGES

MIRZA REHENUMA TABASSUM

Approved:

Signature *Date*

Supervisor: Shah Mostafa Khaled

Committee Member: Dr. Kazi Muheymin-Us-Sakib

Committee Member: Dr. Md. Shariful Islam

Committee Member: Dr. Soo-Bong Kim

To

Mr. Mirza Md. Rafiful Islam and *Mrs. Jahanara Begum*
my lovely parents, the key to my every success

Abstract

Digital image watermarking technique is used to provide authentication and copyright protection. Watermark can be destroyed by applying various distortion to the watermarked image. Different watermarking techniques can stand against different distortions. The challenge is to embed the watermark with such a technique which is robust against most of the distortions preserving the quality of the host image. This research implemented three existing watermarking techniques- visible watermark in spatial domain, invisible watermark in spatial domain and invisible watermark in Discrete Cosine Transform (DCT) domain. The test images were subjected to some common distortions and the results of the three techniques are then compared. The result shows that, invisible watermarking in DCT domain is the most robust among the implemented three methods. Invisible watermarking in DCT domain is imperceptible as well as robust, which is the most desired feature of a good watermark.

Acknowledgments

I thank my honorable supervisor Mr. Shah Mostafa Khaled for the guidance during the research. His wise direction and advice showed the path to explore in the field of this study. The support he extended every time is the key to success in this research work.

My gratitudes to Mr. Emon Kumar Dey, Lecturer, Institute of Information Technology, University of Dhaka who took our Image processing class which helped me to learn the basics of my research field.

I would like to thank my friend Mr. Amit Seal Ami for his tremendous help with setting up the environment for the thesis. I would also like to thank my all other friends who supported me with any help in my study.

I am thankful to my family for the sacrifices they made and their endless support to carry out my research.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

Copyright infringement, authenticity, piracy, identity theft are some major concerns of digital data. Providing security to resources like digital images is a challenge now-a-days. It has become a key factor in digital world [1]. Digital images are copied and distributed over Internet. It leads to unauthorized replication problem [2]. Authentication systems need to be stronger to make the perpetrators fail to break them. Digital image authentication techniques are used for anti-falsification, copyright protection and access control, etc. [3] One of the mostly used technique is digital watermarking.

Watermarking techniques are used to protect the owners of digital media from perpetrators. Embedding a watermark into a digital media is a proof of the owners right to that media. It gives the owner means to ensure that others cannot claim that media is not belongs to the real owner. Watermarking can be used as a tool for authentication, copyright protection, broadcast monitoring, etc. The security issue related to the owners right to the media is ensured by embedding watermark in the original media.

Watermarking is an old idea. Government of almost all countries are using watermark for authentication from a long time ago. In the ancient time, emperors also used tattoos, stamps, hallmarks as watermark. They used this to provide authentication.

The use of digital watermarking is comparatively new. Easy access of Internet brought the question of security related to the ownership of a digital media. The risk of such issues are increasing day by day with the growing Internet users. Until early 90s, works on digital watermarking was limited to research labs [4]. It was spread to the general users after 1995 with commercial venture.

Digital watermarking now-a-days has become very popular and available. Anyone can now embed watermark on their digital images with various software. Watermark can be embedded with various techniques. However, all those techniques cannot stand strongly against image distortions. If someone uses text as watermark on a corner of the original image, the attacker can crop the image and distort the watermark. Again, if someone put the authentication text in the middle of the original image, the quality of the image is degraded. Sometimes the invisible watermarks can be removed by image compression, histogram equalization, etc. operations on the host image. The challenge is to use an appropriate watermarking technique that can handle probable distortions of different circumstances.

Different watermarking algorithms stand against different distortions of image. It is important to find the suitable technique to lessen the risk of being distorted. If the user of digital watermarking can find which type of technique is more likely to survive against which type of distortion, the threat can be reduced.

1.1 Motivation

People upload photos on public network frequently. Some photographers share their work on the Internet. Because of the easy access of the shared images, anyone using the images can claim its ownership. Watermarking is a tool to preserve owners right to the media. A watermark, however, can be removed by cropping, scaling, compressing or other kinds of distortion. It is necessary to make the watermark strong so that it cannot be removed easily.

The motivation came from some practical experiences while sharing images in some social networks in the Internet. Some images taken by the author was claimed by some other persons intellectual property. But there was no way to prove those

were author's property. Again, some of the images watermarked using visual watermarking with copyright text were cropped by the fraud and used as his name. The need of a robust watermarking technique came to the mind to protect the copyright, authenticity, user identification etc.

There are several techniques for embedding watermark. Researchers are proposing more effective methods day by day. A single watermarking technique cannot sustain against all the threats. Users must select which technique is most appropriate for their application. A comparison among some common watermarking technique with some common distortion can show a path to choose the right technique of watermarking.

1.2 Problem Statement

The purpose of this research is to make a comparative study of digital watermarking techniques on still images. Three watermarking methods are implemented in this study. Visible watermarking in spatial domain, invisible watermarking in spatial domain, and invisible watermarking in Discrete Cosine Transform domain are implemented. Several distortions have been done to distort the watermarked images. The survival of the watermarks are checked to get the result.

The main goal of this research is comparing the existing watermarking techniques with watermark sustainability against practical distortions. Proposing a new method in future based on the result of the study to have a robust watermarking technique is an objective of this research.

1.3 Thesis Organization

This report is documented to give the detail of the research work on "A Comparative Study of Digital Watermarking Techniques on Still Images". The report will first give the reader an introduction to this study. Then proceed with the background study which will help the reader to understand the work and the studies necessary for this research. The implemented approaches are also discussed. Experiment and their results followed by the discussion to conclude the study is presented. The chapter outline is given below-

- Chapter 1 is the first chapter of this report. This gives an introduction of this study with the motivation and problem definition of this research.
- Chapter 2 discusses with the background study of this work. Overview of digital watermarking as well as its classification, applications and threats to distort the watermark have been included. The significant work done in digital watermarking is discussed in the later part of the chapter.
- Typical watermarking system and the applied approaches in this research in the content of Chapter 3.
- Experiment and their result after the attacks are discussed in Chapter 4.
- Discussing the result and comparing the implemented three approaches are included in the Chapter 5. Extension of this work in future is also discussed briefly.

Chapter 2

Background Study

Digital watermarking system can be of several types and their applications are also of various kinds. The attacks which distort the watermark from watermarked image act differently. To work with different digital watermarking system we need to know the concepts of it. The upcoming section will discuss about the types of digital watermarking, robustness, applications of digital watermarking, and potential attacks which can distort the watermark. The research studies related to this work are also discussed in this chapter.

2.1 Background

Digital watermarking is a technique of computer-aided information hiding which preserves the information of authenticity of the data that carries the watermark. It is a process of embedding data (watermark) into a multimedia object to help protect the owners right to that object [5].

Digital watermarking describes methods and technologies that can contain information, for example a number or text, in digital media, such as images, video or audio as a symbol of the owner. The watermark needs to be strong in some cases. Sometimes it also needs to be fragile which can be destroyed with a weak attack. It should be strong or weak against various distortions depending on the application [6]. It should be robust or fragile depending on the application.

Digital watermark can be embedded into image, video, text or graphics [6, 7]. There should not be any perceptible difference between the watermarked and original signal, and the watermark should be difficult to remove or alter without damaging

the host signal [8]. Because of the possibility to duplicate digital images without any quality loss, new tools are required [1].

Watermarking techniques can be classified based on many criteria. It can be divided into two types considering its visibility, and two types according to the domain of the image. Robustness is another measure to categorize watermarking [9]. The following section discuss the classification of digital image watermarking, some application of watermark, type of image distortion and quality of good watermarks.

2.1.1 Perceptible and Imperceptible Watermarking

Watermarking techniques can be classified by their visibility. Perceptible watermarking is the type of watermark which is visible, and the invisible watermarking is known as imperceptible.

In visible watermarking the watermark information is visible in the picture or video [10]. It is generally a visible translucent image which is overlaid on the primary image [11]. It can be an opaque or semitransparent image or image that is placed on top of another image so that it is obvious to the viewer of the image [12]. Watermark can be a logo or seal of the organization which holds the rights of the host image. Watermark must allow the primary image to be viewed, but still anyone can it mark it clearly as the property of the owning organization [11]. TV channels put their logo in a corner of the screen to signify their ownership is an example of visible watermarking.

Visible watermarks are more robust than the invisible ones. Because of its perceptibility, anyone can easily notice it. But it degrades the image quality by making the original image unclear. Again, it can be removed by geometrical distortion like

cropping if it is embedded in an insignificant part of the image. So, tradeoff between making the watermark robust and making the original image clear may be needed.

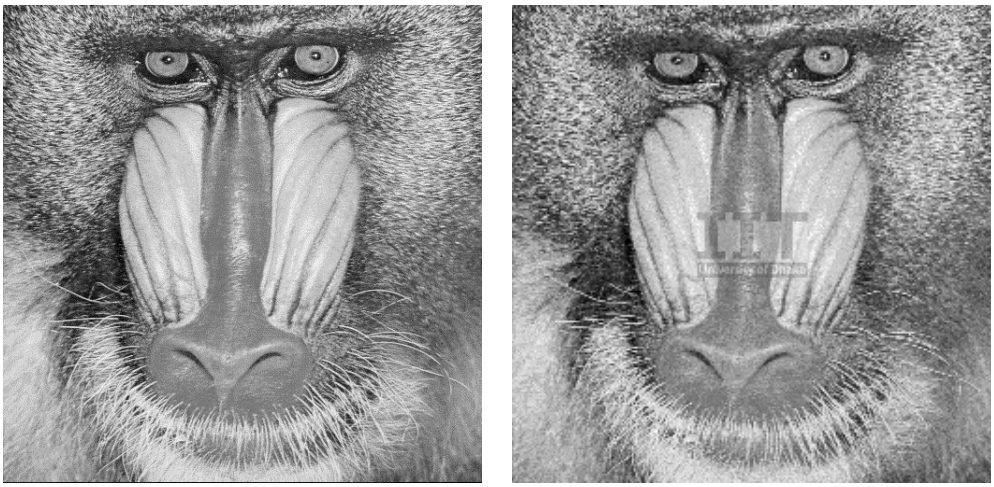
Good visible watermark should have the following characteristics [13]:

1. It has to noticeable in images
2. It must be visible but not considerably incomprehensible the image details beneath it
3. It must be harder to remove
4. It should be embedded in a significant area of the image so that it cannot be removed by cropping or scaling

A copyright mark, seal, watermark image or logo can be the example of visible watermarking. It is easy to embed and detect. A visible watermarking example is given in Figure 2.1.

Visible watermarking is done in spatial domain most of the times [14]. It can cause image fidelity and vulnerable to attack. One of its advantages is that, it does not need any decoder and it is hard to remove without destroying some part of the image.

An invisible watermark is an overlaid image, text or any information used as watermark, which cannot be seen, but can be detected [11]. It is also known as imperceptible watermarking technique. Imperceptible watermark is one which does not noticeably degrade the original host signal [7]. In invisible watermarking, information is added as digital data to picture, but it cannot be supposed as such (although it may be possible to detect that some amount of information is hidden). The watermark can be intended for widespread use, so the detection process must be easy to retrieve the watermark. The watermark can be a form of steganography, where a



(a) Mandrill (b) Watermarked Image

Figure 2.1: Visible Watermarking

party communicates a secret message embedded in the digital signal [10]. It can be a transparent image [7]. There should not be any perceptible difference between the watermarked and original signal, and the watermark should be difficult to remove or alter without damaging the host signal. Because of the possibility to duplicate digital images without any quality loss, new tools are required. Most of the time invisible watermarking is done in transform domain. It cannot be detected by human eyes and needs decoder/detector to find the watermark. Thus, it cannot be distorted with cropping but it can be removed by adding noise or transforming the image. The advantage of using invisible watermarking is, it does not hamper the original image while observing with human eyes.

Invisible watermark is generally embedded by altering a certain pixel several times so that the watermarked image is indistinguishable from the original. A basis of such alteration of pixels is that human eyes are sensitive to changes in flat areas in an image whereas slight changes in edges of the image objects are ignored by the human visual system [15].

