

A COMPARATIVE STUDY OF REVERSIBLE DATA HIDING TECHNIQUES

PROJECT SUBMITTED TO THE DEPARTMENT OF *INFORMATION TECHNOLOGY* OF *BENGAL COLLEGE OF ENGINEERING & TECHNOLOGY* AFFILIATED TO *MAULANA ABUL KALAM AZAD UNIVERSITY OF TECHNOLOGY* FOR THE PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE DEGREE OF *B.TECH.*

PROJECT SUBMITTED BY:

- 1. Abhishek Mukherjee (12500212001)**
- 2. Ashish Kumar Singh (12500212016)**
- 3. Nidhi Krishna (12500212050)**
- 4. Nikhil Sinha (12500212052)**
- 5. Probuddha Singha (12500212064)**

UNDER THE GUIDANCE OF:

Mr. Sayan Chakraborty

Assistant Professor

Department of Computer Science and Engineering



**BENGAL COLLEGE OF ENGINEERING AND TECHNOLOGY
DURGAPUR- 713212**

CERTIFICATE

This is to certify that this project “**A COMPARATIVE STUDY OF REVERSIBLE DATA HIDING TECHNIQUES**” is a bonafide record of work done by:

1. **Abhishek Mukherjee (12500212001)**
2. **Ashish Kumar Singh (12500212016)**
3. **Nidhi Krishna (12500212050)**
4. **Nikhil Sinha (12500212052)**
5. **Probuddha Singha (12500212064)**

We are satisfied with their work which is being presented for the partial fulfilment of the degree of ***Bachelor of Technology in Information Technology.***

Prof (Dr.). P.K. Prasad
Principal
BCET, Durgapur

Prof (Dr.). D.K. Mania
Head of the Dept. (IT)
BCET, Durgapur

Sayan Chakraborty
Asst. Prof., Dept. of CSE
BCET, Durgapur



BENGAL COLLEGE OF ENGINEERING AND TECHNOLOGY
DURGAPUR- 713212

ACKNOWLEDGEMENT

With great esteem & reverence, we wish to express our deep sense of gratitude to our project guide (Mr. Sayan Chakraborty) for valuable guidance and timely suggestions. Our Sincere gratitude is expressed for his help, patronage & for going through the manuscript critically.

We will also want to express our profound thanks to our Project Guide for assigning us the project on “**A COMPARATIVE STUDY OF REVERSIBLE DATA HIDING TECHNIQUES**”.

We would also like to express our heartfelt gratitude to Dr. D.K Mania, H.O.D, IT Dept. and all the faculty members of our college, “Bengal College of Engineering & Technology” and Department of Information Technology, who helped us in all respect to reach our goal successfully.

Last but not the least, we would like to thank all our friends who actively and passively participated in making the project a grand success.

ABSTRACT

Digital watermarking is the practice of hiding a message in an image, audio, video or other digital media elements. Since the late 1990's, there has been an explosion in the number of digital watermarking algorithms published. But there are few widely accepted tools and metrics that can be used to validate the performance claims being asserted by members of the research community.

Robust image watermarks are watermarks designed to survive attacks including signal processing operations and spatial transformations. To evaluate robust watermarks, we need to evaluate how attacks affect the fidelity of an image. The mean square error (MSE) is the most popular metric to measure fidelity. MSE, as it is, cannot measure the fidelity for images that went through geometric attacks such as rotation, pixel loss attacks such as cropping, or valumetric attacks such as gamma correction. We take the approach of evaluating attacks using MSE by compensating valumetric, pixel loss, and geometric attacks using conditional mean, error concealment, and motion compensation, respectively.

Robust watermarks are evaluated in terms of fidelity and robustness. To measure robustness, bit error rate, message error rate and the receiver operating characteristic.

Keywords—Bisection method, RGB color, PSNR, Interpolation method, Gray scale, Green Plane, Blue Plane.

MOTIVATION

Digital image watermarking using bisection method is the main focus of this project. We got interested in this topic due to the increase requirement of watermarking application used now a day. We wanted to know about how one can embed information in an image such that he can later claim the ownership of that image by extracting back the embedded information. Hence, “copyright protection” of images was our first motivation in starting this project.

But as we progressed our aim is also to develop a watermarking program that would be able to implement the robust technique.

As we had no background in image watermarking before we started the project, we set the following as our objectives before starting the project:

1. Understanding the requirements of image watermarking based on its applications. A good understanding of these requirements is the first step in designing algorithms for different watermarking applications.
2. Familiarizing ourselves with the watermarking literature that has been developing fast in the last decade.
3. Understanding how the robustness of the image watermarks can be improved.
4. Implementing bisection watermarking algorithms and examine them in terms of how they meet the requirements of different applications and general requirements of watermarking.

TABLE OF CONTENTS

CHAPTER	PAGE NO.
1. INTRODUCTION	1 – 5
2. PROJECT OBJECTIVE	6 – 8
3. DIGITAL WATERMARKING	9 - 15
2.1 Classification of watermarking techniques	10
2.2 Types of watermarking	11
2.3 Watermarking for various media types	13
2.4 Criteria for a good watermark	14
4. PREVIOUS WORK	16 - 18
5. PROPOSED METHOD	19 - 22
4.1 Algorithm for embedding watermark	20
4.2 Explanation of proposed method	21
6. RESULT AND DISCUSSION	23 - 30
6.1(a) Result of embedding using bisection function	24
6.1(b) Result of extracting using bisection function	26
6.1(a) Result of embedding using squareroot function	27
6.1(b) Result of extracting using squareroot function	29
7. CONCLUSION	31 – 33
8. FUTURE SCOPE	34 – 35
REFERNECES	36 - 39

CHAPTER 1

INTRODUCTION

The advent of the Internet has resulted in many new opportunities for the creation and delivery of content in digital form. Applications include electronic advertising, real-time video and audio delivery, digital repositories and libraries, and Web publishing. An important issue that arises in these applications is the protection of the rights of all participants. It has been recognized for quite some time that current copyright laws are inadequate for dealing with digital data. This has led to an interest towards developing new copy deterrence and protection mechanisms. One such effort that has been attracting increasing interest is based on digital watermarking techniques. Digital watermarking [1] is the process of embedding information into digital multimedia content such that the information (which we call the watermark) can later be extracted or detected for a variety of purposes including copy prevention and control. Digital watermarking [2] has become an active and important area of research, and development and commercialization of watermarking techniques is being deemed essential to help address some of the challenges faced by the rapid proliferation of digital content.

