CHAPTER 1
INTRODUCTION

1.1 INTRODUCTION

This era has very much advanced in the digital information . It has a wide range of connectivity, that is connection throughout the world through various networks such as internet and also a wide range of wireless network.through this revolution many devices such as digital camera ,a, and also camcorder,high quality printer a,digital voise recorder, and also mp3 player,PDA, have reached the consumers to create , and enjoy the data con Innovative devices such as digital camera and camcorder, high quality scanners and printers, digital voice recorder, MP3 player and PDA, have reached consumers worldwide to create, manipulate, and enjoy the multimedia data. The development of very high speed computer networks, has developed new means of business, scientific, the means of entertainment,opportunities in society.Electronic advertising,real-time information delivery, product ordering, magazines ,transaction processing, digital repositories, libraries, web newspapers , network video ,network audio, and also personal communication etc. But in order to make massive quantities of multi-media data will be transmitted by online at a satisfactory speed . else, they can be stored by consuming less space in memory when the network bandwidth is very much limited with small hardware storage, hence it is important for a good image compression scheme making it a secure secret data through the communication networks.

The commercial purposes are increasingly exploting the www(world wide web). Always,A replica of a digital media is similar to the original. This,has led to the use of digital content which has got a malicious intend, to protect the illegal recording of multimedia data and to retransmit it is to embedding a signal, which is called a digital signature also called as copyright else a watermark which authenticates the owner of the data. As it has become easy to edit and perfectly reproduce in digital domain, the protection of the ownership and preventing unauthorized messing up of the data in multimedia(for example,audio, image, video and document,etc).this process of embedding a secondary data in an image, has been a progress in recent years and has gained attention from academia as well as industry. Many Techniques are proposed for a variety of applications, that which claims ownership protection, also gives the authentication and provides the access control.

1.2 HISTORY OF WATERMARK

As we know Watermark is a term from two different streams, Cryptography meaning, “Secret writing” and Steganography, which means in the greek as “Cover writing”. It is also refered to as the knowledge or study of different methods of sending messages in distinct form so that only the sepcific recipients can remove the disguise or watermark hence they can read the message. The intended message which is required to be sent is called as a plain text message and the hidden message is called cipher text. The conversion of a plain text to a cipher text is a enciphering or encryption, and the vice versa the deciphering or decryption.

The technique of impressing into the paper, a form of image, or text derived from the negative in the mold, as the paper fibers are squeezed and dried. This is defined as watermarking scheme.Paper Watermarks have been in wide use since the late middle Ages. Their earliest use seems to have been to record the manufacturer’s trademark on the product so that the authenticity could be clearly established without degrading the aesthetics and utility of the stock. In more recent times, watermarks have been used to certify the composition of paper, including the nature of the fibers used. Today most developed countries also watermark their paper, currencies and postage stamps to make forgery more difficult. The digitization of our world has expanded the concept of watermarking to include immaterial digital impressions for use in authenticating ownership claims and protecting proprietary interests.

A watermark is a recognizable image or pattern in paper that appears as various shades of lightness/darkness when viewed by transmitted light (or when viewed by reflected light, atop a dark background), caused by thickness or density variations in the paper.There are two main ways of producing watermarks in paper; the dandy roll process, and the more complex cylinder mould process.

Watermarks vary greatly in their visibility; while some are obvious on casual inspection, others require some study to pick out. Various aids have been developed, such as watermark fluid that wets the paper without damaging it. Watermarks are often used as security features of banknotes, passports, postage stamps, and other documents to prevent counterfeiting .

A watermark is very useful in the examination of paper because it can be used for dating, identifying sizes, mill trademarks and locations, and the quality of a paper.

Encoding an identifying code into digitized music, video, picture, or other file is known as a digital watermark.

Dandy roll process

A watermark is made by impressing a water-coated metal stamp or dandy roll onto the paper during manufacturing. These watermarks were first introduced in Fabriano, Italy, in 1282.however the dandy roll was invented in 1826 by John Marshall. Watermarks have been used by papermakers to identify their product, and also on postage stamps, currency, and other government documents to discourage counterfeiting. In France, they were introduced during World War II by the Vichy regime, and counterfeited by people such as Adolfo Kaminsky. The invention of the dandy roll revolutionised the watermark process and made it much easier for a company to watermark its paper.

The dandy roll is a light roller covered by material similar to window screen that is embossed with a pattern. Faint lines are made by laid wires that run parallel to the axis of the dandy roll, and the bold lines are made by chain wires that run around the circumference to secure the laid wires to the roll from the outside. Because the chain wires are located on the outside of the laid wires, they have a greater influence on the impression in the pulp, hence their bolder appearance than the laid wire lines.

This embossing is transferred to the pulp fibres, compressing and reducing their thickness in that area. Because the patterned portion of the page is thinner, it transmits more light through and therefore has a lighter appearance than the surrounding paper. If these lines are distinct and parallel, and/or there is a watermark, then the paper is termed laid paper. If the lines appear as a mesh or are indiscernible, and/or there is no watermark, then it is called wove paper. This method is called line drawing watermarks.

Cylinder mould process

This type of watermark is the cylinder mould watermark. When a shaded watermark, first used in 1848, incorporates tonal depth and creates a greyscale image. Without using a wire covering for dandy roll, a shaded watermark can be created by the intended areas of relief on the roll's own surface. Once it becomes dry, the paper can be may then be rolled again in order to produce a watermark of even thickness but with a varying density. The resulting watermark is generally much clearer and more detailed than those made by the already mentioned Dandy Roll process, and as such Cylinder Mould Watermark Paper is the preferred type of watermarked paper for banknotes, passports, motor vehicle titles,some of the   other documents where it is a very important anti-counterfeiting basis of measurement.

Watermarks on postage stamps and stationery

In philately, the watermark is a key feature of a stamp, and often constitutes the difference between a common and a very rare stamp. Collectors who encounter two otherwise identical stamps with so many different watermarks consider each stamps as a separately identifiable issue.The "classic" stamp watermark is a small crown or other national symbol, appearing either once on each stamp or a continuous pattern. Watermarks were nearly universal on stamps in the very early periods that is the 19th and early 20th centuries, but generally fell out of use and are not at all common, but some countries continue to use them.

Also, there are some types of emb In philately, the watermark is considered as a key feature of a stamp, and has the difference between a common and a rare stamp. Collectors who usually encounter two otherwise identical stamps with different watermarks consider each stamp to be a very separately identifiable issue.The "classic" stamp watermark is a very small crown or other national symbol, appearing either once on each stamp or as continuous pattern. Watermarks were nearly universal on stamps in early times, but they have fallen out of use an. issues, but some countries are still using them.

Ealier,Some types of embossing, such as ,that which are used to make the "cross on oval" design on early stamps of Switzerland,often has a resemblance to the watermark in that the paper is thinner, but they can also be distinguished by having sharper edges than is usual for a normal watermark. Stamp paper watermarks also show so many various content which includes,designs, letters, some numbers and also pictorial elements.

The process of bringing out stamp watermark is very simple. Sometimes a watermark in each stamp paper can be seen by looking at unprinted back side of a given stamp. often, the collector must use a few basic items to get a good look for the watermark. Ie,For example, watermark fluid can be applied to the back of a stamp to temporarily reveal the given watermark.

Even using the simple watermarking method described, it is difficult to distinguish some of the watermarks. Watermarks on stamps are often printed in yellow and orange and is difficult to see. Some few mechanical devices are also used by collectors to detect watermarks used on various stamps such as Morley-Bright watermark detector and a very more expensive provided Safe Signoscope. Such devices are very useful for they are used without application of watermark fluid and also allows the collector to look at the watermark for a very longe period of time and hence to more easily detect the watermark.

Another technique,embossing, that used to make a"cross on oval" design on the early stamps provided in Switzerland, resemble a watermark in that the paper is thinner, but can be distinguished by having sharper edges than which is usual for a normal watermark. Stamp paper watermarks can also show various designs, letters, numbers and pictorial elements.

The process of bringing out the stamp watermark is fairly simple. Sometimes a watermark in stamp paper can be seen just by looking at the unprinted back side of a stamp. More often, the collector must use a few basic items to get a good look at the watermark. For example, watermark fluid can also applied to back of a stamp to temporarily reveal the watermark.

Even using the simple watermarking method described, it can be difficult to distinguish some watermarks. Watermarks on stamps printed in yellow and orange can be particularly difficult to see. A few mechanical devices are also are used by collectors to detect watermarks on stamps such as Morley-Bright watermark detector and the more expensive Safe Signoscope. These can be useful as they are used minus the application of watermark fluid and also allow the collector to look at the watermark for a longer period of time to more easily detect the watermark.

Audio watermarking

Audio watermark is a kind of digital watermark — where a marker is embedded within a audio signal, to identify the ownership of copyright for that audio,which is very important. Since we know to embed a watermark means is the process of embedding information into any signal (e.g. audio, video or pictures) so that it is difficult to remove. If the signal is copied, then the information is also being carried in the copy. A signal may also carry several so many different watermarks at the same time. It has also become very much increasingly important to enable copyright protection and ownership verification.

One of the most secured techniques of audio watermarking is a spread spectrum audio watermarking (SSW),which is a general technique for embedding the watermarks that we can implement in any transform domain or also can be in time domain. For example,In SSW, we transmit a narrow-band signal over a very much larger bandwidth such that signal energy presented in any signal frequency is undetectable. hence, the watermark is spread over so many frequency bins so that the energy hidden in one bin is undetectable. A feature of this mentioned watermarking technique is if to destroy it , then it requires noise of high amplitude which is to be added to all frequency bins. This type of watermarking is robust why, since to be confident that we can eliminate a watermark, the attack must attack all possible frequency bins with modifications of considerable strength. This will significantly create visible defects in the data.

Spreading spectrum is done by a sequence namely, pseudonoise (PN) sequence. In conventional SSW approaches, the receiver must also know the PN sequence which is used at the transmitter as well as also the particular location of the watermark in watermarked signal with the aim for detecting a hidden information. This is a very efficient high security feature, becuase any unauthorized and third party user who does not have access this information will not be able to detect any hidden information. Detection of the PN sequence is the   used key factor and it is used to detect hidden data/information from the given ssw.

It is often that the PN sequence detection uses very heuristic approaches like evolutionary algorithms, it consists of very high computational cost of this task and it can make it impractical. computational complexity which if often involved in the common usage of evolutionary algorithms particularly as a optimization tool is due to the fitness function evaluation that which makes it very difficult to define or makes it computationally very expensive. Most recent proposed approaches which helps in fast recovering of the PN sequence is the use of a fitness granulation as a promising fitness approximation scheme. With the use of fitness granulation approach called the Adaptive Fuzzy Fitness Granulation(AFFG), the expensive fitness evaluation step is replaced by an approximate model. When evolutionary algorithms is used as a means to extract the given hidden information, known as Evolutionary Hidden Information Detection, whether fitness approximation approaches (as a tool to accelerate the process) are used or not.

Digital watermarking

A digital watermark is a kind of a marker which is   very cleverly embedded in a noise-tolerant signal such as a audio or image data. It is often used to identifythe coreesponding ownership of the copyright of the given signal. We define

"Watermarking" as earlier is the process of hiding a particular digital information in a carrier signal; henceforth,the hidden information must,But does not need ,it may or may not contain any kind of relation to the carrier signal. Digital watermarks may also be used to verify the authenticity or integrity the corresponding carrier signal or to show the identity of its owners. Henceforth used for tracing the copyright infringements and also for banknote authentication. Like traditional watermarks, most of the digital watermarks are only perceptible under certain conditions given , i.e. after using some algorithm, and imperceptible here after to viewer anytime else.If a digital watermark some how distorts the carrier signal in a way that it becomes very much perceivable, it is of no use. Existing Traditional Watermarks may be applied to the visible media (like images or video), whereas in the case of digital watermarking, the signal may be audio, pictures, video, texts or 3D models. A signal may also carry several different watermarks at the same time. Unlike metadata that which is added to the carrier signal, a digital watermark is unable to change the size of the given carrier signal.