2.1.2 Watermarking in Spatial and Transform Domain

Digital watermark can be divided into two types based on the domain of the image in which they are embedded. One is on spatial domain and the other is on transformed domain.

When a subset of the image pixels are changed by watermark embedding on the actual image pixels, it is called embedding watermark in the spatial domain. It is easy and fast to implement. It is based on direct manipulation of pixels of an image [16]. But it is more vulnerable to attacks like compression and filtering. Besides, the conformity of the original image data can be severely ruined since the watermark is directly applied on the pixel values [17].

Watermarking is mostly implemented in transform domain image like DCT, DWT and DFT domains [18]. Watermark is embedded altering selected transformed coefficients based on different criteria. Thus, some coefficients are selected and modified according to certain rules [19].

Transform frequency domain are more popular because of their robustness though it is harder and time consuming to implement. Transform domain watermarking has dominated the watermark approaches from its early stages [19]. Compared to spatial domain watermarking, it provides more protection under most of the signal processing attack and distortions like compression, geometrical distortion such as scaling, cropping, rotating, re-quantization, re-sampling, etc. [14].

2.1.3 Robustness

Robustness is a measure to show how much a watermark is strong to stand against image distortion. Based on the robustness of the watermark it can be categorized as robust, semi-robust and fragile watermarking technique [9]. This classification is made on how tolerant the watermark is to different transformations.

The watermark is fragile if it cannot be detected after very light modification or distortion. Fragile watermarks are commonly used for tamper detection (integrity proof) [9].

A digital watermark is called semi-fragile if it resists gentle transformations, but fails detection after several transformations. Semi-fragile watermarks are commonly used to detect malignant transformations [9].

Robust watermark exists after strong distortion. It can stand against several transformation. A digital watermark is called robust with respect to transformations if the embedded information may be detected reliably from the marked signal, even if degraded by any number of transformations. Robustness depends on the information capacity of the watermark, strength and visibility of the watermark, and the detection statistics (threshold) [14].

2.1.4 Application of Digital Watermarking

Watermark is used extensively now a days. It emerged for copyright protection and ownership identification [20]. It can be used for copyright protection, authentication detection, user identification, source tracking of digital media, etc. However, the main purpose of it is to protect owners right on media in different ways. In the book 'Digital Image Processing' the authors categorically discuss the uses of watermark

[12]:

1. ***Copyright Identification:*** Watermarks provide information that serves as proof of owners right on the media.

2. ***User Identification or Fingerprinting:*** Identity of legal users of the media is marked (fingerprint) on the media, and when an illegal copy is found, the sources of illegal distribution are traced out by the fingerprint.

3. ***Automated Monitoring:*** Servers/Routers can be used to find where some particular groups of watermarked images are used and this information can be useful for royalty collection.

4. ***Authenticity Determination:*** The originality of media can be checked by the presence of fragile watermarks on it. If it would have been altered, the fragile watermark would have been destroyed and its presence would not be found anymore on it.

5. ***Copy Protection:*** Although not effectively used still, watermarks can specify rules of media usage and copying.

6. ***Broadcast Monitoring:*** Television news often contains watermarked video from international agencies [9].

Watermarking techniques widely used in business now-a-days to enjoy the benefit of the above services. Example of applications are given in [6, 15]. Some of the significant uses in business are given below:

1. ***Data Security:*** Digital watermarking is used extensively for data security. It is implemented for certification, authentication, and conditional access of data. Using watermarks in passports, identity card, etc. are now very common.

2. ***Video Watermarking:*** Spatial and transform domain videos can be watermarked. The main objective is to protect copyright.

3. ***Audio Watermarking:*** It is used for copyright protection of audio signals. Here, the challenge is to synchronize the watermark with the audio signal in such a way that it becomes noiseless. The technique to hide the watermark signal from human ear has been developed.

4. ***Image Tampering:*** To avoid image tampering, fragile watermarks are coded into images.

5. ***Copy Control:*** It can be ensured using watermark that the media cannot be copied.

6. ***Fingerprint:*** Modern cameras and recorders use this feature to insert information like date, time, capturing machine ID number, etc. information into image, video and audio signals. This information can be used for further reference.

7. ***Steganography:*** Though watermark is not a steganography, unlike steganography it does not necessarily need to be hidden [7] but invisible watermark can be also used to carry message like steganography.

8. ***Soft Authentication:*** Digital watermarking with copyright can be used for Soft Authentication.

9. ***Linking Information on Documents:*** For instance, the name of a passport owner is normally printed in clear text. But it would also be hidden as an invisible watermark in the passport photo. If anyone tries to tamper with the passport by replacing the photo it would be possible to detect the change by scanning the passport and verifying the name hidden in the photo [6].

10. ***Media Management:*** To link photo with its negative, watermark can be used by photo development laboratories.

The above discussion shows that, the watermark usually contains the identity of the owner or receiver, transaction information like date and time, serial number, tracking information, etc. It can also carry other information based on the type of application.

2.1.5 Types of Distortion

Several types of distortion into the original image can remove the watermark. Transformation, alteration or some additive noise and cropping, etc. are known as distortion. Many image processing techniques can be used to eradicate the watermark from the original image. From the many kinds of distortion, it can be generalized in two classes [6]:

1. ***Noise Type Distortion:*** This type of distortion is done by adding noise. Compression is a distortion which is categorized as noise type of distortion.

2. ***Geometrical Distortion:*** Changing the geometric information of an image caused geometrical distortion. Resampling and rotation are mainly the geometrical distortion. Rotating, cropping, scaling, sampling, etc. are some example of geometric distortion.

2.1.6 Potential Threats and Attacks

A robust watermark should stand against distortions. It can be attacked by any distortion, but it should exist after majority of those. The attack is something which

attempts to distort the watermark from the original image. It may not be done intentionally, but sometimes some unintentional attack can harm the watermark. Unintentional attacks can occur when the host signal is passing through a communication media, and transformation on the signal may happen. We should be familiar with attacks to be able to design the watermarking algorithms resistant of those attacks.

Some of the potential threats are discussed below [14, 15, 21]:

1. ***JPEG Compression:*** A very common attack to watermark is JPEG compression. It can destruct spatial domain invisible watermarking. When an image is compressed, like JPEG compression, which cause loss of information in image, the watermark signal can be removed.

2. ***Rotation and Scaling:*** This is a type of geometrical distortion. It is one of the most challenging threat for image watermarks. Most correlation based detector cannot work against rotation. Rotation changes the pixel values with changing its position in axis. Scaling change the size of the image like subsampling.

3. ***Additive Noise:*** Additive noise generally increases the threshold at which the correlation detector of watermark verifier works on. Generally transmission errors and A/D and D/A converters are responsible for such increase. An attacker may introduce perceptually insignificant noise in this fashion [15].

4. ***Cropping:*** The watermark can be removed by cutting the image so that the part, where the watermark exists is cut down. This cropping technique can completely remove the watermark. It sometimes does not hamper the message of original image if the watermark was put down on an insignificant area of the image.

5. ***Histogram Equalization:*** Since these transformations affects the intensities of image pixels, histogram equalization might degrade the watermark in the host image. These problems, now a days have been solved by different transform domain watermarking systems [21].

6. ***Gaussian Noise:*** Gaussian Noise can be added which can eliminate the watermark. Sometime the image can be filtered with Gaussian filter.

7. ***Averaging:*** If the image pixels are averaged and then generates the output pixel, the watermark signal can loss its original pixel values.

8. ***Low pass and Median Filtering:*** Low pass filtering can dramatically affect the performance of watermarks. This might happen since spread-spectrum like watermarks, coded in transform domain, use the high frequency components for the embedding process.

9. ***Multiple Watermark:*** The attacker can put new watermarks on the original watermark. It can overlap the owners watermark.

10. ***Print, Xerox, Scan:*** If an image is printed from the digital media and then scan it to make it as digital image again, the original watermarked signal may be destroyed.

Some other distortions can distort watermark. The most common attacks are described briefly in the above points. Attackers do different type of image processing to eradicate the watermark.

All the attacks are not similarly dangerous to different kinds of watermark algorithms. Some attacks are useful when the watermark is embedded in spatial domain, some others are active in transformed domain. Cropping can be very effective when

the watermark is visible and in an insignificant area of image. Again, the noise can remove the invisible watermark. Clearly understanding the types of watermarking and distortions is needed to utilize watermarks effectively in different applications. The discussed section will help to understand the work of this research clearly.

2.2 Related Work

Several works were done on digital watermarking. Many of them are on digital image watermarking techniques. Both visible and invisible watermarking methods are practiced on spatial and transform domain. Different watermarking algorithms have been implemented to test the performance in different researches. Some comparison among different algorithms have also been done to measure their performance with different benchmarks.

Kumari et al. worked on invisible, secure and robust watermarking on gray level images. They claimed their technique as secure and robust [22]. It inserted the least significant bit for watermarking where the gray value of the image pixel remain same or increase or decrease to one. The watermark is imperceptible so that the modification cannot be found by human eyes. The proposed method inserts hidden message on the original image, based on their gray level values and coordinate positions. It ensures high robustness, embedding capacity and enhanced security.

Recently in 2012, another image watermarking research by Ali and Khamis was done based on analyzing histogram for maximum intensity value of pixel of the original image [23]. The original image is first divided into blocks and then the histogram of the blocks are drawn to find the highest frequency of occurrence for intensity moment. Then bit values of the watermark image are used to modulate the histogram peaks of the intensity. This technique is very simple, easy to implement, and is also very

effective to fight against noise, resize and rotation.

Mintzer et al. studied on what should be the performance of visible and invisible watermarking in different circumstances [24]. The paper discussed on the popular watermarking algorithms performance in particular problems.

Li and Guo proposed a robust watermarking technique against geometrical distortion [25]. First they divided the image into some local regions in spatial domain. Then they embedded the watermark into all the local regions repeatedly. The circular regions are first homocentric cirque regions.Watermark bits were embedded quantizing each cirque region into an odd or even region using oddeven quantization. They claimed localized embedding achieved good invisibility and repeated insertion enhances watermark robustness.

Fotopoulos and Skodras worked in transform domain [19]. They considered the length and the position of the watermark. They proposed an adaptive scheme for the selection of the proper coefficients.

Zhu and Sang studied on watermarking in discrete cosine transform (DCT) domain DC component (DC)[26]. The technique adjusted the block DCT coefficient of the image the watermarks and blocked the selected image according to 8×8 pixel, then divided the selected image into four non-overlapping sub image blocks according to 4×4 pixel to embedded the watermark through adjusting their DCT coefficient.

Comparison of four watermark techniques was done in a European project called OCTALIS [1]. Benchmarking results on watermark techniques were presented in their paper. That benchmark includes evolution of watermark robustness the subjective visual image quality. Their model solved the problem of image trading over an insecure network, such as Internet, and employed hybrid watermarking. Their result showed that the tested techniques did not have the same behavior and that no tested methods has optimal characteristics

Vidyasagar et al. made a survey of digital watermarking techniques [27]. They classified the techniques based on different domains in which the data is embedded.

A digital watermarking technique using discrete wavelet transform (DWT) is proposed in [20]. That research considered binary images as watermark.

Cox et al. proposed a secure (tamper-resistant) algorithm for watermarking images, and a methodology for digital watermarking which can be generalized to audio, video, and multimedia data in their research [14]. They generated their watermark from Gaussian random vector and inserted the watermark to the perceptually most significant spectral components of the data. Their method is robust against signal processing operations (such as lossy compression, filtering, digital-analog and analog-digital conversion, requantization, etc.), and common geometric transformations (such as cropping, scaling, translation, and rotation). The work was done in DCT domain.

Most of the researchers worked to develop new watermark embedding techniques. They did their study to make the techniques more robust without degrading image quality. Comparison among different watermarking techniques are also done by some researchers. It is important to find which techniques works best against which type of distortion.