Digital Watermarking: refers to hiding a message within an image or signal; it can be a video also. An image is used as a cover to hide the message which is intended for transfer. Now-a-days, digital watermarking is used in various applications.

Watermarking is mainly used for security purposes. Level of threats faced by watermarking [3] depends on the application area. The properties of a good watermark should include robustness and imperceptibility. Sometimes a watermarked image may be compressed before transferring. In a robust watermarking scheme, an image is less damaged after retrieving. The watermarked image can be noticed easily, if the quality of the watermarked image is seriously affected after embedding. The property of less degradation of an image is referred as imperceptibility. A category of fragile watermarking is reversible watermarking. Reversible watermarking [4] is of lossless type. The secret message is embedded as an invisible mark and recovered back after

the extraction of watermark. The properties are the same as watermarking scheme. The watermark can be easily embedded and retrieved by the users.

Applications of Watermarking:

The technology of digital watermarking has been submitted to be implemented in such many different applications

a) Copyright protection:-

Can be applied to most of the prominent implementations in existence at the present time for supplementing the vital issues of the copyright protection. It gives the kind of allowance for the owner to embed such information that relates to him/her for the purpose of preventing those without official authorizations from asserting such copyright. In consideration of this field of application, it would absolutely necessitate a great level of robustness which is one type of the watermarking requirements.

b) Copy Protection:-

The embedded watermark within this application has the future of disallowing whatever unauthorized duplication that might occur to the original cover. As an illustration, in case of an acquiescent DVD player, it will not playback, and in the same situation, there could be also such data that carry out the watermark [5] sign (copy never) won't function out unless the multimedia item has been purchased from the owner.

c) Content Authentication:-

This sort of implementation is performed for the intention of detecting no matter which potential modifications might occur to the cover item. For as much as in this matter in particularly, the digital watermark [6] will be a type of watermarking technique known as (fragile watermarking).

d) Tamper Detection and Localization: The localization and tamper detection ability is more the same as being related to the data authentication application somehow. The main goal of the tamper detection is to reveal the possible

alterations that could perhaps occur to the cover due to such manipulations or modifications and so on. In a matter of detecting the tamper in the multimedia item such as an image, then it would analyze the case of not being that object genuine.

The tamper localization ability however, permits supplementary investigations by acting as a tamper which can lead straight ahead to identify the regions of the multimedia object which have been tampered. In similarity within the data authentication [7] application, tamper and detection localization technique can also be attained by means of using either one of the watermarking requirements such that robust, fragile or even semi-fragile watermark.

- e) **Transaction Tracking:** This particular application is applied in contemplation of embedding the digital watermark [8] in the interest of carrying out the desired information that relates to the legal recipient of the original cover. This scheme is vital for the purpose of either supervising or else investigating whichever copies of the original cover which are being produced illegally to the public either to individuals. This implementation however is usually referred to as (fingerprinting).
- f) **Broadcast Monitoring:** This application embeds the desired watermark into the cover and using an intentional monitoring to ascertain whether the cover has been broadcasted as it was agreed on or not. As well, the watermark can be embedded into the public announcement section.

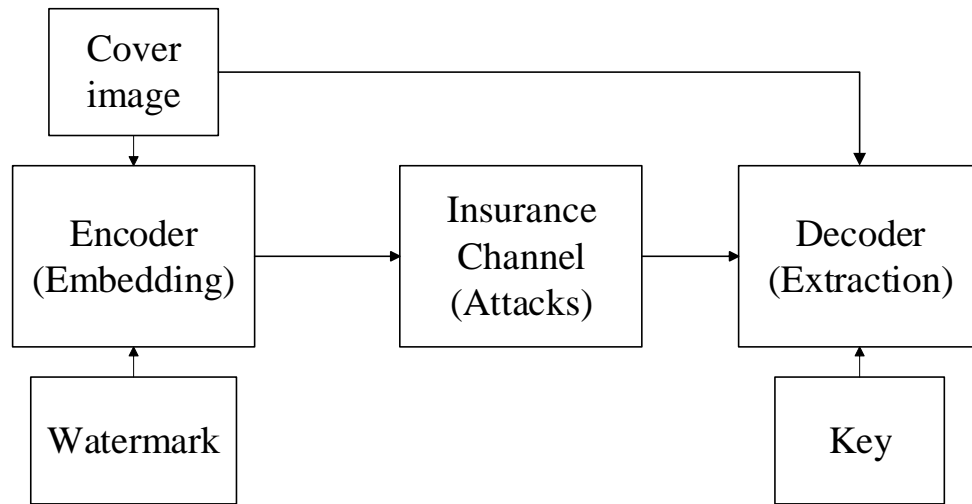


Fig. 1 The generic scheme for digital watermarking technique

All digital watermarking schemes could possibly partake in the same generic principal of the watermarking implementation which are the two watermarking systems and known as embedding and extracting systems. The scheme's input is the watermark itself and it can be such an image or a secret key [9]. The digital watermark can be formed in many different forms such as a text, a number or even an image. The real use of the key the scheme has is to compel the security [10] which then can prevent those unauthorized parties from manipulating either from recovering the watermark. The watermark scheme will have an output which is the watermarked data.

CHAPTER 2

PROJECT **OBJECTIVE**

The project objective is to propose a reversible color watermarking [10] technique to embed secret data bit-streams into the color image, using interpolation technique and bisection method. Our objective is to successfully embed and extract from the image without distorting the original image

Perceptual transparency: The substance that has been watermarked similarly would have the same subjective quality as the original contents.

Imperceptibility: This is an important property which is usually called as imperceptibility of digital watermark or sometimes it is indicated as fidelity or else called perceptual transparency. This property however can be described as the characteristic of hiding a watermark so that it does not degrade the visual quality of the image. Moreover whichever modifications occurred by means of watermark embedding should be then below the perceptible threshold. During the watermark embedding process the models of the human visual system (HVS) can be applied for the reason of enhancing the imperceptibility as well as the robustness of the watermark itself.