The needed properties of a digital watermark depend on the use case in which it is applied. For marking media files with copyright information, a digital watermark has to be rather robust against modifications that can be applied to the carrier signal. Instead, if integrity has to be ensured, a fragile watermark would be applied.

Both steganography and digital watermarking employ steganographic techniques to embed data covertly in noisy signals. But whereas steganography aims for imperceptibility to human senses, digital watermarking tries to control the robustness as top priority.

Since a digital copy of data is the same as the original, digital watermarking is a passive protection tool. It just marks data, but does not degrade it nor controls access to the data.

One application of digital watermarking is source tracking. A watermark is embedded into a digital signal at each point of distribution. If a copy of the work is found later, then the watermark may be retrieved from the copy and the source of the distribution is known. This technique reportedly has been used to detect the source of illegally copied movies.

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

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

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

1.3 ORGANIZATION OF THE REPORT

This report is organized as follows:

- Chapter 2 deals with the concept of compression

- Chapter 3 deals with human visual system and color space
- Chapter 4 deals with the concept of watermarking
- Chapter 5 deals with quality measurement
- Chapter 6 deals with encoder
- Chapter 7 deals with decoder and watermark extraction
- Chapter 8 deals with attacks and results
- Chapter 9 deals the conclusion part and future enhancement of the Project.

CHAPTER 2

COMPRESSION

2.1 INTRODUCTION

This chapter gives the outline about compression and the classical Block Truncation Coding (BTC) process.

2.2 IMAGE COMPRESSION

Compressing an image is significantly different than compressing raw binary data. Of course, general purpose compression programs can be used to compress images, but the result is less than optimal. This is because images have certain statistical properties which can be exploited by encoders specifically designed for them. Also, some of the finer details in the image can be sacrificed for the sake of saving a little more bandwidth or storage space. This also means that lossy compression techniques can be used in this area.

Lossless compression involves with compressing data which, when decompressed, will be an exact replica of the original data. This is the case when binary data such as executable, documents etc. are compressed. They need to be exactly reproduced when decompressed. On the other hand, images (and music too) need not be reproduced 'exactly'. An approximation of the original image is enough for most purposes, as long as the error between the original and the compressed image is tolerable.

2.3 QUANTIZATION

Quantization refers to the process of approximating the continuous set of values in the image data with a finite (preferably small) set of values. The input to a quantizer is the original data, and the output is always one among a finite number of levels. The quantizer is a function whose set of output values are discrete, and usually finite. Obviously, this is a process of approximation, and a good quantizer is one which represents the original signal with minimum loss or distortion.

There are two types of quantization – Scalar Quantization and Vector Quantization. In scalar quantization, each input symbol is treated separately in producing the output, while in vector quantization the input symbols are clubbed together in groups called vectors, and processed to give the output. This clubbing of data and treating them as a single unit, increases the optimality of the vector quantizer at the cost of increased computational complexity. BTC is based on vector quantization.

2.4 BLOCK TRUNCATION CODING

Block Truncation Coding (BTC), which was proposed by Delp and Mitchell in 1979 [1],[2]is an image compression technique which is used for fast compression. It uses two quantization levels in each block, such that overall mean and variance in each block is preserved. Each pixel is coded with one bit indicating the quantization level and for each block the two quantization levels must be transmit. So the lower limit of this compression method is 1 bit/pixel. The basic concept of this technique is to divide the original image into many non-overlapped blocks. For each block the Mean and Standard Deviation are calculated, these values change from block to block. These two values define what values the reconstructed or new block will have, in other words the blocks of the BTC compressed image will all have the same mean and standard deviation of the original image. A two level quantization on the block is where we gain the compression. In traditional BTC, the two values also preserve the first-moment and second-moment characteristics of the original block. When a BTC image is transmitted, each pair of values (2x8 bits/block) and the bitmap which stores the arrangement of the two values in each block (1 bit/pixel) are required. Although BTC cannot provide comparable coding gain as other modern compression techniques, such as JPEG or JPEG2000, the complexity of BTC is much lower than that of these modern techniques, which makes it feasible for less powerful processing kernel, such as Arm-based applications. Suppose the original image of size (PxQ) is divided into non-overlapped blocks, each of which is of size (MxN) and processed independently. For traditional BTC, the first-moment, second-moment, and the corresponding variance are obtained as equations 2.1, 2.2, 2.3.

$$\bar{x} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} x_{ij} \text{(2.1)}$$

$$\bar{x}^2 = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} {x_{ij}}^2 \text{(2.2)}$$

$$\sigma^2 = \bar{x}^2 - (\bar{x})^2 \text{(2.3)}$$

Where, x_{ij} denotes the gray scale value of the original image. The concept of traditional BTC is to preserve the first- and second- moments of a block when original value is substituted by its high- or low-means. Thus, the following equations 2.4, 2.5 should be maintained:

$$m\bar{x} = (m - q)a + qb \text{(2.4)}$$

$$m\bar{x}^2 = (m - q)a^2 + qb^2 \text{(2.5)}$$

Where *m*=MxN , and q is the number of pixels greater than $\bar{x}$. The high- and low-means can be evaluated as given in equations 2.6, 2.7.

$$a = \bar{x} - \sigma\sqrt{\frac{q}{m-q}} \qquad \text{(2.6)}$$

$$b = \bar{x} - \sigma\sqrt{\frac{m-q}{q}} \qquad \text{(2.7)}$$

Where, a and b denote low-mean and high-mean, respectively. Since BTC is a one-bit quantizer, the mean is employed to threshold the block. The binarized result is called bitmap, which is used for recording the arrangement of the two represented values, low-mean and high-mean, these values are obtained using equation 2.8.

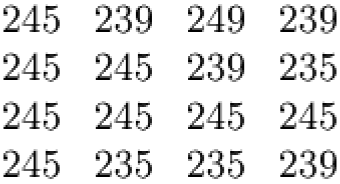
$$y_{ij} = \begin{cases} b, & if\ h_{ij} = 1 \\ a, & if\ h_{ij} = 0 \end{cases} \qquad \text{Where,} \qquad h_{ij} = \begin{cases} 1, & if\ x_{ij} \geq \bar{x} \\ 0, & if\ x_{ij} < x \end{cases} \qquad (2.8)$$

Where, h_{ij} denotes bitmap, and y_{ij} denotes the resulted BTC image.

2.4.1Example

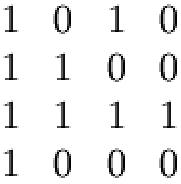
2.4.1.1 Encoder

Consider a 4x4 block from an image, in this case the let’s assume the image values of the block as:



245	239	249	239
245	245	239	235
245	245	245	245
245	235	235	239

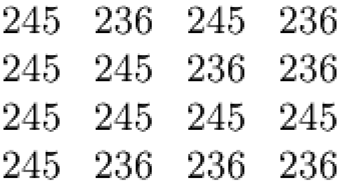
Like any small block from an image this appears rather boring to work with as the numbers are all quite similar, this is the nature of lossy compression and how it can work so well for images. Now we need to calculate two values from this data, which is the mean and standard deviation. The mean can be computed to 241.875, this is a simple calculation which should require no further explanation. The standard deviation is easily calculated as 4.36. From this the values of "a" and "b" can be calculated using the equations. They come out to be 236.935 and 245.718 respectively. The last calculation that needs to be done on the encoding side is to set the matrix to transmit to 1's and 0's so that each pixel can be transmitted as a single bit.



1	0	1	0
1	1	0	0
1	1	1	1
1	0	0	0

2.4.1.2 Decoder

Now at the decoder side all we need to do is reassign the "a" and "b" values to the 1 and 0 pixels. This will give us the following block:



245	236	245	236
245	245	236	236
245	245	245	245
245	236	236	236

As can be seen, the block has been reconstructed with the two values of "a" and "b" as integers (because images aren't defined to store floating point numbers). When working through the theory, this is a good point to calculate the mean and standard deviation of the reconstructed block. They should equal the original mean and standard deviation. Remember to use integers; otherwise much quantization error will become involved, as we previously quantized everything to integers in the encoder.

2.5 SUMMARY

The process of compression and the BTC technique has been discussed. The moment preserving technique of traditional BTC can be over ridded to gain computational efficiency by preserving only the first moment.

CHAPTER 3

HUMAN VISUAL SYSTEM AND COLOR SPACE

3.1 INTRODUCTION

In this chapter the Human Visual System and its short comings and procedures to take advantage of those short comings are discussed.

3.2 HUMAN VISUAL SYSTEM (HVS)

A human visual system model (HVS model) is used by image processing, video processing and computer vision experts to deal with biological and psychological processes that are not yet fully understood. Such a model is used to simplify the behaviors of what is a very complex system. As our knowledge of the true visual system improves, the model is updated. It is common to think of "taking advantage" of the HVS model to produce desired effects. Examples of taking advantage of an HVS model include color television.

The visual system in humans allows individuals to assimilate information from the environment. The act of seeing starts when the lens of the eye focuses an image of its surroundings onto a light-sensitive membrane in the back of the eye, called the retina. The retina is actually part of the brain that is isolated to serve as a transducerfor the conversion of patterns of light into neuronal signals. The lens of the eye focuses light on the photoreceptive cells of the retina, which detect the photons of light and respond by producing neural impulses. These signals are processed in a hierarchical fashion by different parts of the brain, from the retina upstream to central ganglia i.e. the brain [6].

Retina is made of rod cells and cone cells. The rod cells are sensitive to light whereas the cone cells are the one responsible for color sensitivity. Number of rod cells is more than the cone cells thus the sensitivity to color is also less. The human eye has fairly little spatial sensitivity to color, the accuracy of the brightness information of the luminance channel has far more impact on the image detail discerned than that of the color i.e. The color resolution of the HVS was much lower than the brightness resolution. Understanding this human shortcoming, standards such as NTSC reduce the bandwidth of the chrominance channels considerably.

3.3 COLOR SPACE

3.3.1 RGB Color Space

An RGB color space is any additive color space based on the RGB color model. A particular RGB color space is defined by the three chromaticity, red, green, and blue additive primaries, and can produce any chromaticity that is the triangle defined by those primary colors.

3.3.2 YIQ Color Space

YIQ is the color space used by the NTSC color TV system, employed mainly in North and Central America, and Japan. In the U.S., it is currently federally mandated for analog over-the-air TV broadcasting as shown in this excerpt of the current FCC rules and regulations part 73 "TV transmission standard".YIQ map is an m-by-3 matrix that contains the NTSC luminance (*Y*) and chrominance (*I* and *Q*) color components as columns that are equivalent to the colors in the RGB color map. As the human eye has fairly little spatial sensitivity to color, I and Q matrix is compressed more than that of the Y matrix. Thus a good quality image can be achieved with comparatively high compression than that done in RGB plane.

3.3.3 Color Space Conversion

3.3.3.1 RGB to YIQ

The color signal (RGB map) is converted to YIQ (NTSC) color space. The equation for RGB to YIQ transformation is given in equation 3.1

$$\begin{bmatrix} Y \\ I \\ Q \end{bmatrix} = \begin{bmatrix} 0.299 & 0.587 & 0.114 \\ 0.596 & -0.274 & -0.322 \\ 0.211 & -0.523 & 0.312 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix} \qquad (3.1)$$

3.3.3.1 YIQ to RGB

The YIQ i.e. the luminance and chrominance signals are converted to RGB natural color signals. The equation for YIQ to RGB transformation isgiven in equation 3.2

$$\begin{bmatrix} R \\ G \\ B \end{bmatrix} = \begin{bmatrix} 1 & 0.956 & 0.621 \\ 1 & -0.272 & -0.647 \\ 1 & -1.106 & 1.703 \end{bmatrix} \begin{bmatrix} Y \\ I \\ Q \end{bmatrix} (3.2)$$

3.4 SUMMARY

The HVS is studied and the human eyes behavior and sensitivity short comings are used to increase the compression ratio and the method for converting the natural color signals to the YIQ signals has been discussed.

