Watermarking of Digital Images

A Project Report

Submitted in Partial Fulfillment of the

Requirement for the degree of

Master of Engineering

in

System Science and Automation

by

Saraju Prasad Mohanty

Department of Electrical Engineering

INDIAN INSTITUE OF SCIENCE

BANGALORE-560 012, INDIA

JANUARY, 1999

A Note to All Readers

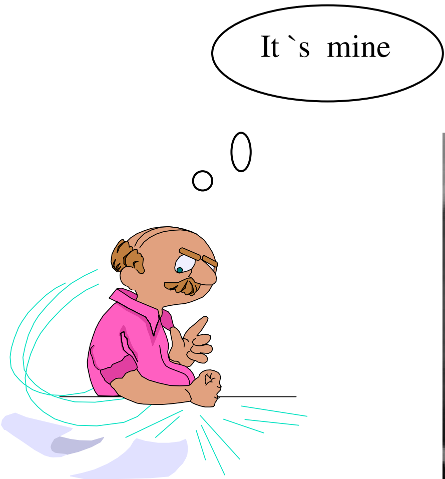
This is not an original electronic copy of the master's thesis, but a reproduced version of the authentic hardcopy of the thesis. I lost the original electronic copy during transit from India to USA in December 1999. I could get hold of some of the older version of the files and figures. Some of the missing figures have been scanned from the photocopy version of the hardcopy of the thesis. The scanned figures have been earmarked with an asterisk.

Saraju P Mohanty
06 Dec 2003

Acknowledgement

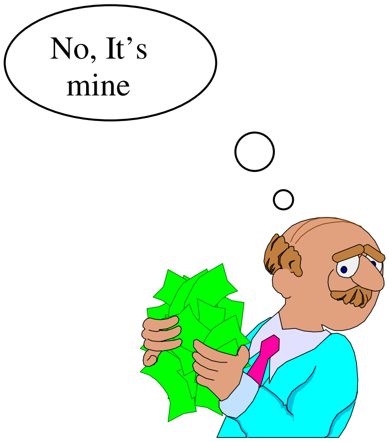
I would like to profusely thank my guide Prof. K. R. Ramakrishnan for is timely advice and encouragement throughout my project work. I would also like to acknowledge Prof. M. Kankanhalli for reviewing my work from time to time. A special note of gratitude goes to Dr. S. H. Srinivas for the support he extended to this work. I would also like to thank all who helped me during my project work.

Saraju Prasad Mohanty

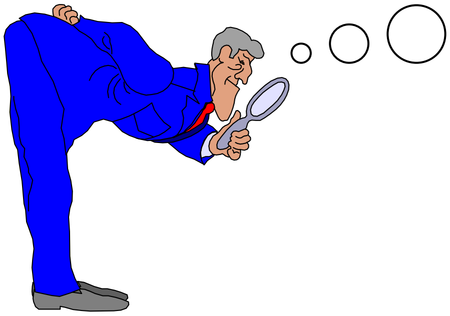


HACKER

IMAGE

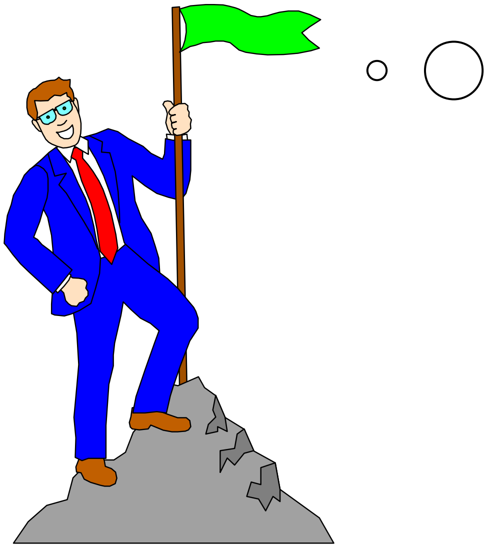


OWNER



- Whose image is it ?
- How to know ?
- What's the solution of this ownership problem?