Robustness: It's the capability of the watermark to withstand distortion that has been introduced by standard or malicious data processing. No person has the ability to eliminate, modify, or damage the watermark without a secret key.

Security: It is the ability that watermark can resist malicious attacks. A watermark is secure if knowing the algorithms for embedding and extraction, it would not help unauthorized party to detect or remove the watermark. Secret key determines the value of watermark and the locations where the watermark is embedded.

Payload: The payload of watermarking is the amount of information to be embedded. In other words, it is the number of bits which are encoded into a message or else the data payload can be thought as the encoded message size of a watermark in such an image.

Capacity: Capacity is the amount of watermark information in an image. Multiple watermarks can be embedded and extracted. For instance, if multiple watermarks are being embedded into an image, then the watermark capacity [11] of the image is the sum of the individual watermark's data payload.

CHAPTER 3

DIGITAL **WATERMARKING**

3.1 Classification of watermarking techniques

- **Blind watermarking** scheme is also known as public watermarking scheme. The blind detection of the digital watermark [12] is referred to the ability of detecting the invisible information without the need for the reference image. The reference image however can be either the original image (cover image) or it is possible to be the stego image with such distinctive digital watermark or else the possibility of being a non-distorted one (stego image). Blind detection is a vital practical feature of watermarking technology so that in order to implement the extracting system for instance, the watermarking method itself should not be relying on the reference image. On the other hand, it should supply the blind detection feature which then can use the image under test only. In a different meaning, we can simply detect the watermark [13, 14] by the use of the test image only based on the blind watermark detection feature. This detection technique will take the test image as an input, and then later on execute the appropriate algorithm for the detection process, and as a result, it will output out the watermark that has been detected. These systems extract n bits of the watermark data from the watermarked data (i.e the watermarked image).
- **Semi-blind Watermarking:** Semi-blind watermarking scheme is also known as semi-private watermarking scheme [15]. This system does not require the cover (original data) for detection. The purpose of this system is to find whether that the watermark can be detected.
- **Non-blind Watermarking:** Non-blind watermarking [16] scheme is also known as private watermarking scheme. The non-blind detection of the digital watermark is more the same as the previous mentioned type that is the blind detection feature of the watermark, except that the non-blind detection type always demands for the reference image for the reason of extracting out the

watermark. However, this future is somehow impractical due to the probability of being the

- Reference image [16, 17] not readily attainable, but it can be more accurate for detecting the watermark signature. This system requires at least the cover (original data) for detection. Type I systems extract the watermark W from the possibly distorted data I' and use the original data as a hint to find where the watermark could be in I' .

3.2 Watermarking Types

There are several procedures for the intention of classifying the methods of watermarking. Such one of the most widely adopted systematic arranging is based on the robustness of watermarking. Beneath this category, digital watermarking can be sorted into three types as described below:

Robust watermark: This type is the watermark that has the feature to oppose the non-malicious distortion

Fragile watermark: The fragile watermarking classification can be easily destroyed by all image distortions.

Semi-fragile watermark: This type can be destroyed by certain types of distortions while it can withstand some other minor changes.

As long as robust watermarks can resist common image processing operation, they would be precisely suitable for copyright protection. Fragile watermark, on the other hand, can be used to discern the modification and verify an image since it's too sensitive to possible changes. However, semi-fragile watermarks are very often applied in some special cases of verification and tamper detection. These arguments may consider lossy image compression as legitimate modifications while highlighting distortions as premeditated attacks. In addition to watermark robustness, digital watermark can be as well classified into either visible or invisible watermark types.

Visible Watermarking:

Visible Watermarking: In the visible watermarking [18] technique, the structure is observable in the image or video for the observer. In a characteristic manner, the information can be referred as either text or a logo which can then acknowledge the rightful owner of the multimedia item. In case that when television broadcasters add up their logo to the corner of broadcast video, this is considered as a visible watermark.

- A visible watermark is considered to be ostensible enough in both color and monochrome images.
- The watermark [19] ought to be scattered in a spacious or consequential region of the image in order to hinder its obliteration by trimming off.
- The watermark need to be perceptible and must not necessarily blear details of the image underneath it.
- The watermark must be rigid to amputate.
- Amputating the watermark should be pricier and require a lot of work than procuring the image from the one who owns it.
- The watermark should be adjusted accordingly to the human interference and exertion.

Invisible Watermarking: In the invisible watermarking [20] approach, the information (watermark) is supplemented as digital data to the entities of multimedia such that video, audio or even still images; however, the inserted hidden information would not be distinguished as such. A significant application of this technique (invisible watermarking) is to copyright protection systems, which are designed for the reason of preventing or even deter such unauthorized copying of the digital multimedia. Furthermore, there happens to be also another type known as Steganography which is an application of digital watermarking, where two parties are

capable of communicating together via a secret message that is intended to be embedded in the digital signal. Annotation of digital photographs with descriptive information is another application of invisible watermarking. We are to express some thoughts about this technique through the next issue.

Steganography: This classification can comprise distinctive methods for concealing the existence of the additional information in a signal. The difference between Steganography and watermarking does not seem to be regularly obvious. Essentially, in case of watermarking the additional information is used to protect the original image (e.g. in case of copyright management), while on the contrary in the Steganography the image is used to protect the additional information (e.g. secret message).

3.3 Watermarking for Various Media Types

Digital Audio Watermarking: Digital audio watermarking involves the concealing of data within a discrete audio file. Applications for this technology are numerous. Intellectual property protection is currently the main driving force behind research in this area. To combat online music piracy, a digital watermark could be added to all recording prior to release, signifying not only the author of the work, but the user who has purchased a legitimate copy. Newer operating systems equipped with digital rights management software (DRM) will extract the watermark from audio files prior to playing them on the system. The DRM software will ensure that the user has paid for the song by comparing the watermark to the existing purchased licenses on the system.