2.3 Summary

Classification of digital watermarking based on their visibility and the image domain are discussed in this chapter. Both visible watermarking and invisible watermarking can embed in the spatial or transform domain. Digital watermarking is used by many applications now-a-days. However, survival against attacks which distort the watermark is a major concern, those were also a part of this chapter 2. The significant works done in digital watermarking have been discussed in brief. Based on the study

and related work done, we will go to the implementation and comparison of some watermarking techniques.

Chapter 3

Digital Image Watermarking Techniques

A digital image watermarking system not only works with the embedding technique of the watermark but also deals with watermark generation to detection on the watermark. All the units of a typical digital watermarking system will be discussed in this chapter. Three watermarking techniques has been implemented in this research. The techniques with their algorithm is given in the later part of this chapter.

3.1 Typical Watermarking System

A watermarking system has four parts. However, some of these parts might be missing in different watermarking systems like in a visible watermarking system, since the watermark can be perceived with naked eyes, it does not need any automated watermark extraction and detection. The components of a digital watermarking system are:

1. Watermark Generation Unit
2. Watermark Embedding Unit
3. Watermark Extraction Unit
4. Watermark Detection Unit

In the following we will describe the responsibilities of each in brief. Figure 3.1 presents the workflow of these units.

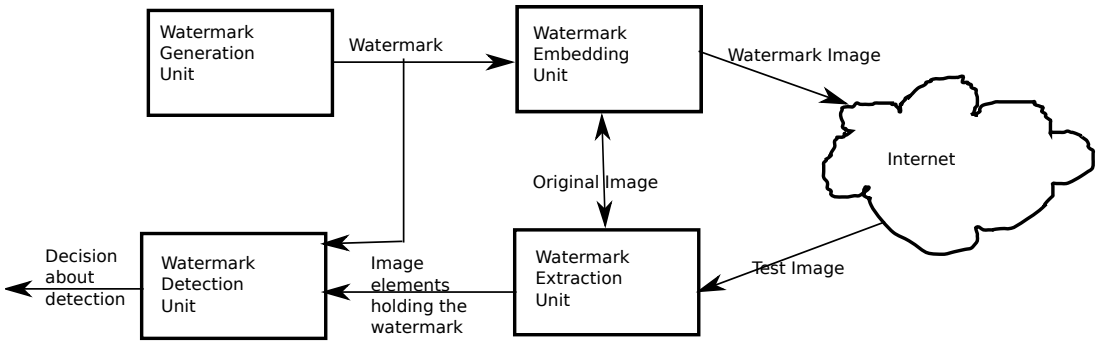


Figure 3.1: Typical Watermarking System

3.1.1 Watermark Generation Unit

This unit generates the watermark. The watermark may have different forms, like it might be another image for a visible watermarking system, this unit has nothing automated to do. The watermarking authority can select any image (for example the company logo) they like to put as watermark and can feed it to the embedding unit. For invisible watermarking, if the watermark contains owner information, in that case the responsibility of this unit is to put all the information in a bundle, and computationally convert the bundle to some format (for example, converting it to binary) and pass to the embedding unit. There are other watermarking systems that use Gaussian noise as watermarks. For these systems the watermark generation unit generates random numbers with Gaussian distribution and pass to the embedding unit.

3.1.2 Watermark Embedding Unit

This unit embeds the watermark into the host image. It gets the watermark as input and the host image on which the watermark is supposed to be put on. It outputs the watermarked image. Embedding may be in spatial or transform domains like DFT, DCT or DWT.

3.1.3 Watermark Extraction Unit

This unit extracts the watermarked coefficients of the image where the presence of watermark is to be tested. It gets test image as input the and sometimes the original host image on which the watermark was put on. It outputs the coefficients of the test image on which the watermark was supposed to be put on. Watermarking systems can be categorized into two groups depending on whether the extraction unit needs the original image and/or the watermark for extraction process. [28] These categories are:

1. **Private or restricted key system:** These systems need a copy of original image and /or a copy of the signature for watermark extraction and detection.

2. **Public or unrestricted key system:** These systems do not need the original image and the original signature for watermark extraction and detection.

Public key systems have a definite advantage over private key systems. If the original host image is not necessary for watermark extraction, anyone can verify whether an image is an authenticated copy of the original just without having copy of the original image. In that sense, public key systems are stronger in terms of security than private key systems.

3.1.4 Watermark Detection Unit

This unit matches the watermarked coefficients of the test image with the coefficients of the watermark, and if they are close enough than the system gives decision about finding presence of watermark in the test image. For measuring similarity between these two, standard statistical measures for correlation are generally used. If the similarity is larger than some predefined threshold than the unit gives decision that presence of the watermark could be found in the test image.

3.2 Implemented Approaches

We have implemented three approaches of digital watermarking compare among them. The first approach is a visible watermarking in the spatial domain [28]. The second is an invisible watermarking in the spatial domain [28]. The third approach is an invisible watermarking in the DCT domain [14]. The approaches are implemented and then the results after distortion are presented in Chapter 4. The following subsections will discuss about the implemented approaches in brief.

3.2.1 Visible Watermarking in Spatial Domain

The visible watermarking [28] that we have studied here uses an image as watermark. The image may contain some artifacts or some text that will appear on top of the host image. Therefore, the watermark generation unit has not any processing to do in this case.

Suppose, w denotes the watermark, f denotes the host image to be watermarked, and f_w is the watermarked image. The watermark insertion unit uses the following

formula for pixel-wise watermark insertion [28]:

$$f_w = (1 - \alpha).f + \alpha.w \tag{3.1}$$

Where $0 \leq \alpha \leq 1$ is the embedding factor that controls the visibility of the watermark. If $\alpha = 1$, then the watermark is fully visible and the underlying image is opaque. If α is a value close to 0, the image is fully visible and the watermark cannot be seen. Generally for visibly watermarking images value of α is chosen between 0.2 and 0.4. In this range the underlying image is visible through the semi transparent watermark image. Another important consideration for visible watermarking is that the watermark should be inserted in the most important area of the image, so that an attacker cannot crop important elements of the image by discarding the watermarked area. A visible watermarking system does not need any watermark extraction or detection unit, since the watermark is visible to naked eyes.

3.2.2 Invisible Watermarking in Spatial Domain

The invisible spatial domain watermarking scheme we studied here [28] also uses an image as watermark. The invisibility in this case is ensured by exploiting the fact that there is visually redundant information in an image. If we can embed the watermark on part of image which human visual system cannot perceive, the watermark cannot be seen by a viewer and hence will be an invisible watermark. In an 8 bit image the two least significant bits have almost no effect in the perception of the image by naked human eye. Again suppose that f is the un-watermarked host image, w is the watermark and f_w is the watermarked image. The following formula (using integer arithmetic) pixel-wise inserts the two most significant bits of the watermark into the

two least significant bits of host image.

$$f_w = 4\left\lfloor \frac{f}{4} \right\rfloor + \left\lfloor \frac{w}{64} \right\rfloor \tag{3.2}$$

An integer division than multiplication by 4 of an 8 bit pixel value sets the least significant two bits of a pixel to 0. The watermark will be inserted in these two bits. Dividing w by 64 shifts the two most significant bits of a pixel to the least significant two bits. Then pixel-wise adding these values generates the output image. This is how the watermark insertion unit works in spatial domain. For the extraction of this watermark, the watermark extraction unit takes two image f and f_w as input. It first divides (integer division) every pixel of f by 4 to clear the LSBs for every pixels and thereby get f_1. The extraction system than pixel wise subtracts f_1 from f_w, and take the absolute value. This absolute value is then multiplied by 64 to scale the two LSBs up to MSB. This value is then saved in an image. The following formula summarizes the process:

$$w = 64(f_w - f_1), where\ f_1 = 4\left\lfloor \frac{f}{4} \right\rfloor \tag{3.3}$$

Again like in the previous case there is no automated detection unit, since the image that is saved after processing can is should have all the perceptual features to be recognized as the watermark by naked human eye.

3.2.3 Invisible Watermarking in DCT Domain

This approach [14] computes Discrete Cosine Transform of the image signal and embeds the watermark on the highest k DCT coefficients of the watermark. It also uses pseudo random Numbers with Gaussian distribution with mean (μ) = 0 and

variance (σ^2) = 1 of k-length as the watermark. The watermark generation unit generates k pseudorandom numbers with mean (μ) = 0 and variance (σ^2) = 1 as the watermark and saves it as a file that will be used by watermark embedding and extraction unit afterwards. For this implementation $k = 100$ has been used.

For the generation of pseudorandom numbers with Gaussian distribution, we have used Algorithm P (Polar method for normal deviates) from the book "The Art of Computer Programming" by Knuth [21]. This algorithm (Algorithm 1) generates a couple of random numbers with Gaussian distribution with mean (μ) = 0 and variance (σ^2) = 1. We run a loop to generate as many such numbers as we need.

Algorithm 1 Pseudorandom Number Generation

Input: None

Output: X_1 and X_2 (floating point random numbers with Gaussian distribution with 0-mean and 1-variance)

1: **Begin**
2: Generate random numbers A and B distributed between 0 and 1
3: $V_1 \leftarrow 2A - 1$ (V_1 is a floating point numbers)
4: $V_2 \leftarrow 2B - 1$ (V_2 is a floating point numbers)
5: $S \leftarrow \sqrt{V_1^2 + V_2^2}$
6: **if** $S \geq 1$ **then**
7: Go to Step 2
8: **else if** $S = 0$ **then**
9: $X_1 \leftarrow 0$, $X_2 \leftarrow 0$
10: **else**
11: $X_1 \leftarrow V_1 \times \sqrt{\frac{-2 \ln S}{S}}$, $X_2 \leftarrow V_2 \times \sqrt{\frac{-2 \ln S}{S}}$
12: **end if**
13: **End**

The embedding unit has a watermark signature of length $100 < w_1, w_2, ..., w_{100} >$ and an input host image of $I_{n\times n}$. It outputs a watermarked image $I'_{m\times n}$ by embedding the signature in the 100 largest DCT coefficients. For this process, first DCT of the input image is computed. Then watermark is embedded into the coefficients, and the output image is computed by the IDCT. The equation to calculate the DCT from the input image is taken from [29]. DCT is calculated from the following equation:

$$DCT(u,v) = \frac{1}{\sqrt{2n}} \times \alpha(u) \times \alpha(v) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} pixel(x,y) \times \cos\left[\frac{(2x+1)u \times \pi}{2n}\right] \times \cos\left[\frac{(2y+1)v \times \pi}{2n}\right] \tag{3.4}$$

Where, pixel(x,y) is the gray level of pixel at coordinates (x,y), DCT(u,v) are DCT coefficients, and

$\alpha(u) = \frac{1}{\sqrt{2}}\ if v = 0$

$\alpha(u) = 1\ if x > 0$

The output image can be found by implementing the inverse DCT with the following equation:

$$pixel(x,y) = \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} \frac{1}{\sqrt{2n}}.\alpha(x).\alpha(y).DCT(u,v).\cos\left[\frac{(2x+1)u.\pi}{2n}\right].\cos\left[\frac{(2y+1)v.\pi}{2n}\right] \tag{3.5}$$

Where, pixel(x,y) is the gray level of pixel at coordinates (x,y), DCT(u,v) are DCT coefficients, and

$\alpha(x) = \frac{1}{\sqrt{2}}\ if x = 0,$

$\alpha(x) = 1\ if x > 0,$

Figure 3.2 summarizes the work of watermark embedding unit for this approach. We also elaborate the full process by Algorithm 2.