MULTIMEDIA RESEARCHER



THE SOLUTION IS:

" WATERMARKING"

SARAJU PRASAD MOHANTY
ME(SSA)

CONTENTS

Abstract

Watermarking is the process of embedding data called a watermark (also known as Digital Signature or Tag or Label) into a multimedia object such that watermark can be detected or extracted later to make an assertion about the object. The object may be an audio, image or video. A simple example of digital watermark would be a visible "seal" placed over an image to identify the copyright. However the watermark might contain additional information including the identity of the purchaser of a particular copy of the object. Based on the purpose of the watermark, it is embedded either visibly or invisibly.

In this work we have start with the type of watermarks and their characteristics. We have done an extensive survey of current watermarking literatures. Four different types of watermarking algorithms are proposed. Two of them are in spatial domain and two are in DCT domain. Further in each of the categories mentioned above, we have one visible and one invisible watermark. The four algorithms appear under the following headings in this thesis.

- An Adaptive Visible Watermarking Technique for Image Data.
- An Adaptive Visible Watermarking for Image Data in DCT Domain.
- An Invisible Image Watermarking Technique in Spatial Domain.
- A Spread Spectrum Watermarking Technique for Digital Images.

The thesis concludes with a discussion of the advantages and disadvantages of the techniques proposed and the future directions of research.

CHAPTER # 1

INTRODUCTION

1.1 History of Data Hiding
1.2 Introduction to Digital Watermarking
1.3 General Framework for Digital Watermarking
1.4 Types of Digital Watermarking
1.5 Applications of Digital Watermarks
1.6 Attacks on Watermarks
1.7 Desired Characteristics of Watermarks
1.8 Contributions and organization of the report

The growth of high speed computer networks and that of **Internet**, in particular, has explored means of new business, scientific, entertainment, and social opportunities in the form of electronic publishing and advertising, real-time information delivery, product ordering, transaction processing, digital repositories and libraries, web newspapers and magazines, network video and audio, personal communication, lots more. The new opportunities can be broadly grouped under the label "electronic commerce". The cost effectiveness of selling software, high quality art work in the form of digital images and video sequences by transmission over **World Wide Web** (www) is greatly enhanced consequent to the improvement of technology. Sending hard copies by post may soon be a thing of past.

Though the commercial exploitation of the www is steadily being more appreciated, apprehension on the security aspect of the trade has only funneled the exploitation to be restricted to the transmission of demo and free versions of software and art. Ironically, the cause for the growth is also of the apprehension – **use of digital formatted data**.

Digital media offer several distinct advantages over **analog media**: the quality of digital audio, images and video signals are higher than that of their analog counterparts. Editing is easy because one can access the exact discrete locations that should be changed. Copying is simple with no loss of fidelity. A copy of a digital media is identical to the original.

The ease by which a digital information can be duplicated and distributed has led to the need for effective copyright protection tools. Various software products have been recently introduced in attempt to address these growing concerns. It should be possible to hide data (information) within digital audio, images and video files. The information is hidden in the sense that it is perceptually and statistically undetectable.

One way to protect multimedia data against illegal recording and retransmission is to embed a signal, called **digital signature** or **copyright label** or **watermark**, that completely characterizes the person who applies it and, therefore, marks it as being his intellectual property.

1.1 HISTORY OF DATA HIDING

Two basic methods of information hiding are **cryptography** and **steganography**. The term steganography means "cover writing" and cryptography means "secret writing"**.**

Cryptography is the study of methods of sending messages in distinct form so that only the intended recipients can remove the disguise and read the message. The message we want to send is called the **plain text** and disguised message is called **cipher**

text. The process of converting a plain text to a cipher text is called **enciphering** or **encryption**, and the reverse process is called **deciphering** or **decryption**. Encryption protects contents during the transmission of the data from the sender to receiver. However, after receipt and subsequent decryption, the data is no longer protected and is in the clear. More about the theory of cryptography and some of its applications can be found in [5-11].