Digital Video Watermarking: A very simple definition of video watermarking would be, "the process of watermarking [21] the sequence of video frames". There are several avenues in case of video to watermark. One can watermark the raw frame data, or the compressed data, where watermark the latter is more challenging. Videos can be considered as a stream of individual images. Hence, all image watermarking techniques are equally applicable to video when the individual frames are treated as

images. Such techniques do not make use of the availability of the temporal domain apart from the domain which image provide. This can lead to the design and use of sophisticated techniques, exploiting the presence of temporal domain. At the same time, the video provide new avenues for designing better attacks as well.

Image Watermarking: Visible watermarks on image can be easily achieved through image editing software. Ex. Image magic or any other, which have the watermark functionality. Invisible watermarks on images can be achieved through some proprietary software.

Text Watermarking: Digital watermarking [22] texts and sensitive documents is a lot more difficult than watermarking images and videos. There are a lot of redundancies in images, music files and videos. Since every pixel carries with it information, watermarking these types of media is a lot easier than doing the same on sensitive documents or text where every letter or word is important.

3.4 Criteria for a Good Watermark

Though watermarks belong to different categories, some of the general characteristics that watermarks must possess are the following:

1. The watermark must be strongly bound to the image and any changes to the watermark must be apparent in the image.
2. Watermark must also be able to withstand changes made to the image. Such changes include modifications and enhancements of images such as size modifications, cropping, lossy compression, to name a few.
3. The watermark must not undermine the visual appeal of the image by its presence (especially for invisible watermarks).
4. Watermark must be indelible and must be able to survive linear or non-linear operations on the image

The following are criteria for a visible watermark:

1. The watermark must be apparent on all kinds of images.
2. The size of the watermark is crucial. The more pervasive the watermark the better so that the watermarked area cannot be modified without tampering with the image itself.
3. The watermark must be fairly easy to implant in the image.

CHAPTER 4

PREVIOUS WORK

Although the art of papermaking was invented in China over one thousand years earlier, paper watermarks did not appear until about 1282, in Italy. The marks were made by adding thin wire patterns to the paper molds. The paper would be slightly thinner where the wire was and hence more transparent. The meaning and purpose of the earliest watermarks are uncertain. They may have been used for practical functions [4, 5] such as identifying the molds on which sheets of papers were made, or as trademarks to identify the paper maker. On the other hand, they may have represented mystical signs, or might simply have served as decoration. By the eighteenth century, watermarks on paper made in Europe and America had become more clearly utilitarian.

To record the date the paper was manufactured, and to indicate the sizes of original sheets. It was also about this time that watermarks [6, 7] began to be used as anti-counterfeiting measures on money and other documents. The term watermark seems to have been coined near the end of the eighteenth century and may have been derived from the German term wassermarke [5] (though it could also be that the German word is derived from the English). The term is actually a misnomer, in that water is not especially important in the creation of the mark. It was probably given because the marks resemble the effects of water on paper. About the time the term watermark was coined, counterfeiters began developing methods of forging watermarks used to protect paper money. Counterfeiting prompted advances in watermarking technology. William Congreve [6], an Englishman, invented a technique for making color watermarks by inserting dyed material into the middle of the paper during papermaking. The resulting marks must have been extremely difficult to forge, because the Bank of England itself declined to use them on the grounds that they were too difficult to make. A more practical technology was invented by another Englishman, Smith [7]. This replaced the fine wire patterns used to make earlier marks with a sort of shallow relief sculpture, pressed into the paper mold. The resulting variation on the surface of the mold produced beautiful watermarks with varying

shades of gray. This is the basic technique used today for the face of President Jackson on the \$20 bill. Four hundred years later, in 1954, Hembrooke [8] of the Muzak Corporation filed a patent for “watermarking” musical Works. An identification code was inserted in music by intermittently applying a narrow notch filter centered at 1 kHz. The absence of energy at this frequency indicated that the notch filter had been applied and the duration of the absence used to code either a dot or a dash. The identification signal used Morse code. It is difficult to determine when digital watermarking was first discussed. In 1979, Szepanski [9] described a machine-detectable pattern that could be placed on documents for anti-counterfeiting purposes. Nine years later, Holt described a method for embedding an identification code in an audio signal. However, it was Komatsu and tominaga [10], in 1988, which appear to have first used the term digital watermark. Still, it was probably not until the early 1990s that the term digital watermarking really came into vogue. About 1995, interest in digital watermarking began to mushroom. In addition, about this time, several organizations began considering watermarking technology for inclusion in various standards. The Copy Protection Technical Working Group (CPTWG) [11] tested watermarking systems for protection of video on DVD disks. The Secure Digital Music Initiative (SDMI) [12] made watermarking a central component of their system for protecting music. Two projects sponsored by the European Union, VIVA and Talisman, tested watermarking for broadcast monitoring. The International Organization for Standardization (ISO) [13] took an interest in the technology in the context of designing advanced MPEG standards. In the late 1990s several companies were established to market watermarking products. More recently, a number of companies have used watermarking technologies for a variety of applications.

CHAPTER 5

PROPOSED METHOD

4.1 ALGORITHM USED

A. Embedding Watermark within an image:

Step 1. Original image is read and divided into multiple 2x2 blocks.

Step 2. Each 2x2 block is converted into 3x3 blocks using interpolation (using bisection method)

Step 3. Logarithmic values of these new elements are taken and stored in a variable.

Step 4. Bit stream is chosen according to log values.

Step 5. The decimal values of those bit streams are embedded in the new elements of 3x3 blocks.

B. Extraction of Watermark from watermarked image:

Step 1. Watermarked image R is divided into 3x3 blocks.

Step 2. Embedded values are extracted from the watermarked image.

Step 3. Embedded bit stream is recovered by just calculating the difference in values of the elements ($R(1,2)$, $R(2,1)$, $R(2,2)$, $R(2,3)$, $R(3,2)$) of the received image and the ones calculated using bisection and are converted from decimal to binary.