CHAPTER 4

WATERMARKING

4.1 INTRODUCTION

In this chapter different classification of watermarking is discussed. The classification is based on different aspects and the sub-classification of the different aspects.

4.2 CLASSIFICATION OF WATERMARKING

There are different classifications of digital watermark algorithms [7, 8]. Based on different aspects they are as follows

4.2.1 Type of Data

Watermarktechniques can be divided into four groups according to the type of data to bewatermarked.

- Text watermarking
- Image watermarking
- Video watermarking
- Audio watermarking

4.2.2 Human Perception

Based on human perception, watermark algorithms can be divided into twocategories:

- Visible watermarking.
- Invisible watermarking.

Visibility is associated with perception of the human eye so that if the watermark isembedded in the data in the way that can be seen without extraction, we call thewatermark visible. Examples of visible watermarks are logos that are used in papersand video. On the other hand, an invisible watermarking cannot be seen by human eye.So it is embedded in the data without affecting the content and can be extracted bythe owner or the person who has right for that. For example images distribute over theinternet and watermarked invisible for copy protection.

4.2.3Information for Detection

Watermark algorithms are classified based on information for detection. Theyare as follows.

• Blind or public watermarking: In public watermarking, there is no need for originalsignal during the detection processing to detect the watermark. Only the secretkey is required. For example, in image blind watermarking we do not need theoriginal image.

• Non-blind or private watermarking: In non-blind or private watermark, originalsignal is required for detection the watermark.

• Semi-blind watermarking: In semi-blind watermarking, sometimes we may needsome extra information for detecting the watermark. Some watermarking requiresaccess to the original signal just after adding the watermarking, which is calledpublished watermarked signal. This form of watermarking is called semi-blindwatermarking.

4.2.4Processing-domain

Based on processing-domain, watermark techniques can be divided into:

• **Spatial domain:** A watermark technique based on the spatial domain, spread watermark data to be embedded in the pixel value. These approaches use minorchanges in the pixel value intensity.

For example, some algorithm inserts pseudo-random noise to image pixels. Other techniques modify the Least Significant Bit(LSB) of the image pixels. The invisibility of the watermark data is obtained on the assumption that he LSB bits are visually insignificant. There are two ways of doing an LSB modification. There are some methods to change the LSB bits.The LSB of each pixelcanbereplacedwiththe secret message or image pixels may be chosen randomly according to a secret key. Here is an example of modifying the LSBs, suppose we have three R,G, and B component in an image. Their value for a chosenpixel is green (R,G,B) =(0,255,0). If a watermark algorithm wants tohidethe bitvalue1inRcomponentthenthenewpixelvaluehas components(R,G,B)=(1,255,0). As this modification is so small, the new image is to the human eye in distinguishable from the original one.

Asanother example, an image is divided into the same size of blocks and a certainwatermark data is added with the sub-blocks [9].

- **Transform domain:** To have imperceptibility as well as robustness, adding of watermarkis done in transform domain. In this method, transform coefficients aremodified for embedding the watermark. Transform domain is also called frequencydomain because values of frequency can be altered from their original. The mostimportant techniques in transform domain are Discrete Cosine Transform (DCT)and Discrete Wavelet Transform (DWT).

4.2.5 Robustness

Classification can be based on the robustness feature. Different techniquesof this category are as follows.

- **Robust watermark:** One of the properties of the digital watermarking is robustness.We call a watermark algorithm robust if it can survive after common signalprocessing operations such as filtering and lossy compression.

- **Fragile watermark:** A fragile watermark should be able to be detected after anychange in signal and also possible to identify the signal before modification. Thiskind of watermark is used more for the verification or authenticity of originalcontent.
- **Semi-fragile watermark:** Semi-fragile watermark is sensitive to some degree of thechange to a watermarked image.

Furthermore,from application point of view, watermark techniques can be grouped as source based or destination based. In source based, all copies of a particular data have a unique watermark, which identifies the owner of that data,while in the destination based; each distributed copy is embedded using a unique watermark data,which identifies a particular destination.

4.3 REQUIREMENTS ANALYSIS

It is important to define the requirements of a watermarking system, because they are used to define a standard for comparison between different systems and selecting any one for use for a particular application. The two key aspects of a watermarking system are: imperceptibility of the watermark within the host signal, and also the security of the watermark against all the common operations or attacks. This security may be further broken down into two features: robustness to signal processing and whether the watermark is private or public in nature. The exact requirements, of course, will vary between applications. All the the three requirements are examined further in the following sections discussed below.

4.3.1 Imperceptibility

Most importantly, the watermark signal should be imperceptible to the end user who is listening to or viewing the host signal. i.e, the perceived quality of the host signal should not be distorted by the watermark. Henceforth, any typical user should never differentiate between watermarked and unwater marked signals. There are two reasons why it is important to ensure that the watermark signal is imperceptible. First reason is that the, the presence or absence of a watermark should not turn away from the primary aim of any host signal, conveying a very high-quality audio or say, visual information.Also, to that, perceptible distortion may indicate the presence of a watermark, and may be its precise location in within a host signal. This knowledge can be used by third party to distort,or replace, or completely degrade or remove the data which is watermarked.

4.3.2 Robustness to Signal Processing

Also,another important requirement is that watermark signals must be reasonably resilient to common signal processing operations. When or once a host signal is encoded with watermark data, distortions may be applied to the signal before, during, and also after transmission across the Internet. These distortions can be designed to grade the quality of the host signal or to compress it before the transmission, may or may not significantly disrupt the host signal. Examples include advantages such as reducing the noise (low pass or mean filtering), enhancing the feature (histogram equalization), and lossy compression.

4.3.3 Private vs. Public Watermarks

The scientist Craver et al has distinguished between types of watermarking systems,as, private and public.Definition of a private watermarking system -original signal is present at the decoder and hence we extract watermark information from the transmitted data.but as we know, a public system dont require access to any original signal so as to decode the watermark. The terms private and public also indicate, to some degree, that the intended audience of watermark data is also being send through a host signal. Where as a public system, would typically be used to send watermarks to the end-users of a host signal, whereas a private watermarking system would be more secure. But, Private watermarking is not practical for those applications where a lot of host signals are present or a lot of end users are involvedso in this case, it is not good to transmit both original and also watermarked versions,ie,for example we can give HDTV(High Definition Digital Telvision).In this case, it is not good to transmit both the original and watermarked versions of the host signal. However, private watermarking is suitable for other applications, such as online stock photography shops, where a private library of digital media is maintained by the business, and watermarked versions are sold to consumers.Here, the emphasis will be on public watermarking algorithms, since it is likely that they are of more use in some of the daily practical applications.

4.4SUMMARY

In this chapter ,so far, we have discussed different classification of watermarking and also went through their sub-classification . In this matter,The work we have discussed is on spatial domain, invisible, semi-blind, image watermarking.

CHAPTER 5

QUALITY MEASUREMENT

5.1 INTRODUCTION

This chapter deals with different error matrices classically used and their limitations and the universal quality index.

5.2 OBJECTIVE QUALITY MEASUREMENT

Objective image quality measures play important roles in various image processing applications. There are basically two classes of objective quality or distortion assessment approaches. The first is mathematically defined measures such as the widely used Mean Squared Error (MSE), Peak Signal to Noise Ratio (PSNR), Root Mean Squared Error (RMSE), Mean Absolute Error (MAE), and Signal to Noise Ratio (SNR). The second class of measurement methods considers Human Visual System (HVS) characteristics in an attempt to incorporate perceptual quality measures.

5.3 MERITS OF MATHEMATICAL APPROACH

Mathematically defined measures are very important and very much intimidating because of two reasons. One is that they are easy to calculate and usually have low computational complexity. Other is that they are independent of viewing conditions and individual observers. Even though people say that the viewing conditions play important roles in human perception of image quality, most of the cases they are not fixed and specific data is generally not available to image analysis system.suppose we say there are N different viewing conditions, a viewing condition dependent method will generate N different measurement results that are inconvenient to use. Also, it becomes the headache of the user to measure the viewing conditions and to calculate and input the condition parameters to the measurement systems. Also , a viewing condition independent measure gives only a a single quality value making the observer to jugde how good is the image.

5.4 ERROR METRICS

Two of the error metrics used to compare the various image compression techniques are the Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR). The MSE is the cumulative squared error between the compressed and the original image, whereas PSNR is a measure of the peak error. The mathematical formulae for the two are given in equations 5.1, 5.2.

$$MSE = \frac{1}{m\times n}\sum_{x=1}^{m}\sum_{y=1}^{n}\left\lfloor I(x,y) - I(\acute{x},y)\right\rfloor^{2} \qquad (5.1)$$

$$\text{PSNR} = \quad 20 * \log10\,(255 / \surd(\text{MSE})) \qquad (5.2)$$

Where, I(x,y) is the original image, I'(x,y) is the approximated version (which is actually the decompressed image) and M,N are the dimensions of the images. A lower value for MSE means lesser error, and as seen from the inverse relation between the MSE and PSNR, this translates to a high value of PSNR. Logically, a higher value of PSNR is good because it means that the ratio of Signal to Noise is higher. Here, the 'signal' is the original image, and the 'noise' is the error in reconstruction. So, if a compression scheme having a lower MSE (and a high PSNR), it can be recognized that it is a better one.

5.5 UNIVERSAL IMAGE QUALITY INDEX (UQI)

The error metric’s mentioned above gives the actual error between the pixel values. When error is to be calculated for an image the HVS has to be considered and only notable difference is to be calculated. Whereas, the UQI gives a block based approach with three different criteria's Loss of correlation, Luminance distortion, Contrast distortion. UQI method does not depend on the image being tested, the viewing conditions or the individual observers [3].

The UQI is given by the equation 5.3, 5.4, 5.5.

$$Q = \frac{4\sigma_{xy}\bar{x}\bar{y}}{\left(\sigma_x^2+\sigma_y^2\right)((\bar{x})^2+(\bar{y})^2)} \tag{5.3}$$

Where

$$X = \{x_i; i = 1,2, \dots., N\} \tag{5.4}$$

$$Y = \{y_i; i = 1,2, \dots., N\} \tag{5.5}$$

X is original image and Y is the test image signal respectively.

$$\bar{x} = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{5.6}$$

$$\bar{y} = \frac{1}{N}\sum_{i=1}^{N} y_i \tag{5.7}$$

$$\sigma_x^2 = \frac{1}{N-1}\sum_{i=1}^{N}(x_i - \bar{x})^2 \tag{5.8}$$

$$\sigma_y^2 = \frac{1}{N-1}\sum_{i=1}^{N}(y_i - \bar{y})^2 \tag{5.9}$$

$$\sigma_{xy} = \frac{1}{N-1}\sum_{i=1}^{N}(x_i - \bar{x})(y_i - \bar{y}) \tag{5.10}$$

Where $\bar{x}$is the mean of x given in equation 5.6, σ_x^2 is the variance of xgiven in equation 5.8, $\sigma_y^2$is the variance of y given in equation 5.9, $\sigma_{xy}$is covariance of x and y given in equation 5.10.

This quality models any distortion as a combination of three different factors

1. Loss of correlation

2. Luminance distortion
3. Contrast distortion

In order to understand this definition of Q can be rewritten as a product of three components given in equation 5.11.

$$Q = \frac{\sigma_{xy}}{\sigma_x \sigma_y} \frac{\overline{2x}\bar{y}}{(\bar{x})^2+(\bar{y})^2} \frac{2\sigma_x \sigma_y}{\sigma_x^2+\sigma_y^2} \tag{5.11}$$

The first component is the correlation coefficient between x and y, which measures the degree of linear correlation between x and y, and its dynamic range is {-1, 1}. The best value is 1. Even if x and y are linearly related, there still might be relative distortions between them, which are evaluated in the second and third components. The second component, with a value range of {0, 1}, measures how close the mean luminance is between x and y. The component measures how similar the contrasts of the images arewith a value range of {0, 1}.