In contrast to cryptography, the heart of **steganography** lies in devising astute and undetectable methods of concealing the message themselves. It is therefore broader than cryptography. There is no theory for steganography. The origin of steganography is biological and physiological [30&31].

The earliest allusion to secret writing in the West appears in **Homer**'s **Ilaid** [12]. Steganographic methods made their record debut a few centuries later in several tales by **Herodotus**, the father of history [13]. Some of them can also be found in [14].

Few other examples of steganography can be found in [14]. An important technique was the use of sympathetic inks. **Ovid** in his "**Art of Love**" suggests using milk to write invisibly. Later, chemically affected sympathetic inks were developed. This was used in **World Wars** 1 and 2.

A whole other branch of steganography, **linguistic steganography**, consists of linguistic or language forms of hidden writing. These are the **semagrams** and the **open code** [14].

Ancient references to secret writing and steganography also appear in Asia. **Indian literature** is replete with references as well as explicit formulas for secret writing. **Kautilya**'s **Arthasa'stra** and **LalitaVista'ra**, and **Vatsa'yana**'s **Ka'masu'tra** are few famous examples. In ancient China, military and diplomatic rulers wrote important messages on thin sheets of silk or paper. For secure transport, the sheets were rolled into balls, covered with wax, and swallowed by and placed in the rectum of messenger [15].

Watermarking techniques are particular embodiments of steganography. The use of watermarks is almost as old as paper manufacturing. Our ancients poured their half-stuff slurry of fiber and water on to mesh molds to collect the fiber, then dispersed the slurry within deckle frames to add shape and uniformity, and finally applied great pressure to expel the water and cohere the fiber. This process hasn't changed too much in 2000 years. One by-product of this process is the **watermark** – 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.

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 our concept of watermarking to include immaterial digital impressions for use in authenticating ownership claims and protecting proprietary interests. However, in principle digital watermarks are like their paper ancestors. They signify something about the token of a document or file in which they inherit. Whether the product of paper press or discrete cosine transformations, watermarks of varying degree of visibility are added to presentation media as a guarantee of authenticity, quality ownership and source.

Digital watermarking differs from digital fingerprinting which produces a metafile that describes the contents of the source file [16&17].

1.2 INTRODUCTION TO DIGITAL WATERMARKING

Digital watermarking technology is an emerging field in computer science, cryptography, signal processing and communications. Digital Watermarking is intended by its developers as the solution to the need to provide value added protection on top of data encryption and scrambling for content protection [18].

Like other technology under development, digital watermarking raises a number of essential questions such as follows.

- **What is it?**
- **How can a digital watermark be inserted or detected?**
- **How robust does it need to be?**
- **Why and when are digital watermarks necessary?**
- **What can watermarks achieve or fail to achieve?**
- **How should digital watermarks be used?**
- **How might they be abused?**
- **How can we evaluate the technology?**
- **How useful are they, that is, what can they do for content protection in addition to or in conjunction with current copyright laws or the legal and judicial means used to resolve copyright grievances?**
- **What are the business opportunities?**
- **What roles can digital watermarking play in the content protection infrastructure?**
- **And many more…**

Many of these questions have yet to be answered thoroughly.

1.3 GENERAL FRAMEWORK FOR WATERMARKING

Watermarking is the process that embeds data called a watermark or digital signature or tag or label into a multimedia object such that watermark can be **detected** or **extracted** later to make an assertion about the object. The object may be an **image** or **audio** or **video**.

A simple example of a digital watermark would be a visible "seal" placed over an image to identify the copyright. However the watermark might contain additional information including the identity of the purchaser of a particular copy of the material.

In general, any watermarking scheme (algorithm) consists of three parts: [19]

- **The watermark**
- **The encoder** (marking insertion algorithm)
- **The decoder and comparator** (verification or extraction or detection algorithm)

Each owner has a unique watermark or an owner can also put different watermarks in different objects the marking algorithm incorporates the watermark into the object. The verification algorithm authenticates the object determining both the owner and the integrity of the object.