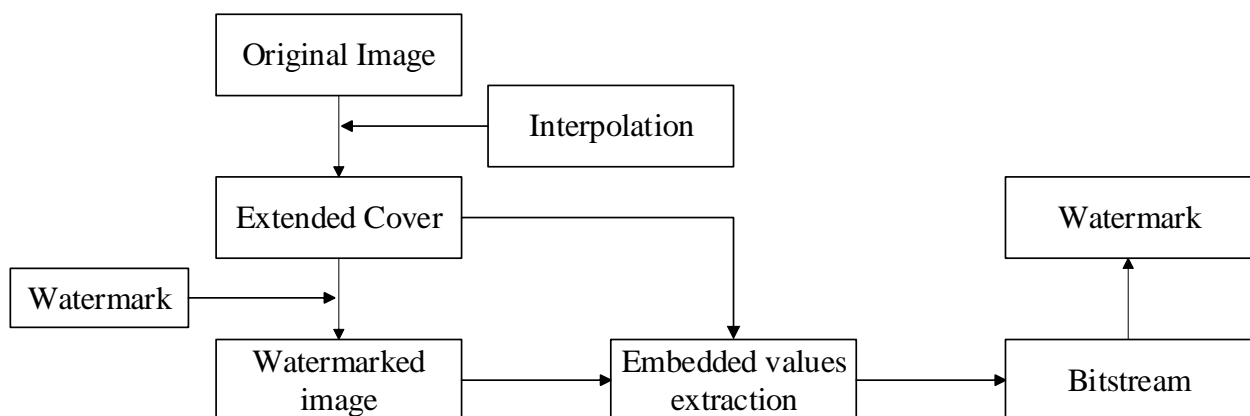


Fig. 2 Block Diagram of the proposed method including Watermark embedding and extraction

4.2 EXPLANATION OF THE PROPOSED METHOD

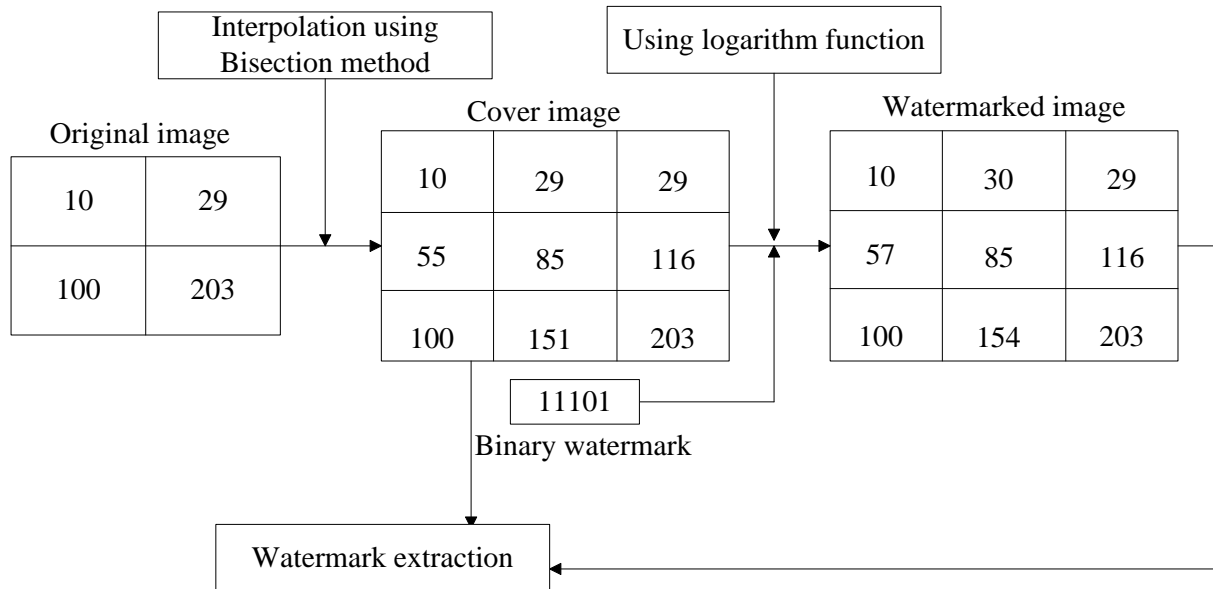


Fig. 3 Watermarking flow chart

Embedding a secret Binary Bit Stream :

- 1) We have an 128x128 cover image. This image is broken into 4096 no. of 2x2 blocks. i.e., [Block_1, Block_2,...Block_4096]
- 2) We take each 2x2 block & convert them into 3x3 blocks using interpolation technique. This done as follows:
Assuming the block is Block_1 :

$$\text{Block_1}[1,1] = \text{Block_1}[1,1]$$

$$\text{Block_1}[1,3] = \text{Block_1}[1,2]$$

$$\text{Block_1}[3,1] = \text{Block_1}[2,1]$$

$$\text{Block_1}[3,3] = \text{Block_1}[2,2]$$

$$\text{Block_1}[1,2] = (\text{Block_1}[1,1] + \text{Block_1}[1,3]) / 2$$

$$\text{Block_1}[2,1] = (\text{Block_1}[1,1] + \text{Block_1}[3,1]) / 2$$

$$\text{Block_1}[2,2] = (\text{Block_1}[1,2] + \text{Block_1}[3,2]) / 2$$

$$\text{Block_1}[2,3] = (\text{Block_1}[1,3] + \text{Block_1}[3,3]) / 2$$

$$\text{Block_1}[3,2] = (\text{Block_1}[3,1] + \text{Block_1}[3,3]) / 2$$
 This is done for each of the 4096 blocks
- 3) The bitstream that is to be embedded is choosen.
- 4) Log values of all the interpolated values are taken.
- 5) Number of bits are choosen from the left of the bitstream, accorrding to the log values. i.e., if log of first interpolated value is 1, only 1 bit is taken from left of the bitsream. Again, if log of the next interpolated value is 2, the next 2bits are taken from the bitstream. And so on.

- 6) Decimal of each binary value is found and is added to their respective previously interpolated values.
- 7) Steps [3-6] is repeated for each of the 4096 blocks
- 8) Finally we get a 192x192 watermarked image.