The quality measurement method is applied using sliding window approach for the local regions. If there are M windows totally the overall quality is given by the equation 5.12.

$$Q = \frac{1}{M} \sum_{j=1}^{M} q_j \tag{5.12}$$

5.6 BIT ERROR RATE (BER)

The water mark embedded is a binary image thus it is enough to find the deviation of the bit map from the source water mark and the extracted watermark. The quality of the extracted watermark is examined by BER. The BER represents the total bits that are miss-allocated or deviated from the actual value.

The BER is given by the equation 5.13.

$$BER = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} w_{ij} (XOR)\, \widehat{w}_{ij} \tag{5.13}$$

Where $m \times n$ is the size of the water mark

W is the original water mark image

$\widehat{W}$ is the extracted water mark image

In digital transmission, the number of bit errors is the number of received bits of a data stream over a communication channel that have been altered because of noise, interference, or else distortion or errors in bit synchronization . The **bit error rate** or **bit error ratio** (**BER**) is defined as the number of bit errors divided by the total number of transferred bits during a particular studied time interval. BER can be said as a unitless performance measure, often expressed as a the percentage.

The bit error probability p_e is said to be the expectation value of the BER. The BER can be considered as an approximate estimate of the bit error probability. This estimate is accurate for a long time interval and a high number of bit errors.

As an example, assume this transmitted bit sequence:

0 1 1 0 0 0 1 0 1 1,

and the following received bit sequence:

0 0 1 0 1 0 1 0 0 1,

The number of bit errors (the underlined bits) is in this case 3. The BER is 3 incorrect bits divided by 10 transferred bits, resulting in a BER of 0.3 or 30%.

The packet error rate (PER) is the number of incorrectly received data packets divided by the total number of received packets. A packet is declared incorrect if at least one bit is erroneous. The expectation value of the PER is denoted packet error probability p_p, which for a data packet length of N bits can be expressed as the equation :$\mathbf{p}_{\mathbf{p=1-(1-}}\ \mathbf{p}_{\mathbf{e)}\wedge n}$ assuming that the bit errors are often independent of each other. For small bit error probabilities, this is approximatel Pp≈PeN.Similar measurements can be carried out for the transmission of frames, blocks, or symbols.

Factors affecting the BER

In a communication system, the receiver side of the BER may be affected by transmission channel noise, also interference,also distortion,some bit synchronization problems, some attenuation, and also the wireless multipath fading, and so on. The BER may be improved by choosing a strong signal strength (unless this causes cross-talk and more bit errors), by choosing a slow and very robust modulation scheme or line coding scheme, and by applying channel coding schemes such as redundant forward error correction codes.The transmission BER is the total sum of number of detected bits that which are incorrect before correction of the errors(as expected), and divided by the total number of the transferred bits (including redundant error codes). The information BER, is approximately equal to the decoding probability of error, is the number of decoded bits that remains incorrect after the error correction, divided by the total number of decoded bits (the useful information). Normally the transmission BER is larger than the information BER. The information included BER is affected by strength of the forward error correction code.

5.7 SUMMARY

In this chapter the UQI method to find the quality and the BER to find the error rate of the binary water mark image has been discussed.

CHAPTER 6

ENCODER

6.1 INTRODUCTION

In this chapter the overall block diagram and the encoder process is presented**6.2 OVERALL PROCESSES**

The generalized overall block diagram is given below.

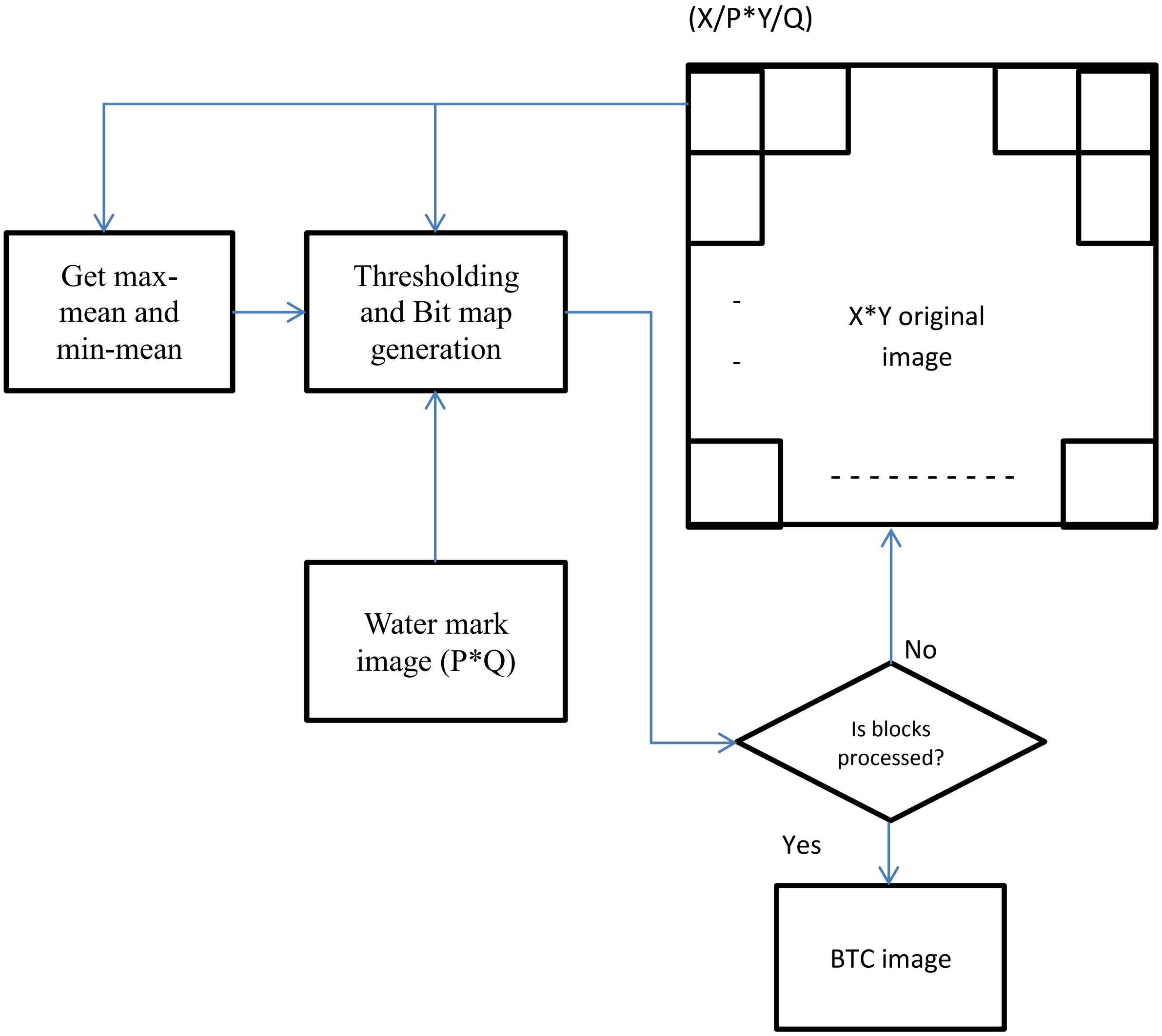
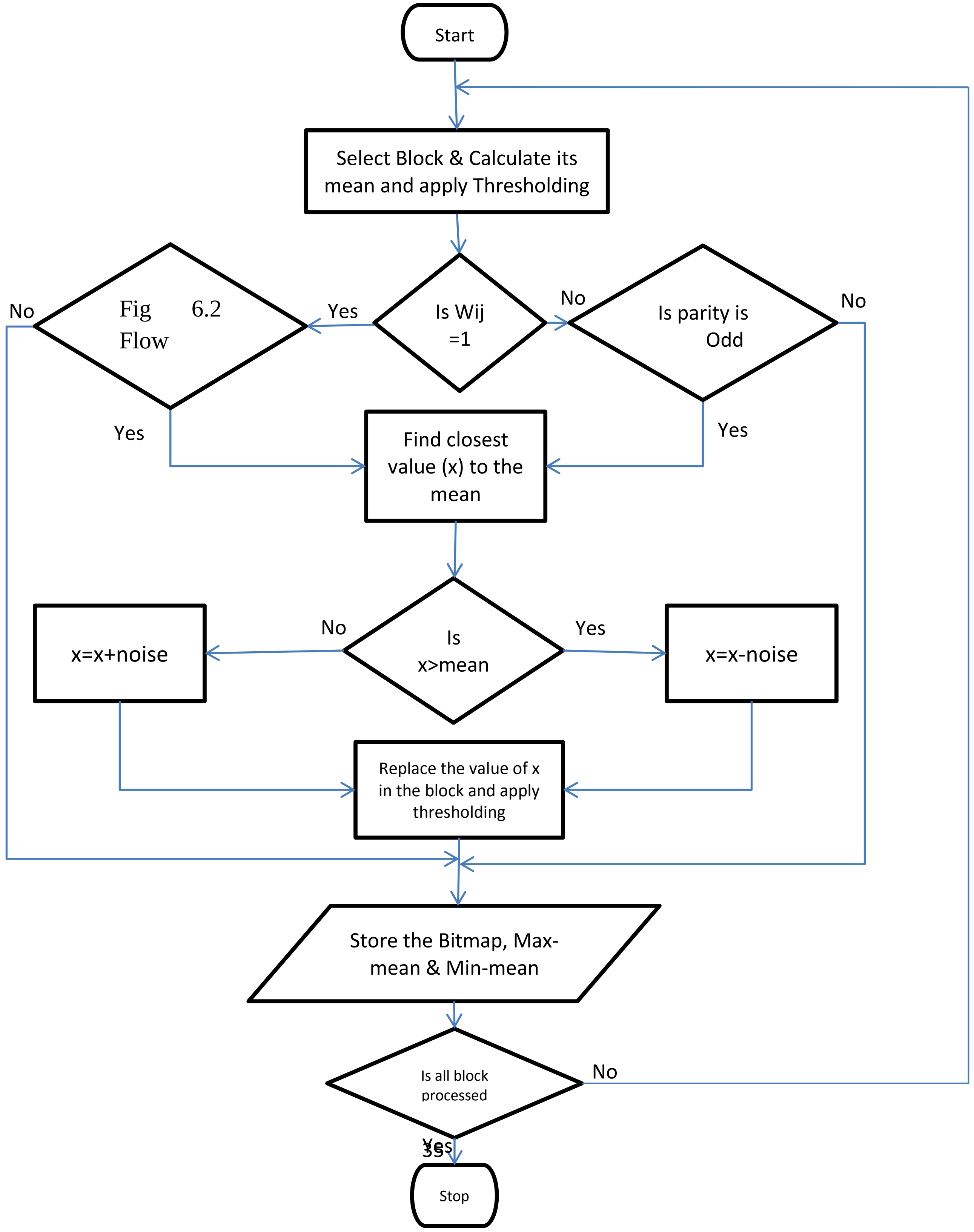


Fig 6.1 Block Diagram of Entire Process

6.3 Encoder

The encoder is the place where the compression takes place and during compression the water mark is added**.** The flow chart of the encoder is given below.


Start
Select Block & Calculate its mean and apply Thresholding
No
Fig 6.2 Flow
Yes
Is Wij =1
No
Is parity is Odd
No
Yes
Find closest value (x) to the mean
Yes
x=x+noise
No
Is x>mean
Yes
x=x-noise
Replace the value of x in the block and apply thresholding
Store the Bitmap, Max-mean & Min-mean
Is all block processed
No
Yes
Stop

The image is first converted from RGB plane to YIQ plane and the encoder process is done for the three planes separately. The BTC based encoding process is as follows.