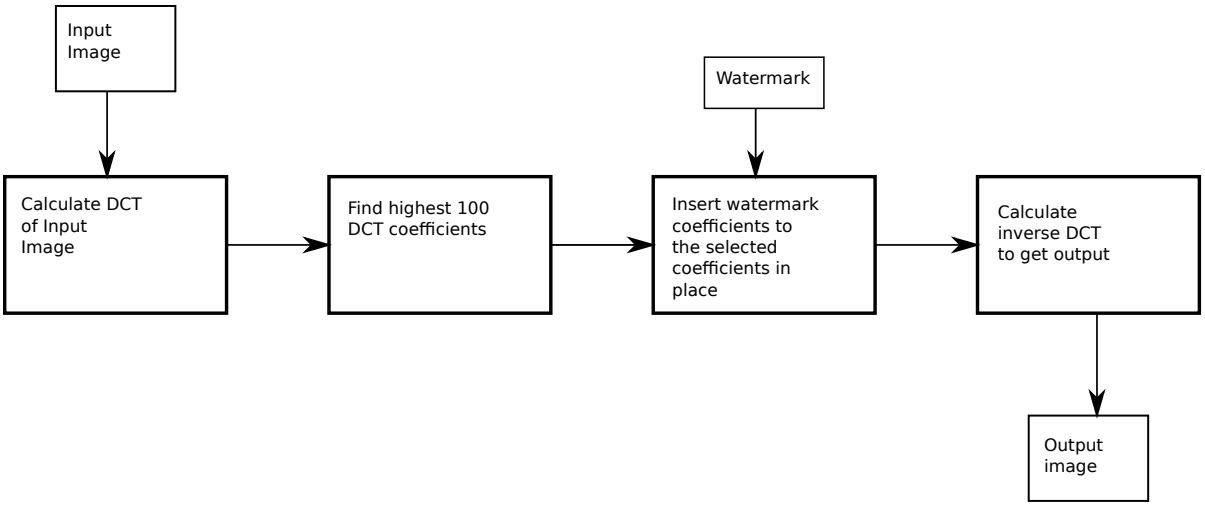


Figure 3.2: Watermark Embedding in DCT Domain

In this implementation the source code is adopted for DCT and IDCT calculation. The watermark extraction unit in this approach takes as input the original unwatermarked image and the test image, computes the DCT of the both, and thereby finds the 100 largest DCT coefficients of the original image and corresponding coefficients of the watermarked image. Based on these two coefficients, it computes the tentative watermark from the test image and saves those in a file to pass on to the detection unit.

Algorithm 2 Watermark Embedding

Input: Watermark signature $< w_1, w_2, w_3, ..., w_{100} >$ and Unwatermarked Image I_{nxn}

Output: Watermarked Image $I'_{n \times n}$

1: **Begin**

2: Calculate 2D DCT of Image $I_{n \times n}$ using equation 3.4

3: Locate 100 largest coefficients by magnitude $< c_1, c_2, c_3, ..., c_{100} >$, in DCT(u,v)

4: Embed watermark into the first 100 largest DCT coefficients from step 3.

$c'_i \leftarrow c_i(1 + \alpha.wf_i)$,

$\alpha = 0.3$

5: Replace original c_i by c'_i in place

6: Compute the inverse DCT of result of Step 5 using equation 3.5

7: Save watermarked image $I'_{n \times n}$

8: **End**

Figure 3.3 describes the process of extracting watermark from DCT domain. The detail is elaborated in Algorithm 3.

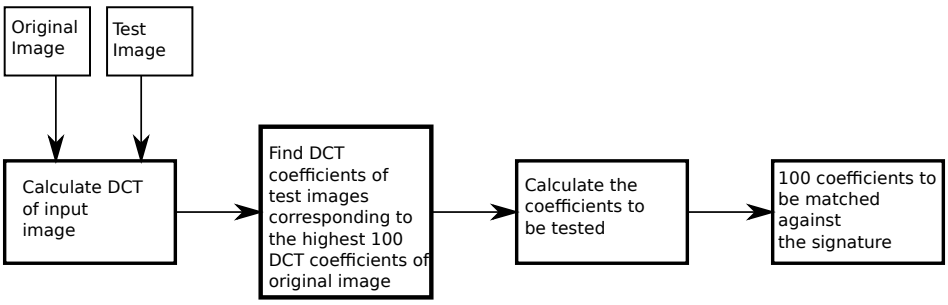


Figure 3.3: Watermark Extraction from DCT Domain

Algorithm 3 Watermark Extraction

Input: Original Image $I_{n\times n}$ and Test Image $I'_{n\times n}$

Output: Tentative watermark $< x_1, x_2, x_3, ..., x_{100} >$

1: **Begin**

2: Calculate 2D DCT of $I_{n\times n}$ and I'_{nxn}

3: Locate 100 largest coefficients by magnitude $< c_1, c_2, c_3, ..., c_{100} >$ in DCT(u,v) of I_{nxn}

4: Locate $< \hat{c_1}, \hat{c_2}, \hat{c_3}, ..., \hat{c_{100}} >$ in DCT(u,v) of I'_{nxn}

5: Calculate the tentative watermark $< x_1, x_2, x_3, ..., x_{100} >$

$x_i = (\frac{\hat{c_i}}{c_i} - 1) \div \alpha$

where, $\alpha = 0.3$

6: Save the tentative watermark $< x_1, x_2, x_3, ..., x_{100} >$ in a file

7: **End**

The watermark detection unit takes as input the signature (the original watermark) $< w_1, w_2, w_3, ..., w_{100} >$, and the tentative watermark $< x_1, x_2, x_3, ..., x_{100} >$ generated by the watermark extraction unit. It computes Normalized Correlation γ between the tentative watermark coefficients and the signature coefficients by the following function.

$$\gamma = \frac{\sum_{i=1}^{100} w_i.x_i}{\sqrt{\sum_{i=1}^{100} w_i^2 . \sum_{i=1}^{100} x_i^2}} \tag{3.6}$$

If the normalized correlation [30] γ is greater than 0.2 the signature is matched, and in that case we conclude that the test image contained a copy of the original watermark. Watermarking in this fashion is robust to operations like A/D-D/A conversion, filtering, lossy compression, requantization, rotation, scaling, cropping

and translation, etc. The use of Gaussian noise ensures good resilience to collusion and multiple watermarking attacks. We will describe test results on some of these in the experiment section.

3.3 Summary

Watermarking system generally consists of four basic units though every technique does not need all the four. Visible watermarking technique does not need a extraction and detection unit as it can be detected by naked eye. Invisible watermarking needs to have an extraction unit. The detection unit is used when the extracted watermark cannot be detected by only checking through eyes. Visible watermarking in spatial domain, invisible watermarking in spatial domain and invisible watermarking in DCT domain has been implemented in this study. These are discussed in this chapter with the overview of a typical watermarking system.

Chapter 4

Experiment and Result

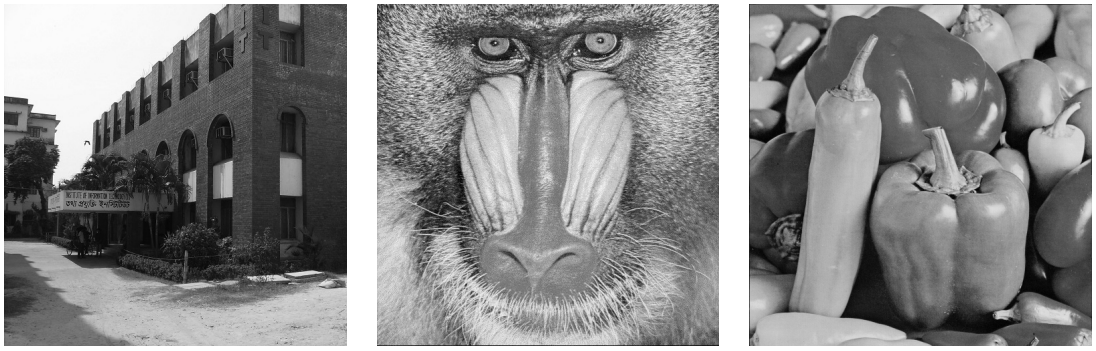
The three techniques discussed in the previous chapter has been implemented. The experiment took place with those mentioned techniques with some attacks to distort the watermarked images, where the watermarks are embedded with the implemented techniques in this study. The same images are used for all the three different watermarking techniques. We will discuss about the experiment with the experimental setup in the following section. After distorting the watermarked images, the results are written based on visualizing for visible watermark in spatial domain, the extraction module with visualizing the extracted watermark for invisible watermark in spatial domain, and with the help of detection unit for invisible watermarking in DCT domain.

4.1 Experimental Setup

The experiment with different watermark techniques is done in a personal computer with 4 GB RAM and 2.5 GHz Intel Core i5-24500M processor. The program is executed in Linux environment. Ubuntu 12.04 is the OS where the program are run to embed and fetch the watermarks. C++ is used as programming language to code the different watermarking algorithm. Several libraries are used to do the work. One of the significant library is libnetpbm which can easily process the PGM image format. Portable Gray map Format (PGM) images are used in this experiment. The mentioned library has the functions to work with PGM images. Thus, that library is selected to add in the program.

Test images are collected from three [31, 32, 33] websites where standard PGM

image can be downloaded for free. The image mandrill, vegetables and iit, files of dimension 512×512 are used. The logo of IIT is used as the watermark image which is also a PGM file with dimension 119×71 and the logo of University of Dhaka is used as the second watermark for multiple watermarking with 208×243. In Figure 4.1, 4.1(a) represents the figure of IIT, Figure 4.1(b) represents the figure of Mandrill, and Figure 4.1(c) shows the figure of Vegetables. IIT logo and University of Dhaka logo are represented in Figure 4.2 as watermark images.



(a) IIT (b) Mandrill (c) Vegetables

Figure 4.1: Test Images

(a) Watermark (b) Watermark 2

Figure 4.2: Watermark Image

4.2 Applied Distortions and their Effects

This section focuses on the performance of the three discussed approaches. We subjected the watermarked images to different transformation (as presented in the following subsections). The mentioned test images are distorted with several techniques. Then the watermak is tested. The visible watermark with visible watermarking in spatial domain (Approach 1) is tested whether the watermark can visualize and recognize or not. The IIT logo is used for watermarking in Approach 1 and invisible watermarking in spatial domain (Approach 2). For invisible watermarking in DCT domain (Approach 3) we generate 100 random numbers of Gaussian distribution with zero mean and 1 variance. The success of Approach 3 as suggested by [14] and [28] is measured against the correlation with the original watermark. With a undistorted watermarked image the correlation value will be generally 0.99. If the correlation is higher than 0.2 we conclude that the watermark could be detected, otherwise not.

(a) Approach 1: Visible in Spatial Domain

(b) Approach 2: Invisible in Spatial Domain

(c) Approach 3: Invisible in DCT Domain

Figure 4.3: Watermarked Images (IIT)

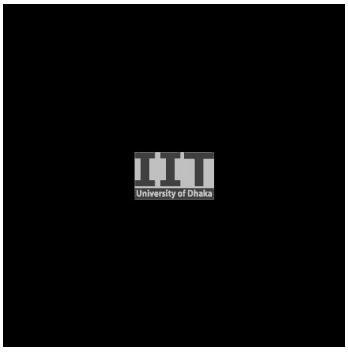
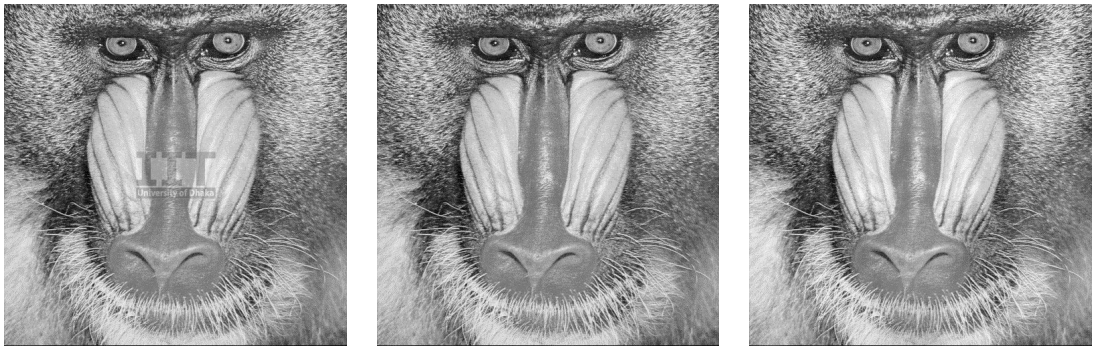


Figure 4.4: Result of detection algorithm on image of 4.3(b)



(a) Approach 1: Visible in Spatial Domain

(b) Approach 2: Invisible in Spatial Domain

(c) Approach 3: Invisible in DCT Domain

Figure 4.5: Watermarked Images (Mandrill)

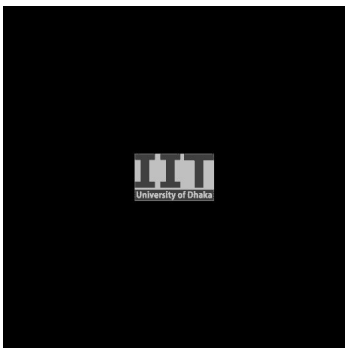


Figure 4.6: Result of detection algorithm on image of 4.5(b)

(a) Approach 1: Visible in Spatial Domain

(b) Approach 2: Invisible in Spatial Domain

(c) Approach 3: Invisible in DCT Domain

Figure 4.7: Watermarked Images (Vegetables)

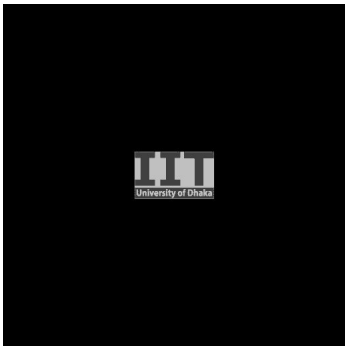


Figure 4.8: Result of detection algorithm on image of 4.7(b)

4.2.1 Histogram Equalization

Watermarked applied by the mentioned three approaches on test images have been made subject to histogram equalization to produce Figure 4.9, 4.11, and 4.13.