Extracting the secret Binary Bit Stream :

- 1) We have the 192x192 watermarked image. This image is broken into 4096 no. of 3x3 blocks. i.e., [Block_1, Block_2,...Block_4096]
- 2) Embedded bit stream is recovered by just calculating the difference in values of the elements (R(1,2), R(2,1), R(2,2), R(2,3), R(3,2)) of the received image and the ones calculated using bisection and are converted from decimal to binary. i.e., if the block is Block_1,

$$a = R(1,2) - [(Block_1[1,1] + Block_1[1,3])/2]$$

$$b = R(2,1) - [(Block_1[1,1] + Block_1[3,1])/2]$$

$$c = R(2,2) - [(Block_1[1,2] + Block_1[3,2])/2]$$

$$d = R(2,3) - [(Block_1[1,3] + Block_1[3,3])/2]$$

$$e = R(3,2) - [(Block_1[3,1] + Block_1[3,3])/2]$$
- 3) Binary of all the values a,b,c,d,e are found and are concatenated to find the secret binary bit stream
- 4) Steps [2-3] is repeated for each of the 4096 blocks
- 5) Finally we get the whole secret bit stream embedded in the entire image.

For Using Squareroot function,

We use the function $\sqrt{(Block_x[y1,z1]^2 + Block_x[y2,z2]^2)}/2$ in place of the bisection function.

CHAPTER 6

RESULTS AND DISCUSSION

The proposed method has been implemented using MATLAB R2013a on a 2.20 GHz Intel Core 2 Duo processor on Microsoft Windows 8.1 operating system. Images were watermarked using MATLAB [14].

6.1(a) Result of embedding using bisection function : $(a+b)/2$

Below result is obtained using Method 1:



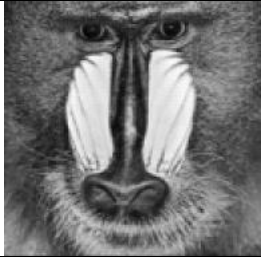




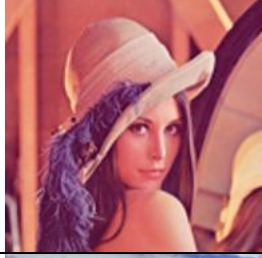












Images	Original	Grayscale	Gray Watermarked	Color Watermarked
Baboon				
Lena				
Airplane				
Pup				
Zelda				



Figure 4: (Col #1) Original image [size 128 x 128] , (Col #2) Original grayscale image [size 128 x 128], (Col #3) watermarked grayscale image (size 192 x 192) , (Col #4) Watermarked Color image (size 192 x 192).

Col #1 : The initial cover 128x128 color image is loaded

Col #2 : The 128x128 blue plane of the image in **Col#2** is extracted. This gives us the gray scale image. All pixel manipulations have been done on this blue plane itself

Col #3 : The secret binary image is embedded in the blue plane of the image in **Col#2**. This gives us the 192x192 watermarked grayscale image.

Col #4 : The image in **Col#3** is merged with the red & green planes to get the final 192x192 color watermarked image in **Col#4**

The ratio between the maximum possible power of any image and the power of corrupting noise which harms the fidelity of its representation is known as PSNR (Peak Signal to Noise Ratio). PSNR can be used to determine the transparency and distortion of the watermarked image with respect to original image. High PSNR value refers to better invisibility of the watermark.

$$PSNR = \frac{XY \max_{x,y} P_{x,y}^2}{\sum_{x,y} (P_{x,y} - \bar{P}_{x,y})^2} \quad (1)$$

Where, X and Y are referred to rows and columns in the original image used.

The original image is defined by $P_{x,y}$ whereas $\bar{P}_{x,y}$ is the watermarked image.

Table 1:Obtained PSNR value from blue plane:

Images	PSNR Value
Baboon 128×128	89.9833
Lena 128×128	99.2701

Airplane 128 x 128	85.8006
Pup 128 x 128	98.7364
Zelda 128 x 128	95.6211
Goldhill 128 x 128	88.0415
Baboon 256 × 256	88.6719
Lena 256 × 256	103.9073
Airplane 256 x 256	113.8924
Pup 256 x 256	120.0481
Zelda 256 x 256	119.8219
Goldhill 256 x 256	115.6049

Table 1 shows PSNR of original image and watermarked image. High PSNR shown in table 1 establishes robustness of our proposed method.

6.1(b) Result of extraction using bisection function : $(a+b)/2$

Below result is obtained using Method 1:



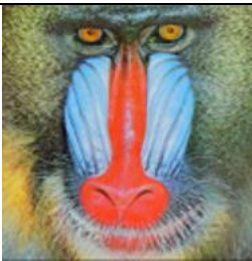



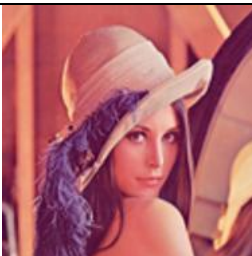

Original Carrier Image [128 X 128]	Embedded Secret Binary Image [128 X 128]	Watermarked Image [192 X 192]	Extracted Secret Binary Image [128 X 128]	Correlation
				1
				1

Figure 5: Watermark embedding and extraction using bisection

- Col #1 :** The initial cover 128x128 color image is loaded
- Col #2 :** The 128x128 secret binary image is loaded
- Col #3 :** The secret binary image is converted into a [1x16384] bit stream. This bitstream is then embedded in the **Col#1** image using our Proposed Embedding Method described in **Chapter 5** & we get the Watermarked image in **Col#3**
- Col #4 :** Now the [1x16384] bitstream is extracted from the **Col#3** image using our Proposed Extraction Method described in **Chapter 5** & it is resized into the [128x128] binary image in **Col#4**
- Col #5 :** The correlation between the embedded & extracted binary image is found.

Figure 5 shows the embedded and extracted secret binary image. The Correlation between the embedded and the extracted image gives the value 1. This means the image that was embedded is perfectly identical to the image that is extracted.