The Y plane is where the water mark is added the Y plane is segmented into non-overlapping blocks of size say, 4x4 and the process is done for every block in a raster path, which means from left to right and top to bottom. For the selected block the mean is calculated using the formula [10]

$$\bar{x} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} x_{ij} \tag{6.1}$$

Where M, N is the block size and x_{ij} is the corresponding element of the block.

Now thresholding is done to the entire block i.e. those element values which are greater than or equal to $\bar{x}$ is altered to “1” and those less than $\bar{x}$ is changed to “0”, thus a Bit map is generated.

Now

$$v_{ij} = x_{ij+e} \tag{6.2}$$

Where,

$$e = \begin{cases} N, & if\ the\ request\ of\ h_{ij}\ is\ different\ from\ the\ obtained\ parity \\ 0, & otherwise \end{cases}$$

$$N = \begin{cases} -n, if the\ element\ closest\ to\ \bar{x} > \bar{x} \\ +n, if the\ element\ closest\ to\ \bar{x} < \bar{x} \end{cases}$$

Now again the thresholding is done for the modified block values. Thus the actual Bit map is generated. The max-mean and min-mean are calculated using the formula given in equation 6.3, 6.4.

$$max - mean = \frac{1}{n} \sum_{k=1}^{n} l_k \tag{6.3}$$

Where, l_k is the element v_{ij}if $v_{ij} \geq \bar{x}$, n is the number of elements.

$$min - mean = \frac{1}{n} \sum_{k=1}^{n} l_k \tag{6.4}$$

Where, l_k is the element v_{ij} if$v_{ij} < \overline{x},$ n is the number of elements.

Similarly I and Q planes are encoded without inserting the water mark i.e. during initial thresholding itself the values is stored.

6.3.1Example

Let us consider a block of 4x4 with the values

161	160	161	159
162	163	162	162
163	160	162	161
164	161	160	161

The mean=161.375, the max-mean=162.5 and the min-mean=160.6667.

Thus after applying threshold the block becomes

0	0	0	0
1	1	1	1
1	0	1	0
1	0	0	0

Now assume that the water mark bit to be added is ‘0’ and the parity of the block acquired is odd. Since the parity is need to be changed the value closest to the mean is found which is 161, since it is less than mean an additive noise say 1 is added to the value thus the block value is altered to

162	160	161	159
162	163	162	162
163	160	162	161
164	161	160	161

Again thresholding is done with the same mean thus the bit map generated becomes as

1	0	0	0
1	1	1	1
1	0	1	0
1	0	0	0

Thus the parity is changed and a bit is secretly hidden in the block.

6.4 SUMMARY

In this chapter a detailed description of the entire encoder is given. The image is converted from RGB plane to YIQ plane. Then encoding is done, the output of the encoder is of the form a binary bit map and two values representing the values of the block. These outputs are transmitted.

CHAPTER 7

DECODER AND WATERMARK EXTRACTION

7.1 INTRODUCTION

In this chapter deals with the detailed processing of the receiver section that is the decoding process and the watermark extraction from the uncompressed or the decoded image.

7.2 Decoder

In the decoder end the features of the image are reconstructed to retrieve the image. The decoding or the decompression is very simple process. The Block size, Bit map, max-mean, min-mean values are obtained in the transmitter end the binary map or the bit map of every block is selected and the ones are replaced by the max-mean value and the zeros are replaced by the min-mean values of the corresponding block. This process is repeated until all blocks are completed.

The equation is given by the equation 7.1.

$$y_{ij} = \begin{cases} max - mean, \ if \ \ h_{ij} = 1 \\ min - mean, \ if \ \ h_{ij} = 0 \end{cases} \tag{7.1}$$

The process is repeated for I and Q planes. Now the YIQ plane is converted to RGB plane and the image is ready to display.The detailed flow chart of the image reconstruction i.e. decoding is show below:

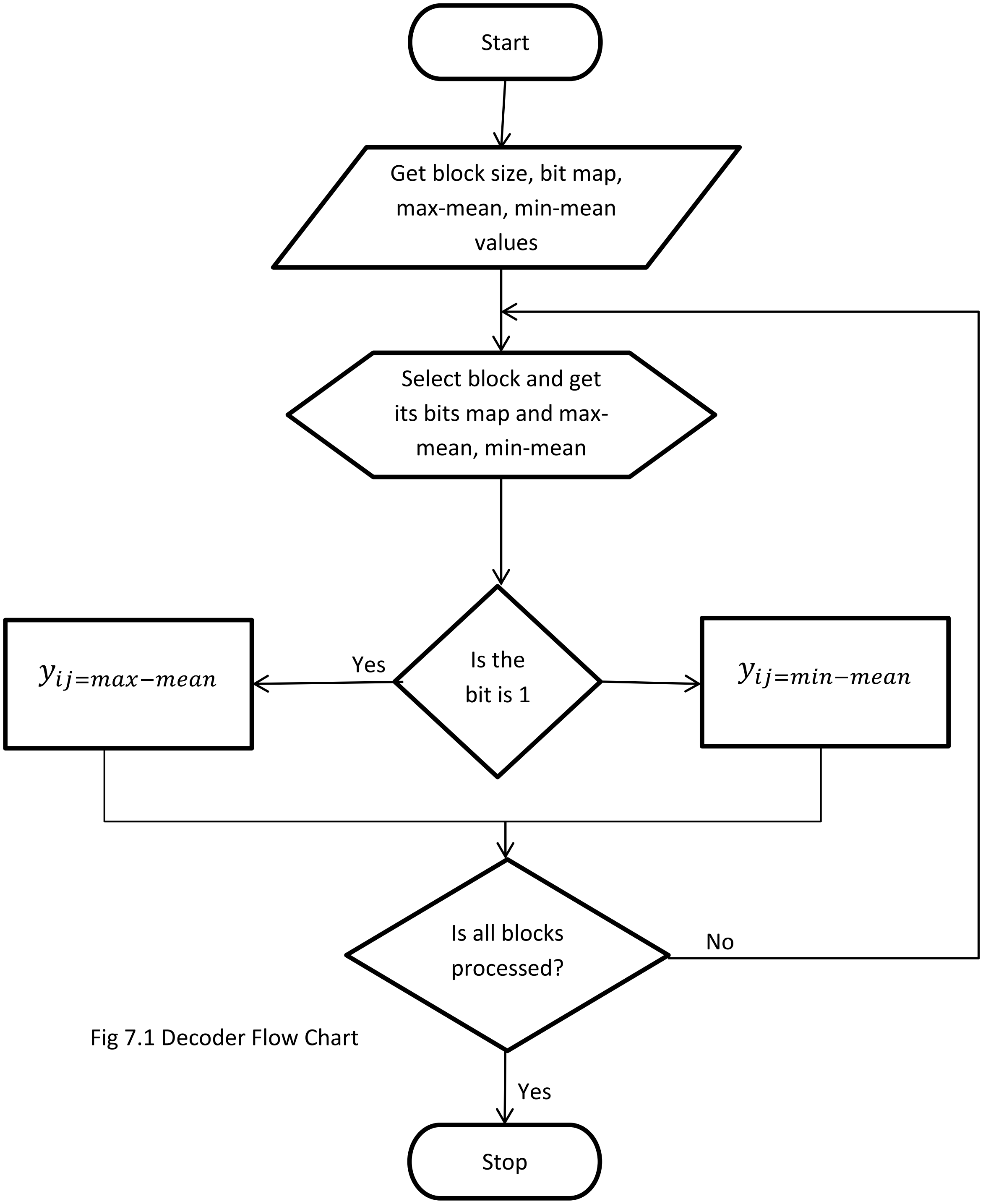

Start
Get block size, bit map, max-mean, min-mean values
Select block and get its bits map and max-mean, min-mean
Is the bit is 1
Yes
$y_{ij=max-mean}$
$y_{ij=min-mean}$
Is all blocks processed?
No
Yes
Stop

Fig 7.1 Decoder Flow Chart

7.3 WATER MARK EXTRACTION

The image is first converted from RGB plane to YIQ plane and the water mark extraction is done for the Y plane since the water mark is embedded in the Y plane only. The water mark extraction is as follows:The Y plane is segmented into non-overlapping

blocks of same size of that of encoding and the process is done for every block in a raster path. For the selected block the mean is calculated using the formula given in equation 7.2.$\bar{y} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} y_{ij}$ (7.2)

Where M, N is the block size and y_{ij} is the corresponding element of the block.Now, thresholding is done to the entire block i.e.those element values which are greater than or equal to $\bar{y}$ is altered to “1” and those less than $\bar{x}$ is changed to “0”, thus a Bit map is generated. From the bit map the water mark information is retrieved. The parity of every block is calculated if the parity is even the bit corresponding to the block is marked as 1 or else it is marked as 0.The detailed flow chart of watermark extraction from the reconstructed image-.

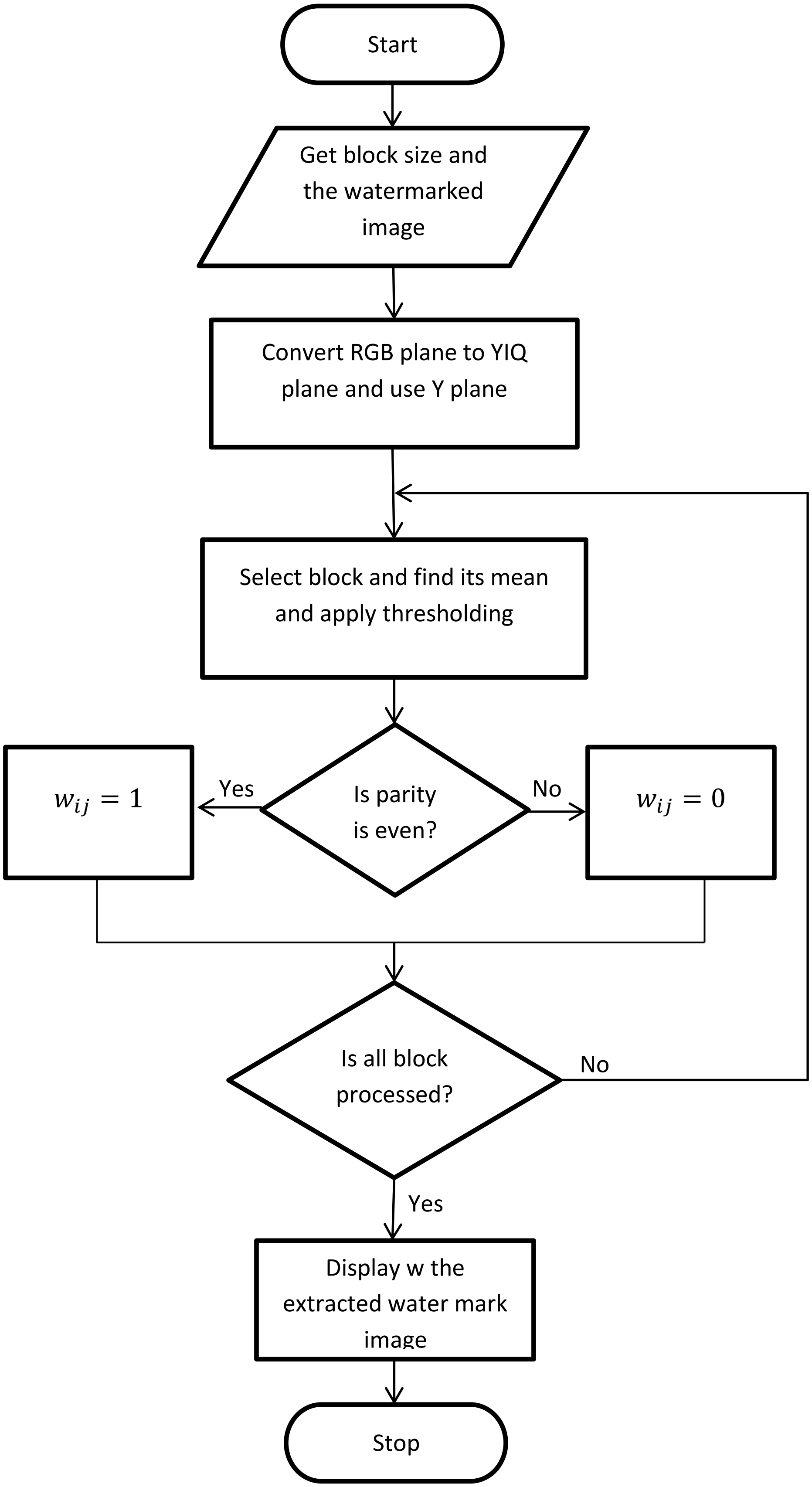

Start
Get block size and the watermarked image
Convert RGB plane to YIQ plane and use Y plane
Select block and find its mean and apply thresholding
Is parity is even?
Yes
No
$w_{ij} = 1$
$w_{ij} = 0$
Is all block processed?
No
Yes
Display w the extracted water mark image
Stop

Fig 7.2 Flow Chart of Watermark Extraction

7.4 SUMMARY

In this chapter detailed process of decoding and water mark extraction has been explained.