(a) Approach 1: Visible in Spatial Domain

(b) Approach 2: Invisible in Spatial Domain

(c) Approach 3: Invisible in DCT Domain

Figure 4.9: After Histogram Equalization (IIT)

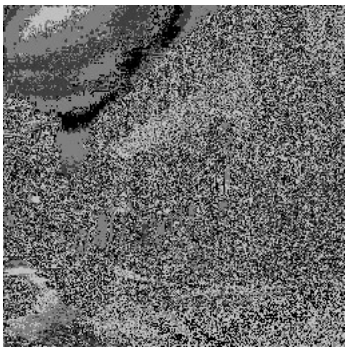
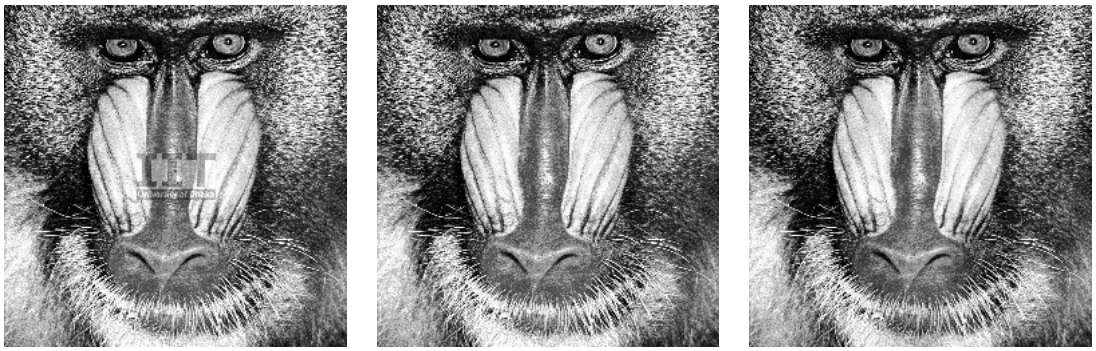


Figure 4.10: Result of detection algorithm on image of 4.9(b)



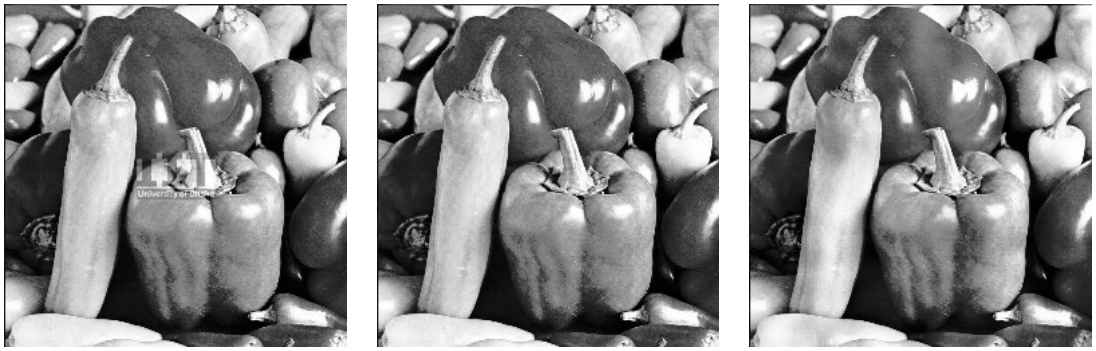
(a) Approach 1: Visible in Spatial Domain

(b) Approach 2: Invisible in Spatial Domain

(c) Approach 3: Invisible in DCT Domain

Figure 4.11: After Histogram Equalization (Mandrill)

Figure 4.12: Result of detection algorithm on image of 4.11(b)



(a) Approach 1: Visible in Spatial Domain

(b) Approach 2: Invisible in Spatial Domain

(c) Approach 3: Invisible in DCT Domain

Figure 4.13: After Histogram Equalization (Vegetables)

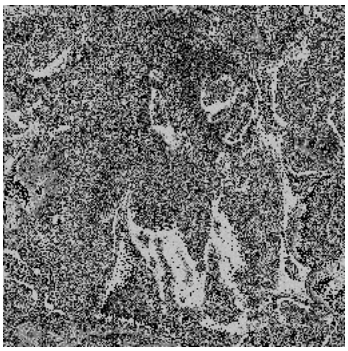


Figure 4.14: Result of detection algorithm on image of 4.13(b)

The watermark embedded by Approach 1 is still visually recognizable in all the

images after histogram equalization. After applying watermark with Approach 2, as it is the invisible watermark, the watermark is extracted from the images after distortion. However, when we try to detect the watermark for Approach 2 we see the image as in Figure 4.10, 4.12, and 4.14, the watermark is no more recognizable. Running the extraction and detection module of Approach 3 on image of Figure 4.9(c), 4.11(c) and 4.13(c) we find that the value of correlation is 0.621292, 0.662718 and 0.738525 respectively which signifies a successful detection of the watermark even after applying global histogram equalization on the image.

4.2.2 Cropping

The test images are randomly cropped to produce Figure 4.15, 4.17, and 4.19.

(a) Approach 1: Visible in Spatial Domain (b) Approach 2: Invisible in Spatial Domain (c) Approach 3: Invisible in DCT Domain

Figure 4.15: After Cropping (IIT)

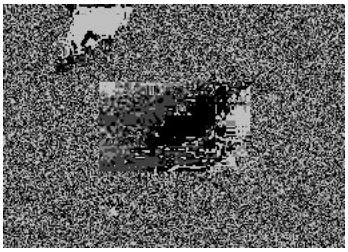


Figure 4.16: Result of detection algorithm on image of 4.15(b)

(a) Approach 1: Visible in Spatial Domain

(b) Approach 2: Invisible in Spatial Domain

(c) Approach 3: Invisible in DCT Domain

Figure 4.17: After Cropping (Mandrill)

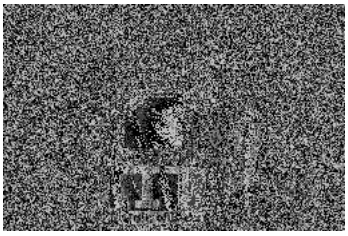
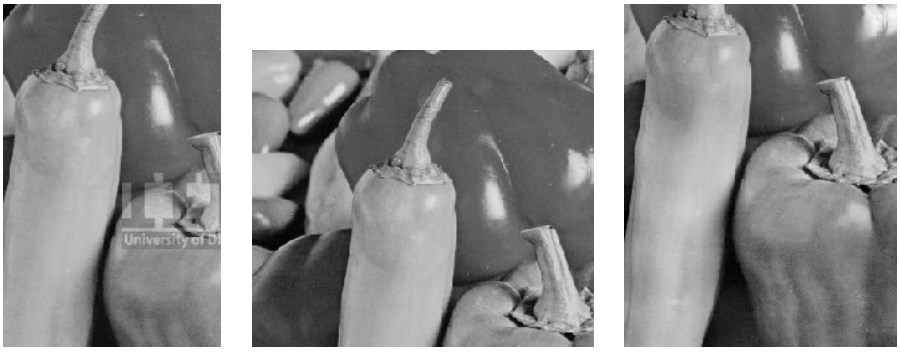


Figure 4.18: Result of detection algorithm on image of 4.17(b)



(a) Approach 1: Visible in Spatial Domain

(b) Approach 2: Invisible in Spatial Domain

(c) Approach 3: Invisible in DCT Domain

Figure 4.19: After Cropping (Vegetables)

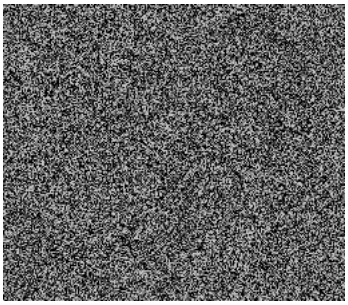


Figure 4.20: Result of detection algorithm on image of 4.19(b)

As the watermark is embedded to the middle of the image with Approach 1, the watermark would exist unless the middle of the image is cropped. In all the four test images, a part of the watermark is visible. With Approach 2, the watermarks are not clearly visible after extracting it from the watermarked test images. The extracted watermark from the three images cannot be recognized except the image of Mandrill. Running the extraction and detection module of Approach 3 on the cropped image of Figure 4.15(c), it is found that the value of correlation is 0.785291, which signifies a successful detection of the watermark after cropping and merging.

But for Figure 4.17(c) and 4.19(c) it is -0.110787 and -0.066374 respectively, which shows the unsuccessful detection.

4.2.3 Motion Blurring

Watermarked images of all the three approaches have been made subject to linear motion blurring with length=20 and angle=20 to produce Figure 4.21, 4.23, and 4.25.

(a) Approach 1: Visible in Spatial Domain

(b) Approach 2: Invisible in Spatial Domain

(c) Approach 3: Invisible in DCT Domain

Figure 4.21: After Motion Blurring (IIT)

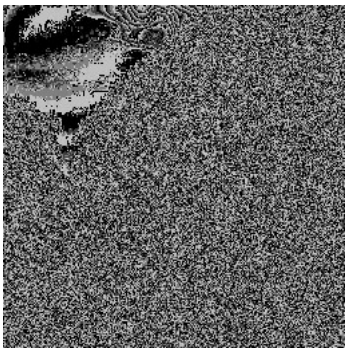


Figure 4.22: Result of detection algorithm on image of 4.21(b)

(a) Approach 1: Visible in Spatial Domain

(b) Approach 2: Invisible in Spatial Domain

(c) Approach 3: Invisible in DCT Domain

Figure 4.23: After Motion Blurring (Mandrill)

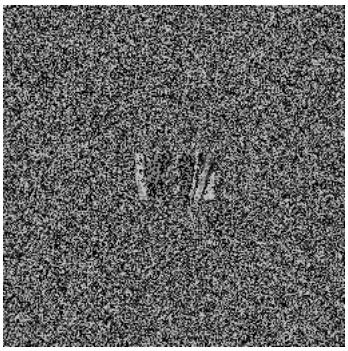


Figure 4.24: Result of detection algorithm on image of 4.23(b)

(a) Approach 1: Visible in Spatial Domain

(b) Approach 2: Invisible in Spatial Domain

(c) Approach 3: Invisible in DCT Domain

Figure 4.25: After Motion Blurring (Vegetables)

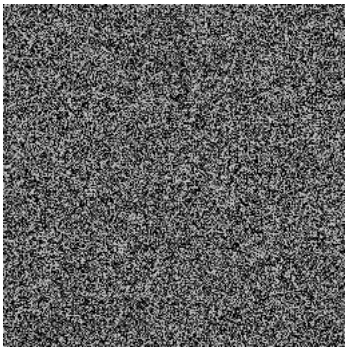


Figure 4.26: Result of detection algorithm on image of 4.25(b)

The watermark is almost gone after motion blurring where applied with Approach 1. It is very slightly recognized in Figure 4.23(a). When the watermark is tried to be detected for Approach 2, the watermark is no more visible. Running the extraction and detection module of Approach 3 on image of Figure 4.21(c), 4.23(c), and 4.25(c) we found that the value of correlation are 0.338621, 0.171488, 0.281509. The second one is lower than 0.2 and therefore signifies a unsuccessful detection of the watermark after applying motion blurring on the image. Though the other two correlations are greater than 0.2, they are not big enough to prove the watermark is detected successfully. The images are distorted so much by motion blurring that the watermarks are washed out.