6.2(a) Result of embedding using squareroot function : $(\sqrt{a^2+b^2})/2$

Below result is obtained using Method 2:



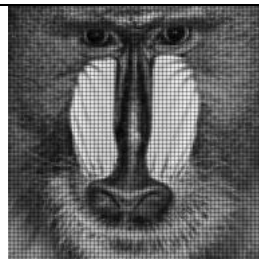
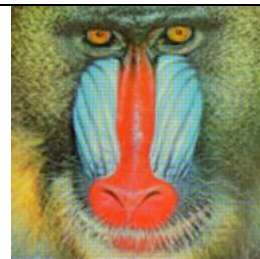



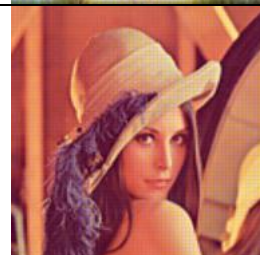
Images	Original	Grayscale	Gray Watermarked	Color Watermarked
Baboon				
Lena				



Figure 6: (Col #1) Original image [size 128 x 128] , (Col #2) Original grayscale image [size 128 x 128], (Col #3) watermarked grayscale image (size 192 x 192) , (Col #4) Watermarked Color image (size 192 x 192).

Col #1 : The initial cover 128x128 color image is loaded

Col #2 : The 128x128 blue plane of the image in **Col#2** is extracted. This gives us the gray scale image. All pixel manipulations have been done on this blue plane itself

Col #3 : The secret binary image is embedded in the blue plane of the image in **Col#2**. This gives us the 192x192 watermarked grayscale image.

Col #4 : The image in **Col#3** is merged with the red & green planes to get the final 192x192 color watermarked image in **Col#4**

Table 2: Obtained PSNR value from blue plane:

Images	PSNR Value
Baboon 128 × 128	58.5466
Lena 128 × 128	61.7353

Airplane 128 x 128	50.2555
Pup 128 x 128	61.0620
Zelda 128 x 128	68.4401
Goldhill 128 x 128	60.5162
Baboon 256 × 256	58.2299
Lena 256 × 256	61.3591
Airplane 256 x 256	50.2642
Pup 256 x 256	60.9434
Zelda 256 x 256	68.4506
Goldhill 256 x 256	61.1088

The current work, assessed correlation coefficient which is one of the well-known assessment methods of image quality. It can be calculated using equation 2.

$$r = \frac{\sum_{i=1}^{row} \sum_{j=1}^{col} (X(i, j) - \mu_x)(Y(i, j) - \mu_y)}{\sqrt{\left(\sum_{i=1}^{row} \sum_{j=1}^{col} (X(i, j) - \mu_x)^2 \sum_{i=1}^{row} \sum_{j=1}^{col} (Y(i, j) - \mu_y)^2 \right)}} \quad (2)$$

6.2(b) Result of extraction using squareroot function: $(\sqrt{a^2+b^2})/2$

Below result is obtained using Method 2:




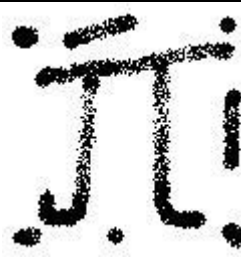



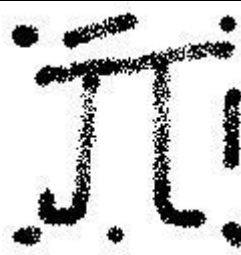
Original Carrier Image [128 X 128]	Embedded Secret Binary Image [128 X 128]	Watermarked Image [192 X 192]	Extracted Secret Binary Image [128 X 128]	Correlation
				1
				1

Figure 7: Watermarking embedding and extraction

Col #1 : The initial cover 128x128 color image is loaded

Col #2 : The 128x128 secret binary image is loaded

Col #3 : The secret binary image is converted into a [1x16384] bit stream. This bitstream is then embedded in the **Col#1** image using our Proposed Embedding Method described in **Chapter 5** & we get the Watermarked image in **Col#3**

Col #4 : Now the [1x16384] bitstream is extracted from the **Col#3** image using our Proposed Extraction Method described in **Chapter 5** & it is resized into the [128x128] binary image in **Col#4**

Col #5 : The correlation between the embedded & extracted binary image is found

Figure 7 shows the embedded and extracted secret binary image. The Correlation gives the value 1. This means the image that was embedded is perfectly identical to the image that is extracted.

CHAPTER 7

CONCLUSION

Here, we can embed numerous bits of watermark in every single block of the carrier image. If we have more bits to be embedded then we can use the other 3X3 blocks. The watermark is embedded in cover image and then resized, this can lead to imperceptibility. To avoid this problem, the size of the image is maintained in final step.

Digital watermarks are only perceptible under certain conditions, i.e. after using some algorithm, and imperceptible otherwise. If a digital watermark distorts the carrier signal in a way that it becomes perceivable, it is of no use. Traditional Watermarks may be applied to visible media (like images or video), whereas in digital watermarking, the signal may be audio, pictures, video, texts or 3D models.

In our project, we feel that our proposed method has some advantages & disadvantages.

Advantages :

- In each of the cases, the embedded secret binary image & the extracted secret binary image, both are exactly identical to each other. The correlation value between both the images is 1. This is a very impressive feat. i.e., there is no data loss in our secret message both while embedding & extracting.
- The algorithm used is simple enough to implement.

Disadvantages :

- In our proposed method, we have only used the blue plane only. If we had used the other 2 planes too, (i.e., Red, Green & Blue planes) our algorithm & watermarking technique could be made more secure from attacks.
- The PSNR values were not that impressive & were varying for the images
- The algorithm used is very simple. More complicated algorithms lower the risk of information being extracted from attacks.
- There is a limit to the number of bits that can be embedded into a cover image. For example, if we have an image of size $M \times M$ then,

Max. No. of bits that can be embedded into its watermarked image =

$$\frac{M \times M}{2 \times 2} \times 10$$

i.e., a 128x128 can embed at most 40960 bits.

Digital watermarking is a rapidly evolving area of research and development. One key research problem that we still face today is the development of truly robust, transparent and secure watermarking technique for different digital media including images, video and audio. Another key problem is the development of semi-fragile authentication techniques. The solution to these problem will require application of known results and development of new results in the fields of information and coding theory, adaptive signal processing, game theory, statistical decision theory, and cryptography. Although a lot of progress has already been made, there still remain many open issues that need attention before this area.