CHAPTER 8

RESULTS AND DISCUSSION

8.1 INTRODUCTION

In this chapter different attacks and the result obtained are discussed.

8.2 ATTACKS

Attacks are those which are done to the watermarked image to destroy the watermark either purposely or unknowingly while compression or image enhancement.

Attacks on a signal can vary, but they are normally categorized into two sets: inadvertent and intentional. The set of inadvertent attacks (or modifications) are those that normally occur to images and do not allow us to assume that the attacker has any idea that a watermark is present or is making a conscious attempt to remove it. Common inadvertent attacks include JPEG compression, linear and non-linear filtering, contrast enhancement, and cropping. Intentional attacks are modifications that a normal user would probably not perform on an image or signal and it can be assumed that the attacker is actively trying to remove the watermark. Some examples of intentional attacks include add noise, printing and rescanning or adding additional watermarks.

8.2.1 NECESSITY OF ATTACKS:

Attacks are done to check the robustness of the watermark. Thus to develop better methods of watermarking attacks are necessary.

The attacks which are tested includes

- JPEG compression
- Brightness or intensity adjustment

- Contrast adjustment
- Crop
- Hue adjustment
- Saturation adjustment
- Gray scale conversion
- Exposure adjustment

8.3 RESULTS AND DISCUSSION

8.3.1Parameters

Two different parameters are involved in the process the noise increment and the block size. These parameters are tested for various test images and the characteristics are plotted. The host image is of size 512x512 and the water mark size depends on the block size.The figure 8.1 shows the graph plotted between the Bit Error Rate and the Noise increment for the Lena color image of size 512x512 and the block size of 4x4 and the water mark of size 128x128. The graph shows that at Ni=0, the error rate is making since no watermark is added. As the Ni is increased to 1 the BER reduces less than 0.1 and as the Ni increases more and more the BER reduces to almost zero.

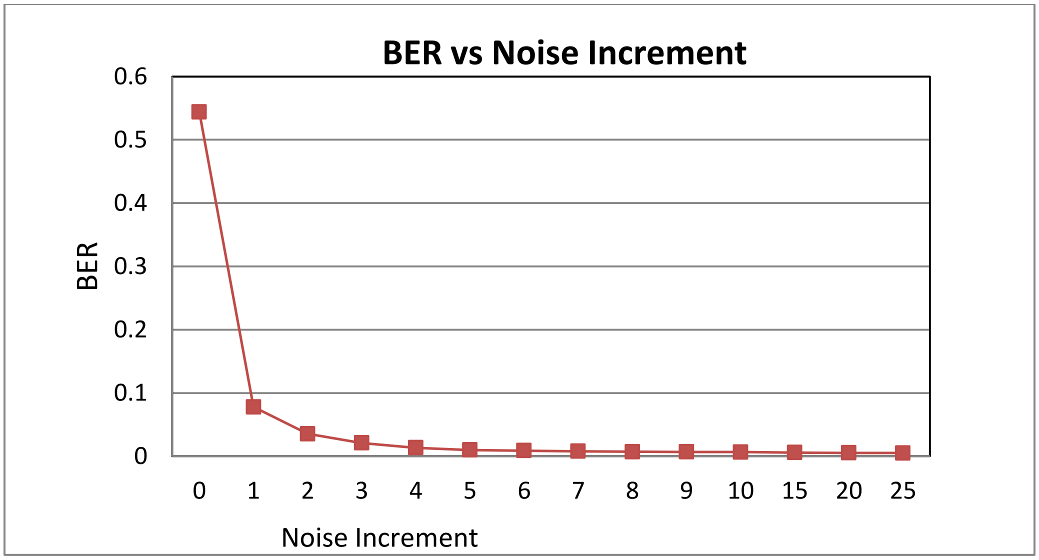


Fig 8.1 BER vs. Noise Increment

The figure 8.2 shows the graph plotted between the Universal quality index and the Noise increment for the Lena color image of size 512x512 and the block size of 4x4 and the water mark of size 128x128. As the noise increases the value of the quality index reduces and remains constant after the noise level reaches 3. Thus noise increment after certain level does not affect the quality of the image.

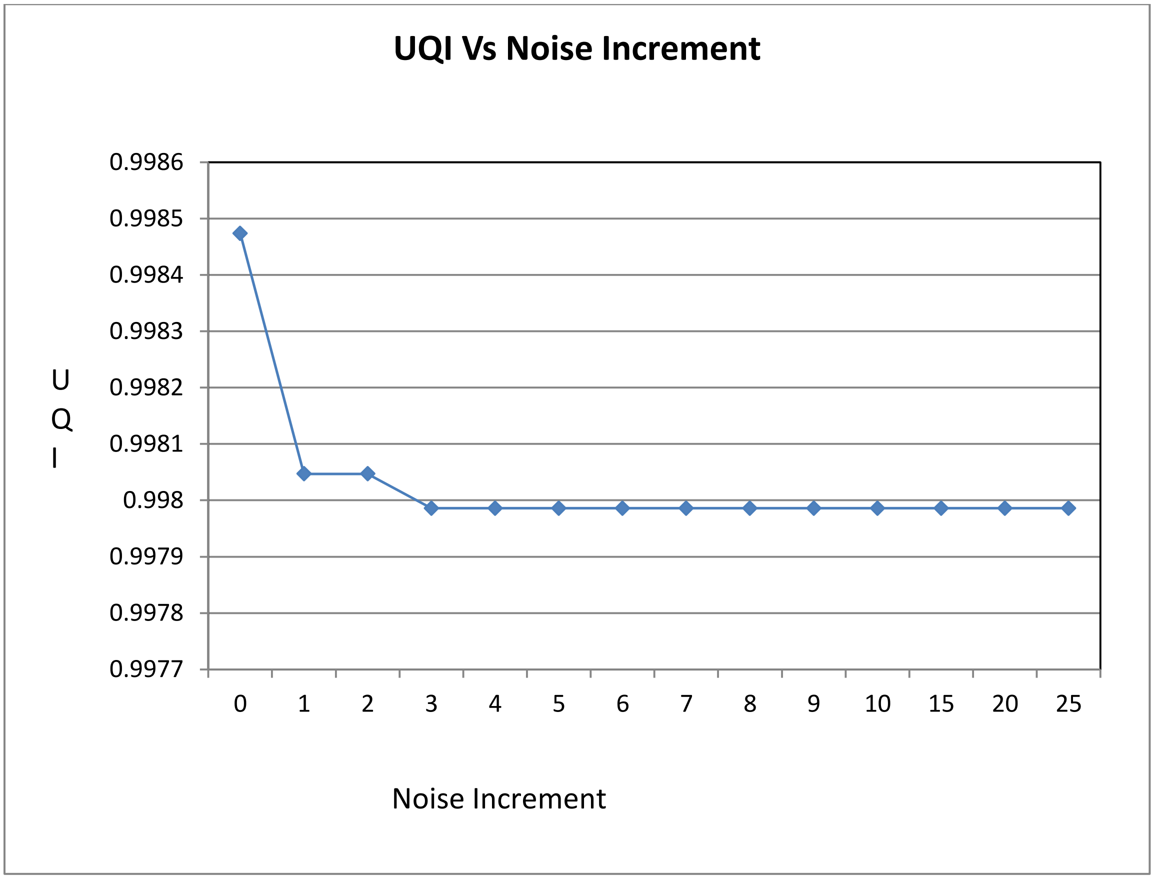


Fig 8.2 UQI vs. Noise Increment

Ni	0	1	2	3	4	5	6	7	8	9	10	15	20	25
BER	0.5439	0.0780	0.0355	0.0209	0.0135	0.0099	0.0089	0.0079	0.0070	0.0068	0.0065	0.0059	0.0054	0.0051
UQI	0.9985	0.9980	0.9980	0.9980	0.9980	0.9980	0.9980	0.9980	0.9980	0.9980	0.9980	0.9980	0.9980	0.9980

Table 8.1 Ni vs. BER and UQI

The figure 8.3 shows the graph plotted between the Bit Error Rate and the Block size for the Lena color image of size 512x512 and the noise increment of 4. As the block size increases the BER reduces.

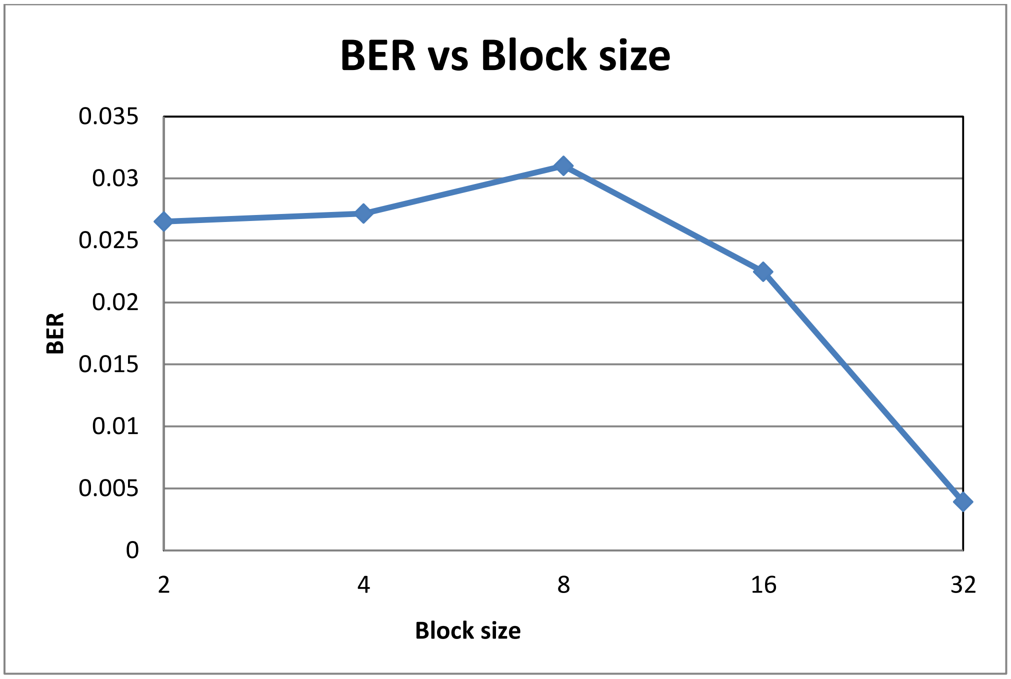


Fig 8.3 BER vs. Block size

Block Size	BER
2	0.02652
4	0.027161
8	0.031006
16	0.022461
32	0.003906

Table 8.2 Block Size vs. BER

The figure 8.4 shows the graph plotted between the Universal quality index and the Block size for the four different color image (Baboon, Lena, Peppers, Flight) of size 512x512 and the noise increment of 4. As the block size increases the UQI reduces but the BER decreases as the block size increases. Thus there exists a compromise between them.