4.2.4 Rotation

To distort the watermarked images, 90 degree counter clockwise rotation is applied. The resultant images are Figure 4.27, 4.29, and 4.31.

(a) Approach 1: Visible in Spatial Domain

(b) Approach 2: Invisible in Spatial Domain

(c) Approach 3: Invisible in DCT Domain

Figure 4.27: After Rotation (IIT)

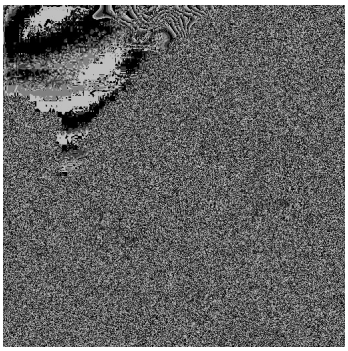
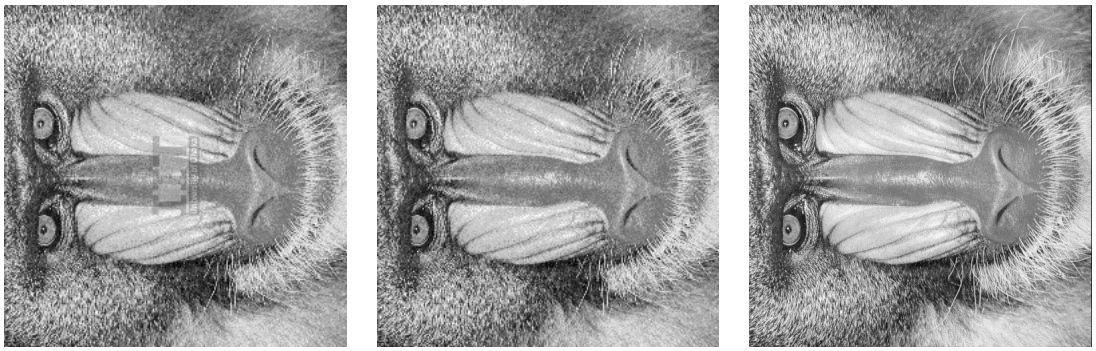


Figure 4.28: Result of detection algorithm on image of 4.27(b)



(a) Approach 1: Visible in Spatial Domain

(b) Approach 2: Invisible in Spatial Domain

(c) Approach 3: Invisible in DCT Domain

Figure 4.29: After Rotation (Mandrill)

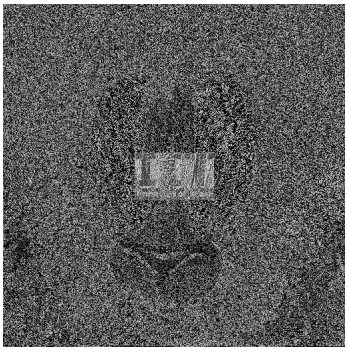


Figure 4.30: Result of detection algorithm on image of 4.29(b)

(a) Approach 1: Visible in Spatial Domain

(b) Approach 2: Invisible in Spatial Domain

(c) Approach 3: Invisible in DCT Domain

Figure 4.31: After Rotation (Vegetables)

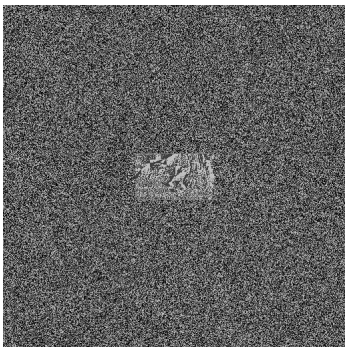


Figure 4.32: Result of detection algorithm on image of 4.31(b)

The watermark using Approach 1 can completely recognized in the test images.

The rotation just rotated the watermark as the rotation of the image. The watermark can be slightly visible in the extracted image from invisibly watermarked images with Approach 2 after re-rotating. In Figure 4.30 and Figure 4.32 the watermark can be recognized. But for the extracted watermark from IIT image, it cannot be detected as watermark. Applying watermark in DCT domain with Approach 3 and then rotating it with 90 degree counter clockwise and re-rotate it ,the correlation of the test images are 0.747898, 0.954937 and 0.964354 for Figure 4.27(c), 4.29(c), and 4.31(c) which indicate that the detection is successful. The watermark applied with Approach 3 sustained after rotation.

4.2.5 Flipping

The images are flipped horizontally. After applying watermark with the 3 approaches Figure 4.33, 4.35, and 4.37 are the resultant images.

(a) Approach 1: Visible in Spatial Domain (b) Approach 2: Invisible in Spatial Domain (c) Approach 3: Invisible in DCT Domain

Figure 4.33: After Flipping (IIT)

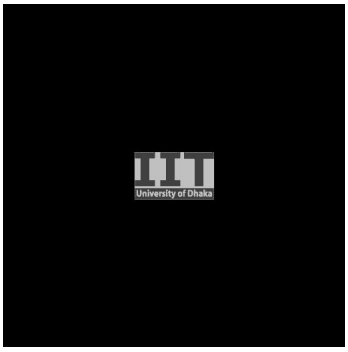
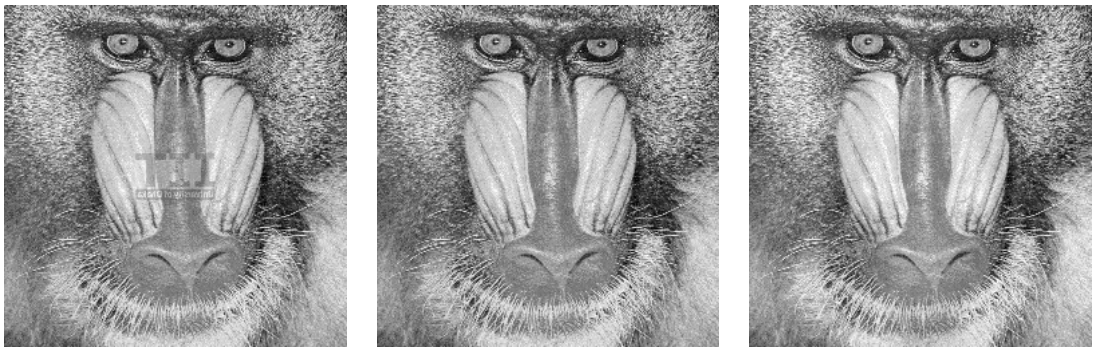


Figure 4.34: Result of detection algorithm on image of 4.33(b)



(a) Approach 1: Visible in Spatial Domain

(b) Approach 2: Invisible in Spatial Domain

(c) Approach 3: Invisible in DCT Domain

Figure 4.35: After Flipping (Mandrill)

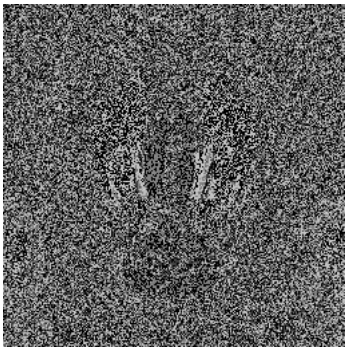


Figure 4.36: Result of detection algorithm on image of 4.35(b)

(a) Approach 1: Visible in Spatial Domain

(b) Approach 2: Invisible in Spatial Domain

(c) Approach 3: Invisible in DCT Domain

Figure 4.37: After Flipping (Vegetables)

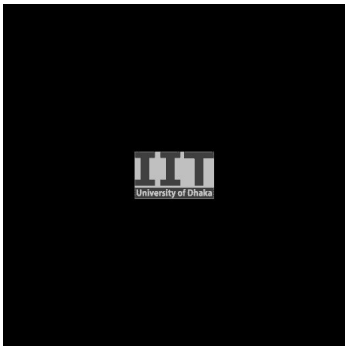


Figure 4.38: Result of detection algorithm on image of 4.37(b)

The watermark with Approach 1 can be clearly recognized after flipping and re-flipping. Flipping the image make the watermark flipped also, but it is recognizable. Applied watermark with Approach 2 and then distort it by flipping and flipping back, the extracted watermark is completely recognizable in Figure 4.33(b) and Figure 4.37(b). However, for Figure 4.35(b), the watermark is no more distinguishable after extracting. With Approach 3 watermark can exist after flipping. The correlations are 0.786335 for Figure 4.33(c), 0.999904 for Figure 4.35(c), 0.999706 for Figure 4.37(c). Detection is successful after flipping and re-flipping.

4.2.6 Unsharp Masking

Watermarked images of all the three approaches have been made subject to Unsharp masking with Radius=5.0, Amount=0.5 and Threshold=0 to produce Figure 4.39, 4.41, and 4.44.

(a) Approach 1: Visible in Spatial Domain (b) Approach 2: Invisible in Spatial Domain (c) Approach 3: Invisible in DCT Domain

Figure 4.39: After Unsharp Masking (IIT)

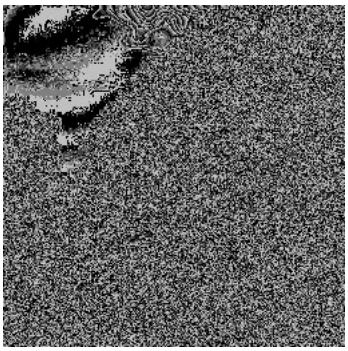
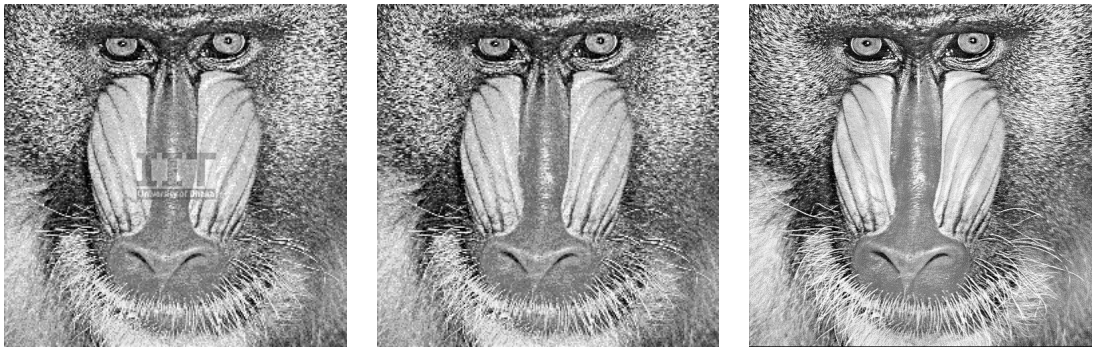


Figure 4.40: Result of detection algorithm on image of 4.39(b)



(a) Approach 1: Visible in Spatial Domain

(b) Approach 2: Invisible in Spatial Domain

(c) Approach 3: Invisible in DCT Domain

Figure 4.41: After Unsharp Masking (Mandrill)