CHAPTER 8

FUTURE SCOPE

This project can be improved in future in many ways and can be made more secure to attackers:

- In our proposed method, we have only used the blue plane only for watermarking. The other 2 planes too, (i.e., Red, Green & Blue planes) can be used. This will make our algorithm & watermarking technique could be made more secure from attacks.
- Multiple layers of interpolation can improve the security of data. This can done by interpolating the interpolated values once again.
- PSNR values can be improved by using more optimised algorithms.
- In spite of using bisection, other functions can also be used to improve the algorithm. For example, trigonometric function can be used.
- Usage of different transformations. (Discreet Cosine Transforms, etc.)

REFERENCES

- [1] Poonkuntran R.S., Eswaran R.P. (2010), 'Reversible imperceptible semi-fragile watermarking scheme for digital fundus image authentication, *Int. J. of Signal and Imaging Systems Engineering*, Vol. 3, No.2 pp. 116 - 125.
- [2] Fadzil M.H.A., Iznita I.Z.L., Nugroho H.A. (2011) 'Area analysis of foveal avascular zone in diabetic retinopathy colour fundus images', *Int. J. of Medical Engineering and Informatics* 2011, Vol. 3, No.1 pp. 84 - 98
- [3] Zana, F., Klein, J. (2001) 'Segmentation of vessel-like patterns using mathematical morphology and curvature evaluation', in *IEEE Trans. Image Process.*, Vol. 10, No. 7, pp. 1010 -1019.
- [4] Hoover A., Goldbaum M. (2003) 'Locating the optic nerve in a retinal image using the fuzzy convergence of the blood vessels', in *IEEE Transaction on Medical Imaging*, Vol. 22, No. 8, pp. 951 -958.
- [5] Jiang X., Mojon D. (2003) 'Adaptive local thresholding by verification based multithreshold probing with application to vessel detection in retinal images', in *IEEE Trans. Pattern Anal. Mach. Intell.*, Vol. 25, No. 1, pp. 131 -137.
- [6] Niemeijer M., van Ginneken B., Staal J. J., Suttorp-Schulten M. S. A., Abramoff M. D. (2005) 'Automatic detection of red lesions in digital color fundus photographs', in *IEEE Transaction on Med. Imaging*, Vol. 24 , No. 5, pp. 584 - 592.
- [7] Foracchia M., Grisan E., Ruggeri A. (2005) 'Luminosity and contrast normalization in retinal images' in *Med. Image Anal.*, Vol. 9, No. 3, pp. 179 - 190.
- [8] Mendonça A. M., Campilho A. (2006) 'Segmentation of retinal blood vessels by combining the detection of centerlines and morphological reconstruction', in *IEEE Trans. Med. Imag.* Vol. 25, No. 9, pp. 1200 -1213.
- [9] Anderson, R.J. and Petitcolas, F.(1998) "On the Limits of Stenography." *IEEE Journal of Selected Areas in Communications*, vol. 16, Issue: 4, May, pp. 474 – 481.

- [10] Katzenbeisser, S. and Petitcolas, F. (2000) "Information Hiding Techniques for Stenography and Digital Watermarking", Artech House, 2000, pp. 245 – 267.
- [11] Sin-Joo Lee, Sung-Hwan Jung (2001) "A survey of watermarking techniques applied to multimedia Industrial Electronics", Proceedings. ISIE 2001. IEEE International Symposium on June, vol. 1, pp. 272 – 277.
- [12] Elizabeth, F. and Matthew, M. (1999) "A Survey of Digital Watermarking", February 25, pp. 127- 156.
- [13] Schyndel, R. Tirkel, A. and Osborne, C. (1994) "A Digital Watermark", *Proc. IEEE Int. Conf. on Image Processing*, Nov, vol. II, pp. 86-90.
- [14] Hwang, M.S. Chang, C. and Hwang, K. F. (2000) "Digital watermarking of images using Neural Networks", *Journal of Electronic Imaging*, pp. 548-555.
- [15] Zhang Zin-Ming, Li Rong-Yon, Wang Le, "Adaptive watermark scheme with RBF neural networks", *IEEE Intl. Conf. Neural Networks & Signal Processing*, pp. 1517-1520.
- [16] Gerhard C. Langelaar, Iwan Setyawan, and Reginald L. Lagendijk, "Watermarking Digital Image and Video Data", *IEEE Signal Processing magazine*, Sep. 2000, pp. 1053-1078.
- [17] Hartung, J. K. Su, and. Girod, B "Spread spectrum watermarking: Malicious attacks and counterattacks", *Proc. SPIE 3657: Security and Watermarking of Multimedia Contents*, San Jose, CA, January, 1999.
- [18] George, M. Chouinard, Y. and Georganas, N. " Spread Spectrum Spatial and Spectral Watermarking of for Images and Video", *Proc. 1999 IEEE Can. Workshop in Information Theory (CWIT'99)*, Kingston, Ont., June 1999.
- [19] Kutter, M. and Petitcolas, F. "A fair benchmark for image watermarking systems", *proceedings of Electronic Imaging '99, Security and Watermarking of Multimedia Contents*, vol. 3657, pp. 226~239, San Jose, California, U.S.A., January 1999.

- [20] Cox, I. J. Kilian, J. .Leighton, F.T and Shamoon, T. "Secure Spread Spectrum Watermarking for Multimedia", IEEE Trans. Image Proc., Vol. 6, No. 12, Dec. 1997.
- [21] Yeung, M.M and Mintzer, F. "An Invisible Watermarking Technique for Image Verification," *Proceedings of IEEE ICIP'97*, Santa Barbara, CA, Oct. 1997.
- [22] Craver,S. Memon,N. Yeo, B.L and Yeung, M.M "Resolving Rightful Ownership with Invisible Watermarking Techniques: Limitations, Attacks and Implications," *IEEE JSAC*, March 1997.
- [23] S. R. Chowdhury, R. Ray; N. Dey; S. Chakraborty; W. Ben Abdessalem Karaa & S. Nath, "Effect of demons registration on biomedical content watermarking", 2014 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), July 2014, pp.509-514.