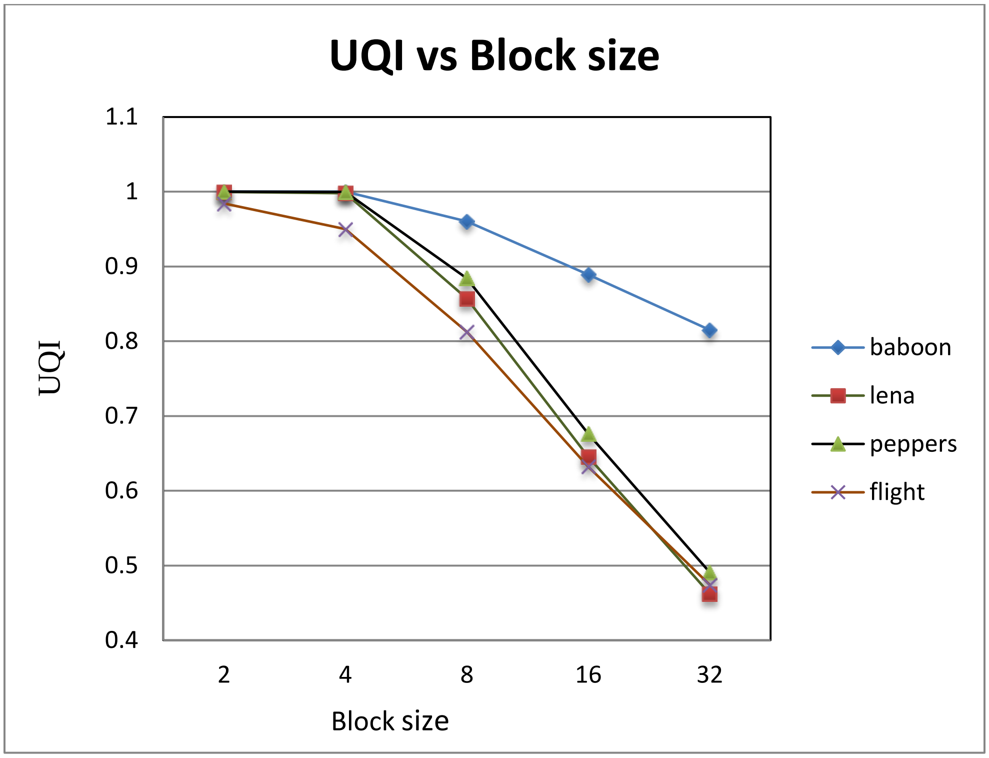
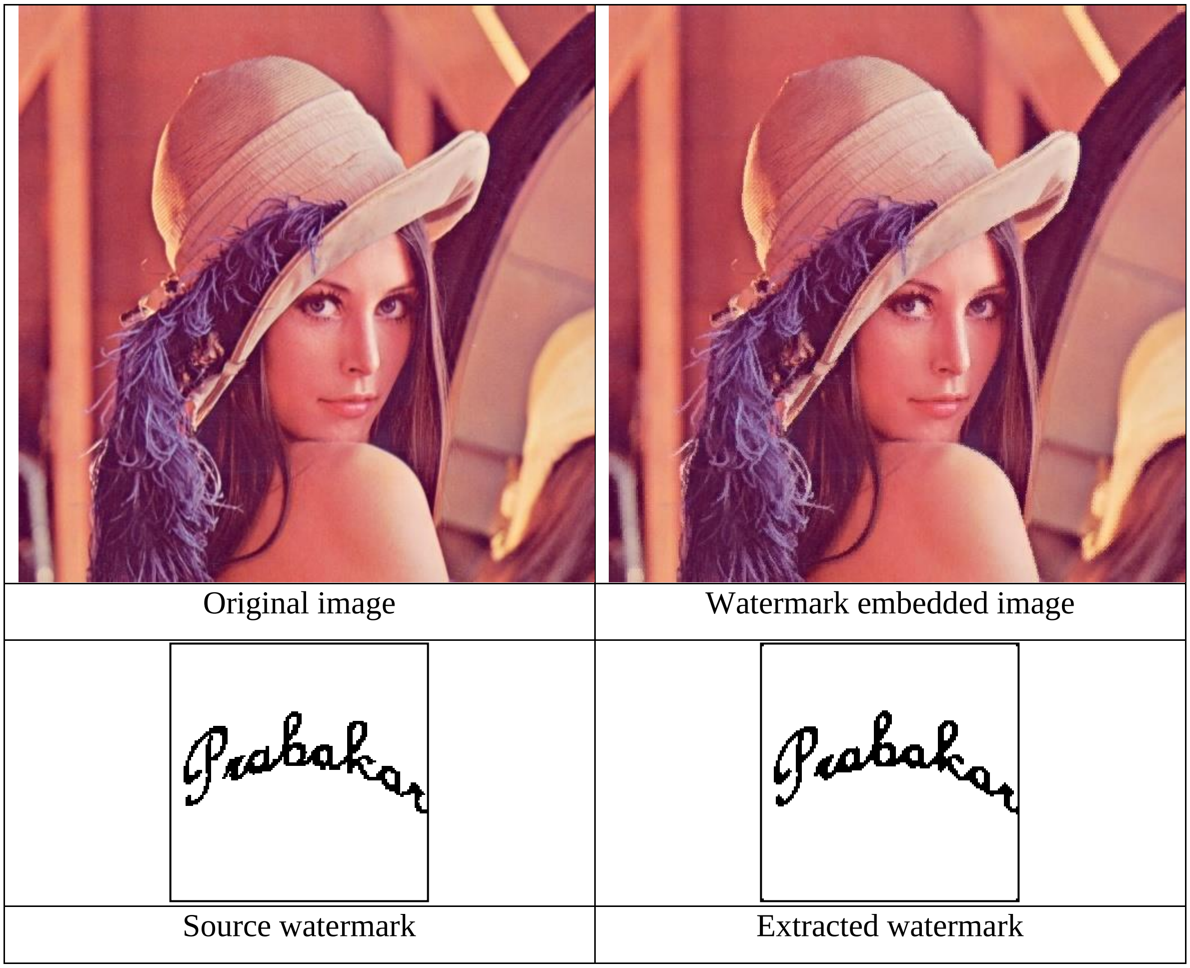


Figure 8.4 UQI vs. Block Size

Block size	Baboon	Lena	Peppers	Flight
2	1	0.999573	0.999939	0.984192
4	1	0.997986	0.999573	0.94989
8	0.960022	0.857117	0.884155	0.812317
16	0.889099	0.645325	0.676453	0.632263
32	0.81488	0.462036	0.490662	0.47406

Table 8.3 UQI vs. Block Size

The figure 8.5 shows the input cover image and the source watermark image and the watermark embedded image and the extracted watermark image with block size of 4x4 and the cover image of size 512x52. And the Ni value is kept as 4.



Original image

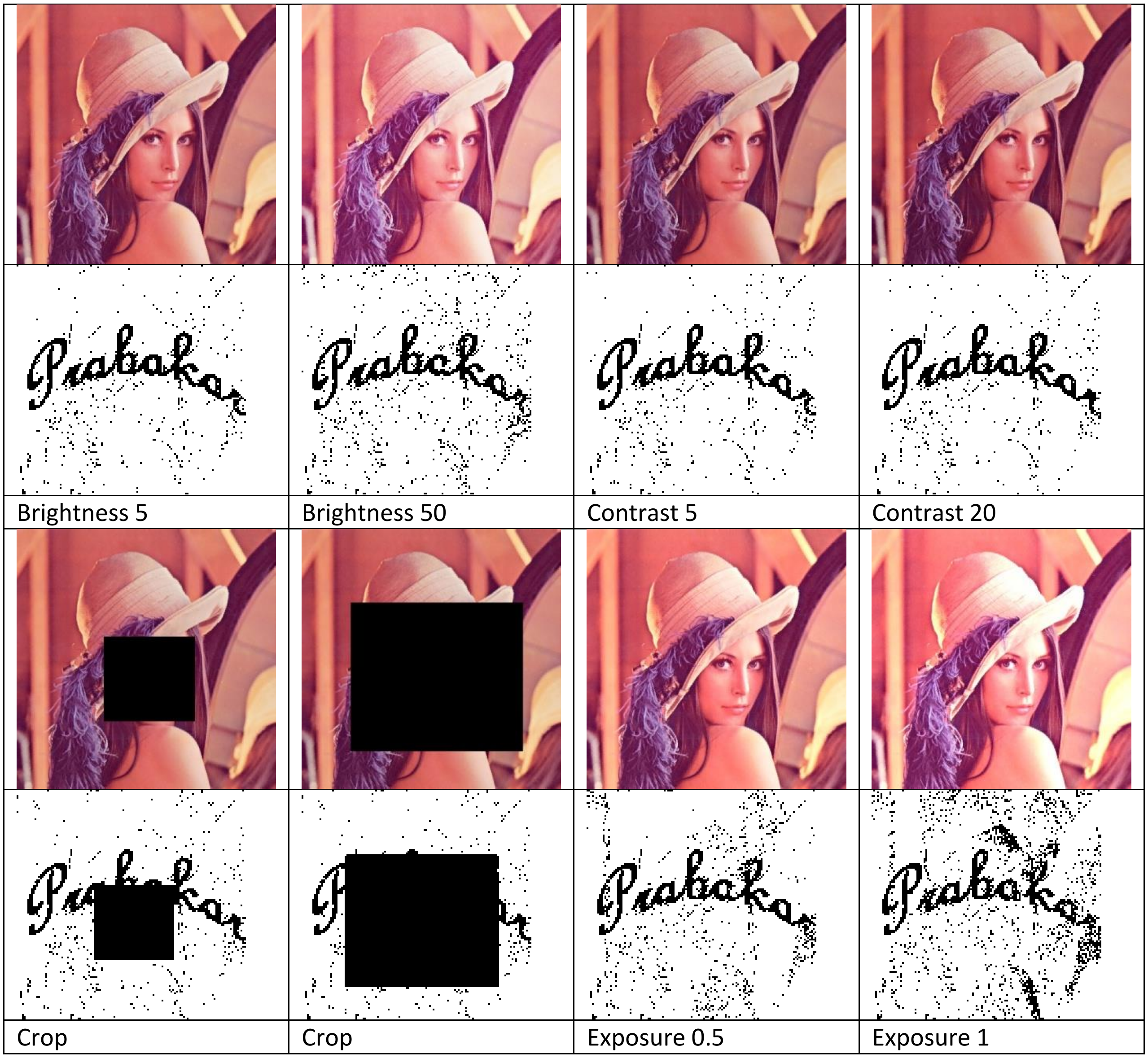
Watermark embedded image

Source watermark

Extracted watermark

Figure 8.5 Source and Output Images

The figure 8.6 and 8.7 shows the image which is gone through different attacks and the watermark extracted from the attacked image.