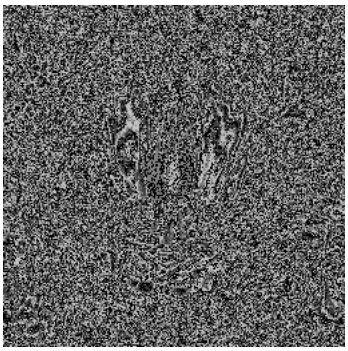
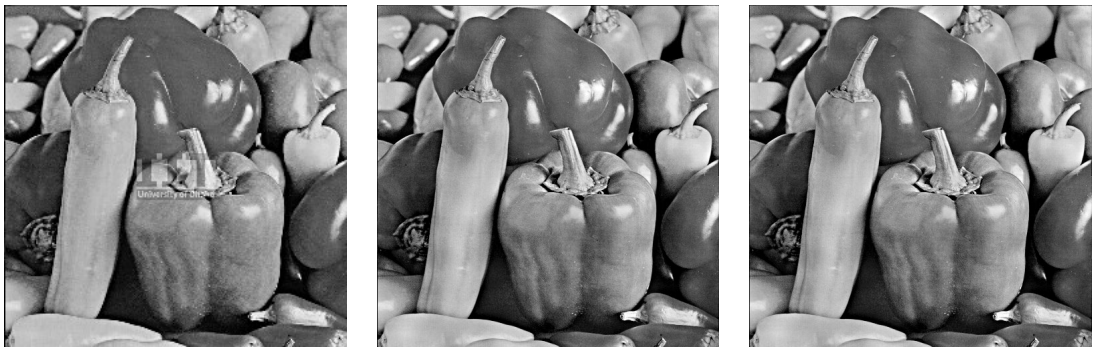


Figure 4.42: Result of detection algorithm on image of 4.41(b)



(a) Approach 1: Visible in Spatial Domain

(b) Approach 2: Invisible in Spatial Domain

(c) Approach 3: Invisible in DCT Domain

Figure 4.43: After Unsharp Masking (Vegetables)

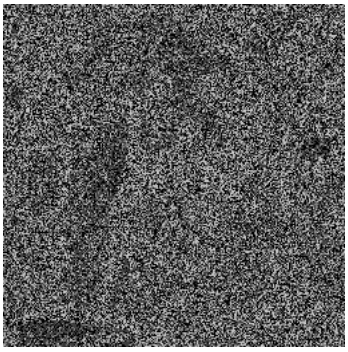


Figure 4.44: Result of detection algorithm on image of 4.43(b)

After applying unsharp masking in the visibly watermarked image, the watermark is completely recognizable. But unsharp masking washed out the watermark which where applied with Approach 2. The watermark sustained which are applied using Approach 3. The correlation are 0.795079 for Figure 4.39(c), 0.919131 for Figure 4.41(c), and 0.972506 for Figure 4.43(c).

4.2.7 Scaling

The test images are scaled to 256×256 pixels to produce Figure 4.45, 4.47 and 4.49.

(a) Approach 1: Visible in Spatial Domain (b) Approach 2: Invisible in Spatial Domain (c) Approach 3: Invisible in DCT Domain

Figure 4.45: After Unsharp Masking (IIT)

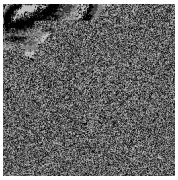
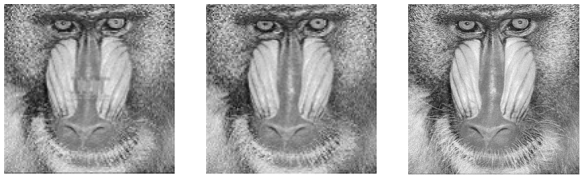


Figure 4.46: Result of detection algorithm on image of 4.45(b)



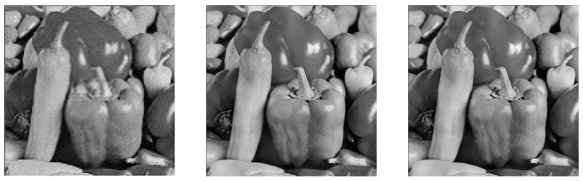
(a) Approach 1: Visible in Spatial Domain

(b) Approach 2: Invisible in Spatial Domain

(c) Approach 3: Invisible in DCT Domain

Figure 4.47: After Scaling (Mandrill)

Figure 4.48: Result of detection algorithm on image of 4.47(b)



(a) Approach 1: Visible in Spatial Domain

(b) Approach 2: Invisible in Spatial Domain

(c) Approach 3: Invisible in DCT Domain

Figure 4.49: After Scaling (Vegetables)

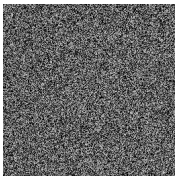


Figure 4.50: Result of detection algorithm on image of 4.49(b)

The visible watermak with Approach 1 is exists after scaling down the images. But the invisible watermark in spatial domain cannot exist after scaling down. The watermarks are not visible in the extracted images. The watermark with Approach 3 cannot exist afetr scaling down. The correlations show unsuccessful detection of watermark. Correlations are -0.246409, 0.009970 and 0.006814 for the image of IIT, Mandrill and Vegetables after scaling down.

4.2.8 JPEG Compression

JPEG compression has been applied to the test images. 85% quality is preserved with smoothing=0.0 while compressing the images. Figure 4.51, 4.53, and 4.55 are the images after JPEG compression.

(a) Approach 1: Visible in Spatial Domain (b) Approach 2: Invisible in Spatial Domain (c) Approach 3: Invisible in DCT Domain

Figure 4.51: After JPEG Compression (IIT)

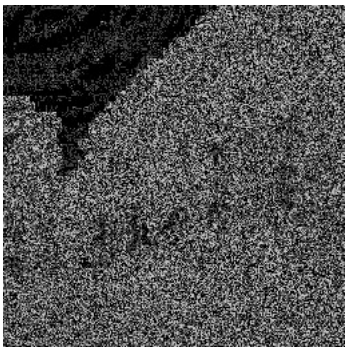
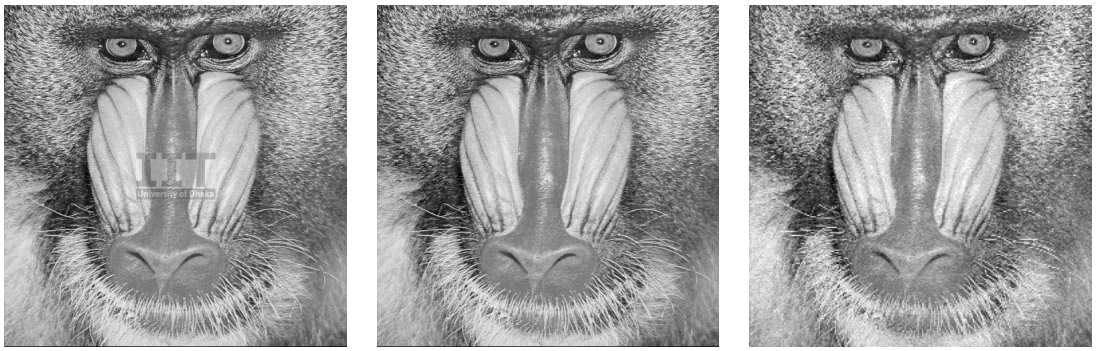


Figure 4.52: Result of detection algorithm on image of 4.51(b)



(a) Approach 1: Visible in Spatial Domain (b) Approach 2: Invisible in Spatial Domain (c) Approach 3: Invisible in DCT Domain

Figure 4.53: After JPEG Compression (Mandrill)

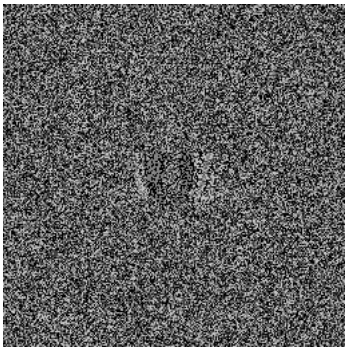


Figure 4.54: Result of detection algorithm on image of 4.53(b)

(a) Approach 1: Visible in Spatial Domain

(b) Approach 2: Invisible in Spatial Domain

(c) Approach 3: Invisible in DCT Domain

Figure 4.55: After JPEG Compression (Vegetables)

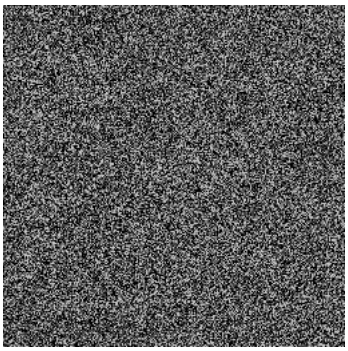


Figure 4.56: Result of detection algorithm on image of 4.55(b)

The watermark applied with Approach 1 is clearly visible after JPEG compres-

sion. Approach 2 watermarked images gave the negative result after extracting. The invisible watermark cannot be detected after JPEG compression. The result shows a successful detection for Approach 3 after JPEG compression. The correlations are 0.786335, 0.999706 and 0.999706 for Figure 4.51(c), Figure 4.53(c) and Figure 4.55(c) respectively.

4.2.9 Multiple Watermarking

The original images are multiply watermarked by logo of IIT and University of Dhaka. First time it is watermarked with Figure 4.2(a). Again, the watermarked images are watermarked by Figure 4.2(b) to generate Figure 4.57, 4.59, and 4.61.

(a) Approach 1: Visible in Spatial Domain

(b) Approach 2: Invisible in Spatial Domain

(c) Approach 3: Invisible in DCT Domain

Figure 4.57: After Multiple Watermarking (IIT)

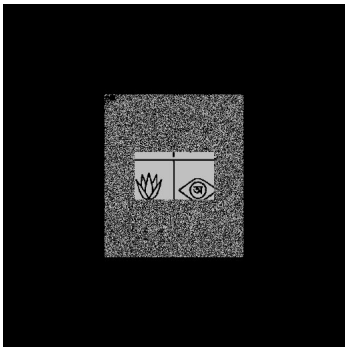
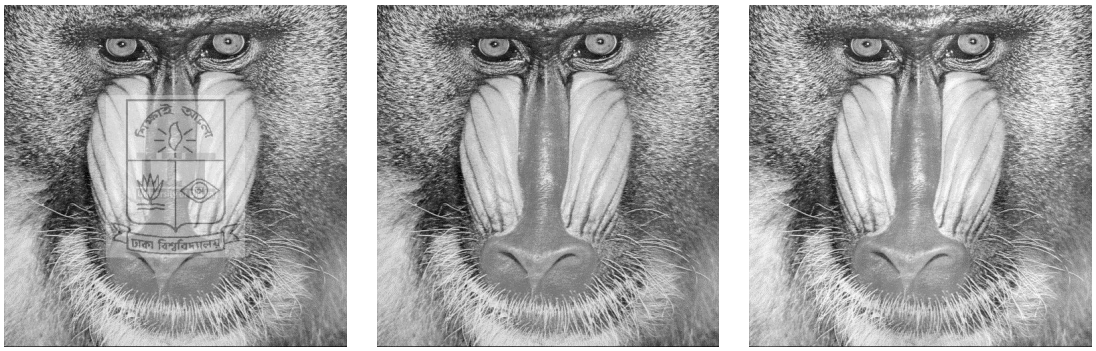


Figure 4.58: Result of detection algorithm on image of 4.57(b)



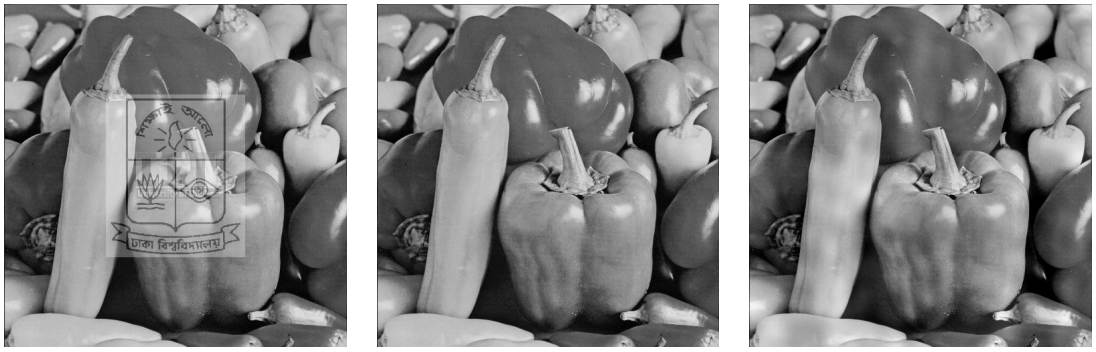
(a) Approach 1: Visible in Spatial Domain

(b) Approach 2: Invisible in Spatial Domain

(c) Approach 3: Invisible in DCT Domain

Figure 4.59: After Multiple Watermarking (Mandrill)

Figure 4.60: Result of detection algorithm on image of 4.59(b)



(a) Approach 1: Visible in Spatial Domain (b) Approach 2: Invisible in Spatial Domain (c) Approach 3: Invisible in DCT Domain

Figure 4.61: After Multiple Watermarking (Vegetables)

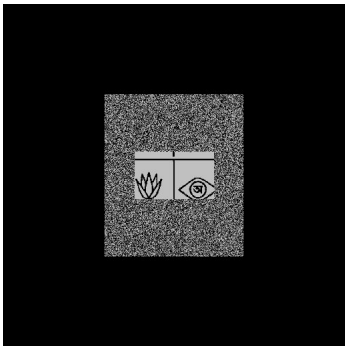


Figure 4.62: Result of detection algorithm on image of 4.61(b)

In multiply watermarked images made by the visible watermark in spatial domain technique, the first watermarks are not clear in the three test images. Approach 2, which means invisible watermark in spatial domain also failed to detect the first watermark after trying to extract the first watermark from the multiply watermarked images. Invisible watermarking in DCT domain has given successful watermark detection after multiple watermarking and extracting the first watermark. The correlations are 0.655371, 0.784655, and 0.721794 for Figure 4.57(c), 4.59(c), and 4.61(c) respectively.