Brightness 5

Brightness 50

Contrast 5

Contrast 20

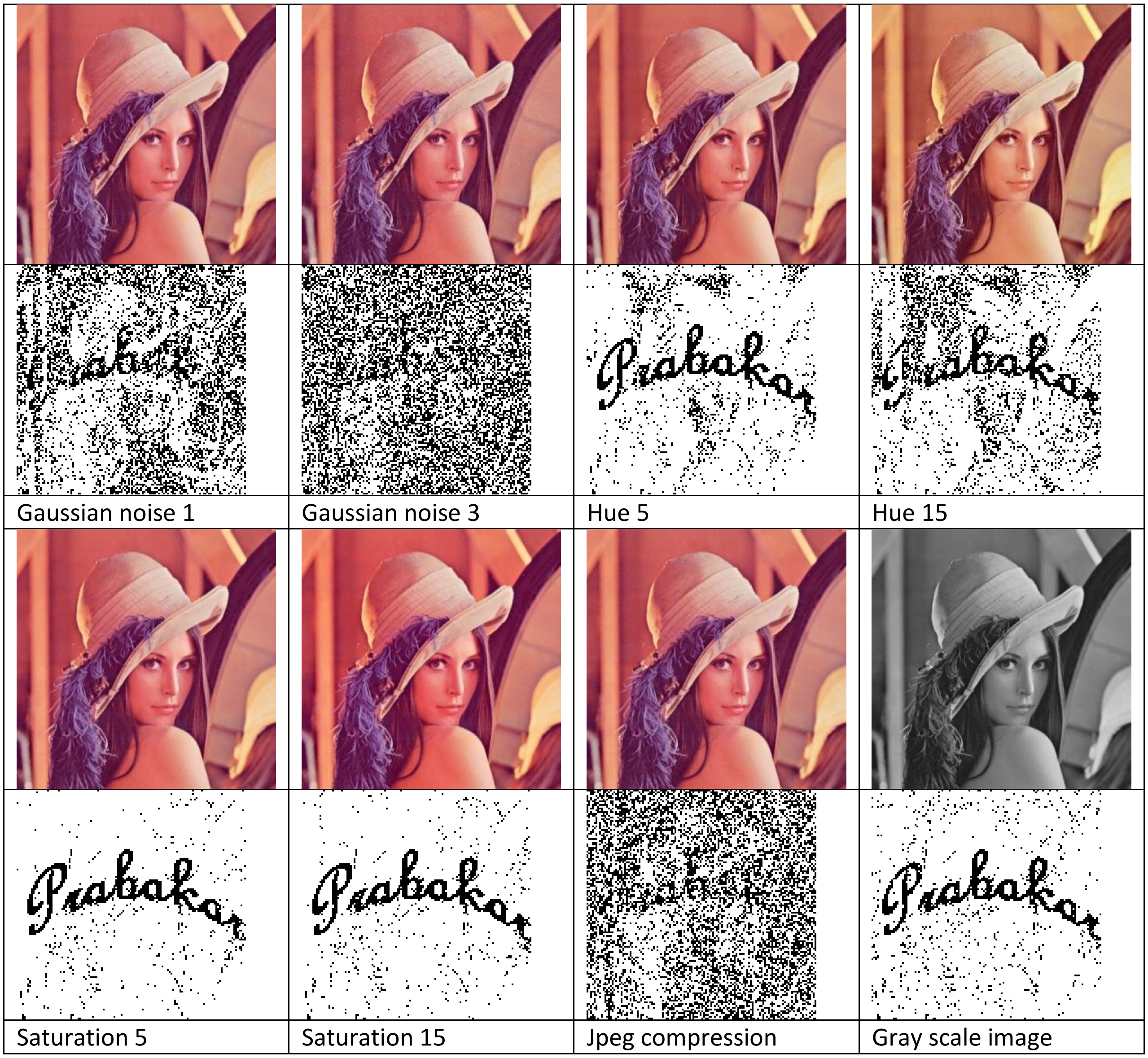
Crop

Crop

Exposure 0.5

Exposure 1

Figure 8.6 Attacked Image and Extracted Watermark (a)



Gaussian noise 1 | Gaussian noise 3 | Hue 5 | Hue 15

Saturation 5 | Saturation 15 | Jpeg compression | Gray scale image

Figure 8.7 Attacked Image and Extracted Watermark (b)

The different attacks that the image has undergone are

Brightness adjustment: the brightness or the light intensity of the image is been modified to two values 5 and 50 i.e. the brightness values are increased by 5 and 20 respectively. From the extracted watermark it is clear that the water mark with stands brightness based attack.

Contrast adjustment: the contrast of the image is been modified to two values 5 and 20 i.e. the contrast values are increased by 5 and 20 respectively. From the extracted watermark it is clear that the water mark with stands contrast based attack.

Cropping: cropping is done to the image so, that some of the image region is discarded. Since the watermark is spread over the entire cover image the bits corresponding to cropped region are lost whereas, the extracted watermark shows clearly that the water mark is present.

Exposure: exposure is very much similar to brightness adjustment it increases the overall lightness present in the image. The water mark extracted from exposure level of 0.5 and 1 says that the watermark is robust to exposure alteration.

Gaussian noise: the image is attacked using Gaussian noise of factor 1 and 3. From the extracted water mark we can clearly say that as the Gaussian noise level increases the quality of the water mark becomes poorer and at 3 the water mark is quite invisible so, the water mark is influenced by Gaussian attack.

Hue: hue attack refers to the adjustment of the color of the image. In this the hue manipulated using two values of 5 and 15. The extracted water shows that the image is robust to hue type attacks.

Saturation: saturation refers to the maximum level the color pixels represent. The saturation is increased by 5 and 15. And it is clear that the water mark sustains this attack.

JPEG compression: the watermarked image is compressed using jpeg compression and the water mark is extracted from the compressed image. From the extracted water mark it is clear that only some traces of water mark is visualized and the image is vulnerable to jpeg compression.

Gray scale: for some applications the image may be converted to gray scale thus the watermarked image is converted to gray scale and water mark is extracted from the gray scale image thus it is clear that the water mark is robust.

From these results we can see that though some traces of watermark are available from jpeg compression and Gaussian noise the water mark is vulnerable. But in all other cases the water mark is robust to attacks.

All the attacks mentioned above are carried out using Photoshop CS5 on the decoded image.

8.4 SUMMARY

In this chapter the different attacks that could affect the image are discussed and the result of the test image is shown and the extracted water mark of the attacked images are shown.

CHAPTER 9

CONCLUSION AND FUTURE ENHANCEMENT

9.1 CONCLUSION

Nowadays, most images are compressed before they are transmitted or stored, and, thus, watermarking is highly suggested to be catered into compressed domain of an image. In this watermarking technique using block truncation coding (BTC) for color images improves the coding efficiency by not preserving the moments of the block Two parameters, block size and noise increment, are employed The Block size controls the quality of an embedded image, decoded watermark, and processing efficiency; the amount of noise increment provides the tradeoff between embedded image quality and decoded watermark quality.

9.2 FUTURE ENHANCEMENT

This method embeds the watermark only into Y component of image. However, it is possible to extend the scheme by watermarking chromatic components also. Such an approach will improve the robustness, while not losing from imperceptibility due to low sensitivity of chromatic components. If watermark is embedded in all the three planes then there is possibility of multiple watermarking which will naturally improve the robustness of the watermark.

REFERENCE

[1] E. J. Delp and O. R. Mitchell, ”Image compression using block truncation coding”, IEEE Trans. Commun., vol. 27, no. 9, pp. 1335–1342, Sep1979.

[2] D. R. Halverson, N. C. Griswold, and G. L. Wise, ‘A generalized block truncation coding algorithm for image compression’, IEEE Trans. Acoust., Speech, Signal Process., vol. ASSP–32, no. 3, pp.664–668,Jun 1984.

[3] Zhou Wang and Bovik, A.C,’ A universal image quality index’, IEEE Signal Processing letters’, vol.9, pp.81 – 84, 2002.

[4] S. F. Tu and C. S. Hsu, “A BTC-based watermarking scheme for digital images,” Int. J. Inf. Security, vol. 15, no. 2, pp. 216–228, 2004.

[5] M. H. Lin and C. C. Chang, “A novel information hiding scheme based on BTC,” in Proc. Int. Conf. Computer and Information Technology, vol. 14–16, pp.66–71, 2004.

[6] D.J. Granrath. “ The role of human visual models in image processing”, IEEE transactions on image processing, Vol. 69, No. 5, pp. 552 – 561, 2005.

[7] S. J. lee and S. H. Jung, ‘A Survey of Watermarking Techniques Applied toMultimedia’, Proc. IEEE Int. Symp. on Industrial Electronics, June 2001.

[8] Y.Yusof and O. O. Khalifa,’ Digital Watermarking For Digital Images Using Wavelet Transform’, Proc. IEEE Int. Conf. on Telecommunications, May 2007.

[9] R. B. Wolfgang and E. J. Delp, “A Watermark for Digital Images”, Proc. IEEE Int.Conf.onImage Processing, , pp. 219–222, 1996.

[10] Jing-Ming Guo and Yun-Fu Liu,”Joint Compression/Watermarking Scheme Using Majority-Parity Guidance and HalftoningBased Block Truncation Coding” IEEE Transactions On Image Processing, Vol.19, NO8, pp.2056- 2069, Aug 2010.

[11] Joint wavelet compression and authentication watermarking

Liehua Xie ; Dept. of Electr. & Comput. Eng., Delaware Univ., Newark, DE, USA Arce,G.R

[12] Improved Block Truncation Coding using Optimized Dot Diffusion
Guo, J.-M. ; Dept. of Electr. Eng., Nat. Taiwan Univ. of Sci. & Technol., Taipei, Taiwan ;
Liu, Y.-F.

[13] Majority-Parity-Guided Watermarking for Block-Truncated Images
; Dept. of Electr. Eng., Nat. Taiwan Univ. of Sci. & Technol., Taipei, Taiwan ; Liu, Y.-

[14] Texture orientation modulation for halftoning watermarking
Dept. of Electr. Eng., Nat. Taiwan Univ. of Sci. & Technol., Taipei, Taiwan ; Su, C.-C. ;
Liu, Y.-F.

[15] Continuous-tone Watermark Hiding in Halftone Images
Dept. of Electr. Eng., Nat. Taiwan Univ. of Sci. & Technol., Taipei, Taiwan ;

[16] Hidden digital watermarks in images CT Hsu, JL Wu - Image Processing, IEEE Transactions on, 1999 - ieeexplore.ieee.org

[17] Oriented Modulation for Watermarking in Direct Binary Search Halftone Images
JM Guo, CC Su, YF Liu, H Lee… - Image Processing, IEEE …, 2012 - ieeexplore.ieee.org

[18] High capacity data hiding scheme in BTC domain combining visual perception
H Yang, G Sun - Jisuanji Gongcheng yu …, 2011 - … Technology Institute,.

[19] Visual data hiding in dot diffusion images X Wu, W Sun - … (ICCIT), 2010 5th International Conference on, 2010 - ieeexplore.ieee.org

[20] Multitone block truncation coding Y Wan, Y Yang, QQ Chen - Electronics letters, 2010 - ieeexplore.ieee.org.

[21] Complementary steganography in error-diffused block truncation coding images
JM Guo - Intelligent Information Hiding and Multimedia Signal …, 2007
ieeexplore.ieee.org

[22] High Capacity Data Hiding for Error-Diffused Block Truncation Coding
J Guo, Y Liu - 2012 - ieeexplore.ieee.org

[23] Based upon RBTC and LSB substitution to hide data CY Yang - … Computing, Information and Control, 2006. ICICIC' …, 2006 - ieeexplore.ieee.org

[24] Parallel and element-reduced error-diffused block truncation coding
JM Guo, CY Lin - Communications, IEEE Transactions on, 2010 - ieeexplore.ieee.org

[25]Alteration detection and image recovery using Halftone Replacement Prior Watermark Embedding JM Guo, T Kao, YF Liu, JT Wang - Machine Learning and …, 2010 - ieeexplore.ieee.org

[26] Reversible data hiding in highly efficient compression scheme JM Guo, JJ Tsai - … and Signal Processing, 2009. ICASSP 2009. …, 2009 - ieeexplore.ieee.org

[27] Lossless data hiding for color images based on block truncation coding CC Chang, CY Lin, YH Fan - Pattern Recognition, 2008 – Elsevier

[28] Quality compressed steganography using hidden referenced halftoning JM Guo, JH Chen - Multimedia, 2007. ISM 2007. Ninth IEEE …, 2007 - ieeexplore.ieee.org

[29] Halftone-Image Security Improving Using Overall Minimal-Error Searching
JM Guo, YF Liu - Image Processing, IEEE Transactions on, 2011 - ieeexplore.ieee.org

[30] Watermarking in halftone images with noise balance strategy
JM Guo, SC Pei, H Lee - International Journal of Imaging …, 2010 - Wiley Online Library

Websites refered are:

www.mit.edu.

www.wikipedia.org

www.ieee.org

www.google.com