4.3 Summary

Watermarks are embedded in some standard and arbitrary images and then they are distorted by some attacks which is also a part of this research. The test images are same for every experiment in this research. General attacks are discussed in Chapter 2. Among them, common nine distortion techniques are used to check the strength of watermark using three different techniques. The result after distorting the images has been included in this chapter. Result indicated the robustness of the implemented watermarking techniques which will be discussed in the next chapter.

Chapter 5

Conclusion

The results of the experiments shows the capability of the watermarks to sustain after attacks. The robustness of the techniques can be compared based on the result. This chapter will discuss the result written in the last chapter from a comparative view. Discussion about the techniques with the results after distorting the images are included in the next section. The conclusion will be drawn with a decision based on the experiment's result. This work will be carried on to achieve the goal of proposing a new method for digital watermarking. A touch of the future work will be added in this chapter.

5.1 Discussion

Digital watermark should be embedded with different techniques based on their usages. The users need to choose the method to apply watermark in their images according to the circumstance. A single technique cannot stand against all the distortion preserving the quality of the image. It needs a trade-off between image quality and robustness of watermark. Robust watermark is not always desired for every application. Some applications like authenticity determination needs fragile watermark also. Our experiment found the most robust and fragile watermarking techniques among the three techniques. The result has given the clear view of the strength of the techniques after distortions. Table 5.1 presents the result of this experiment in brief.

Table 5.1: Result Comparison of Three Watermarking Techniques

Distortion	**Approach 1**	**Approach 2**	**Approach 3**
Histogram Equalization	√	×	√
Cropping	√	×	×
Motion Blurring	×	×	√
Rotation	√	√	√
Flipping	√	√	√
Unsharp Masking	√	×	√
Scaling	√	×	×
JPEG Compression	√	×	√
Multiple Watermarking	×	×	√

The experiment shows that the visible watermark is robust against almost all attacks. Watermark embedded with visible watermarking in spatial domain technique can stand after the distortions made on the test images in this experiment. It cannot survive only against those distortions where the original image degraded in such extent that it is no more usable. Visible watermarking in spatial domain can be claimed as the most robust watermarking technique. However, it degrades the image quality and visibility. If the watermark is embedded in an insignificant part of image, it can be removed by cropping or another distortion. Embedding watermark in a significant portion of the image obscure the original image beneath the watermark. For this reason, the visible watermarking technique is not a good choice for sophisticated images where every detail needs to be perceptible.

Invisible watermark in spatial domain is the most sensitive to the tested distortions. Since invisible watermarking technique is sensitive even to the minimum possible degradation, therefore it is the obvious choice when a fragile watermark is

needed. The result of the experiment shows, it only remain after rotation-rerotation and flipping-reflipping attack which are not very significant distortion. These transformations do not change any information of the image. This method however degrades the detail information of the host image in the process of watermark insertion. The two LSBs of the original image under the watermark are washed out by embedding process of invisible watermarking in spatial domain. This technique cannot be a good choice for robust watermarking.

Watermarking in DCT is the most robust and imperceptible watermarking technique as observed in our experiment. It can stand against most attacks. The results indicate that the watermark cannot exist after cropping and scaling, but cropping and scaling also abolish the original image. It preserves the watermark against strong distortion as well as preserves the quality of the image. It is the robust and imperceptible watermarking which is best choice for many applications as been observed in our experiment. Achieving robustness and imperceptibility together is the desired characteristic of the watermarking technique. DCT based invisible watermarking is the best choice of all the three approaches tested in this experiment.

While embedding the watermark, the environment and the requirement should be checked to apply a specific watermarking technique. Though the watermarking in DCT domain shows the best results, it need extra module to extract and detect the watermark which is not possible in all the cases. Sometimes the watermark need to be detected by the human eyes so that anyone can know about the copyright or authentication only by visualizing. Hence, the circumstance and the use must be kept in mind before putting a watermark with the most appropriate method.

5.2 Future Work

The DCT based invisible watermarking algorithm is the most robust and imperceptible watermarking technique. However, if we compare it with the visible watermarking in spatial domain approach, the visible one is the most robust technique though it lacks in the issue of perceptibility. Thus invisible watermarking in DCT domain cannot be declared as best of all techniques. We are working forward to boost this approach. Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) will be used together to make the watermark embedding technique more robust.

Results and discussion exhibit that the most robust technique is the invisible watermarking in Discrete Cosine Transform domain among the implemented techniques. The sustainability of watermarks after distorting the images with distortions was in the consideration to conclude in a decision. The target to have a comparative study of digital watermarking techniques on still images has been gained.

Bibliography

[1] L. Piron, M. Arnold, M. Kutter, W. Funk, M. Boucqueau, and F. Craven, "OCTALIS benchmarking: Comparison of four watermarking techniques," in *Proceedings of Security and Watermarking of Multimedia Contents, 1999.*, vol. 3657, pp. 240–250, SPIE, April 1999.

[2] B. Gunjal and R. Manthalkar, "An overview of transform domain robust digital image watermarking algorithm," *Journal of Emerging Trends in Computing and Information Sciences*, vol. 2, no. 1, pp. 37–42, 2011.

[3] X. Zhang and Y. Yang, "Image authentication scheme research based on fragile watermarking," *Acta Electronica Sinica*, vol. 35, no. 1, pp. 34–39, 2007.

[4] J. Bloom, *A Brief Look at the History of the Watermarking Business.* http://www.dialogic.com/den/blogs/corporate/archive/2009/09/04/a-brief-look-at-the-history-of-the-watermarking-business.aspx, 2009. Accessed on December, 2012.

[5] S. Mohanty, K. Ramakrishnan, and M. Kankanhalli, "A DCT domain visible watermarking technique for images," in *Proceedings of International Conference on Multimedia and Expo (ICME), 2000.*, vol. 2, pp. 1029–1032, IEEE, 2000.

[6] AlpVision, *Digital Watermarking.* http://www.alpvision.com/watermarking. Accessed on December, 2012.

[7] C. Podilchuk and E. Delp, "Digital watermarking: algorithms and applications," *Signal Processing Magazine, IEEE*, vol. 18, no. 4, pp. 33–46, 2001.

[8] SMIT and VANWYK. http://www.svw.co.za/blog/digital-watermarking-as-a-means-to-protect-against-copyright-infringement.htm. Accessed on July, 2012.

[9] *Digital Watermarking.* http://en.wikipedia.org/wiki/Digital_watermarking, 2012. Accessed on December, 2012.

[10] PicMarkr, *What is Digital watermarking?* http://picmarkrpro.com/watermarking/index.htm, 2008. Accessed on December, 2012.

[11] Image Library Applications in IBM Research, *Watermarks: Protecting the image.* http://www.research.ibm.com/image_apps/watermark.html, 2003. Accessed on December, 2012.

[12] R. Gonzalez, R. Woods, and S. Eddins, *Digital Image Processing Using MATLAB.* Pearson Education India, 2 ed., 2009.

[13] M. Yeung, F. Mintzer, G. Braudaway, and A. Rao, "Digital watermarking for high-quality imaging," in *IEEE First Workshop on Multimedia Signal Processing, 1997.*, pp. 357–362, IEEE, June 1997.

[14] 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, 1997.

[15] F. Perez-Gonzalez and J. Hernandez, "A tutorial on digital watermarking," in *IEEE 33rd Annual 1999 International Carnahan Conference on Security Technology, 1999. Proceedings*, pp. 286–292, IEEE, 1999.

[16] S. Zahidahadi, *Spatial domain, Frequency domain, Time domain and Temporal domain*. http://ippr-practical.blogspot.com/2012/04/spatial-domain-frequency-domain-time.html, 2012. Accessed on December, 2012.

[17] N. Nikolaidis and I. Pitas, "Copyright protection of images using robust digital signatures," in *1996 IEEE International Conference on Acoustics, Speech, and Signal Processing, 1996. ICASSP-96. Conference Proceedings.*, vol. 4, pp. 2168–2171, IEEE, 1996.

[18] X. Xia, C. Boncelet, and G. Arce, "Wavelet transform based watermark for digital images," *Optics Express*, vol. 3, no. 12, pp. 497–511, 1998.

[19] V. Fotopoulos and A. Skodras, "Transform domain watermarking: adaptive selection of the watermarks position and length," in *Visual Communications and Image Processing*, vol. 5150, (Lugano, Switzerland), SPIE, July 2003.

[20] M. Khalili, "A comparison between digital image watermarking in tow different color spaces using DWT2," *Technical Report, Cornell University Library*, 2012.

[21] M. Barni, F. Bartolini, V. Cappellini, and A. Piva, "A DCT-domain system for robust image watermarking," *Signal processing*, vol. 66, no. 3, pp. 357–372, 1998.

[22] G. R. N. Kumari, B. VijayaKumar, L. Sumalatha, and V. Krishna, "Secure and robust digital watermarking on grey level images," *International Journal of Advance Science and Technology*, vol. 11, 2009.

[23] H. Ali and S. Khamis, "Robust digital image watermarking technique based on histogram analysis," *World of Computer Science and Information Technology Journal(WCSIT)*, vol. 2, no. 5, pp. 163–168, 2012.

[24] F. Mintzer, G. Braudaway, and M. Yeung, "Effective and ineffective digital watermarks," in *International Conference on Image Processing.*, vol. 3, pp. 9–12, IEEE, 1997.

[25] L. Li and B. Guo, "Localized image watermarking in spatial domain resistant to geometric attacks," *AEU-International Journal of Electronics and Communications*, vol. 63, no. 2, pp. 123–131, 2009.

[26] G. Zhu and N. Sang, "Watermarking algorithm research and implementation based on DCT block," *World Academy of Science, Engineering and Technology*, vol. 45, pp. 38–42, 2008.

[27] V. Potdar, S. Han, and E. Chang, "A survey of digital image watermarking techniques," in *3rd IEEE International Conference on Industrial Informatics.*, pp. 709–716, IEEE, 2005.

[28] R. C. Gonzalez and R. E. Woods, *Digital Image Processing*. Prentice Hall, 3 ed., 2008.

[29] K. Cabbin and P. Gent, *Image Compression and Discrete Cosine Transform*. College of Redwoods, Eureka, California, USA.

[30] S. Craver, N. Memon, B. Yeo, and M. Yeung, "Can invisible watermarks resolve rightful ownerships?," in *Electronic Imaging'97*, pp. 310–321, International Society for Optics and Photonics, 1997.

[31] *Test Images*. http://decsai.ugr.es/cvg/dbimagenes/index.php, 2012. Accessed on December, 2012.

[32] *Image files for Math 625*. http://www.math.umbc.edu/ rouben/2003-09-math625/images.html. Accessed on December, 2012.

[33] *Standard Images*. http://pami.uwaterloo.ca/tizhoosh/images.htm. Accessed on September, 2012.