ENCODING PROCESS: The Fig. 1.1 illustrates the encoding process.

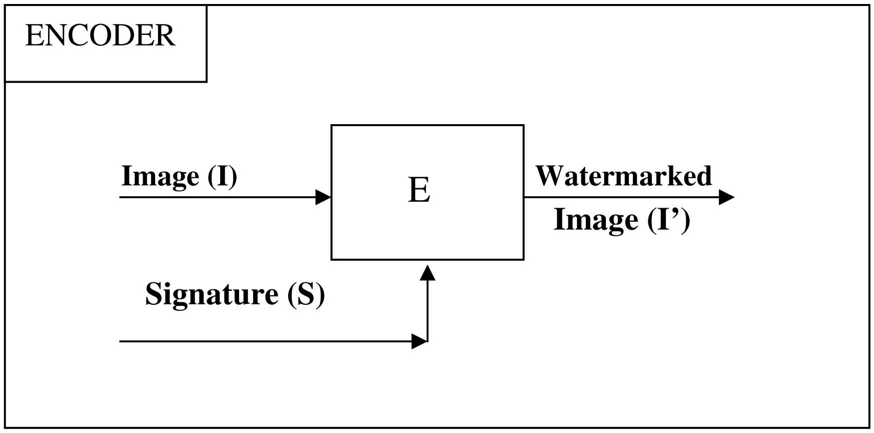


Fig. 1.1 Encoder

Let us denote an image by I, a signature by S = { s_1, s_2, … } the watermarked image by I'. E is an encoder function, it takes an image I and a signature S, and it generates a new image which is called watermarked image I', i.e.

$$E\,(I, S) = I' \qquad (1.1)$$

It should be noted that the signature S may be dependent on image I. In such cases, the encoding process described by (1.1) still holds.

DECODING PROCESS: The fig 1.2 illustrates the decoding process.

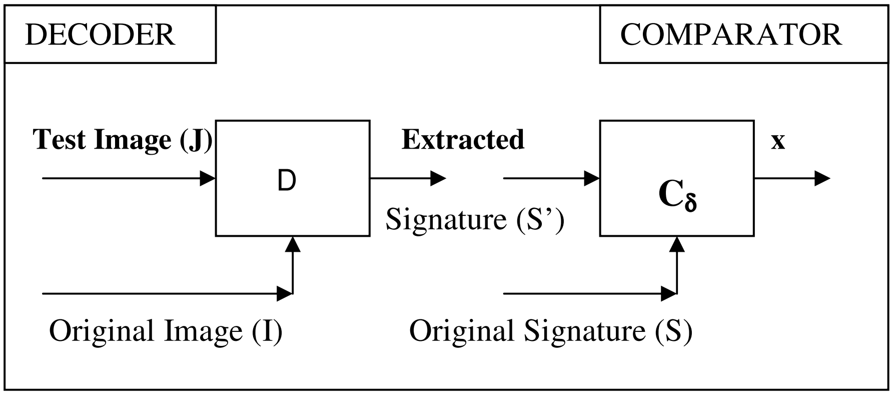


Fig. 1.2 Decoder

A decoder function D takes an image J (J can be a watermarked or un-watermarked image, and possibly corrupted) whose ownership is to be determined and recovers a signature S' from the image. In this process, an additional image I can also be included which is often the original and un-watermarked version of J. This is due to the fact that some encoding schemes may make use of the original images in the watermarking process to provide extra robustness against intentional and unintentional corruption of pixels. Mathematically,

$$D\,(J, I) = S' \qquad (1.2)$$

The extracted signature S' will then be compared with the owner signature sequence by a comparator function C_δ and a binary output decision generated. It is 1 if there is a match and 0 otherwise.

$$C_\delta\,(S', S) = \begin{cases} 1\,, & c >= \delta \\ 0\,, & \text{otherwise} \end{cases} \qquad (1.3)$$

Here, c is the correlation of two signatures and □ is certain thresold. Fig1.3 shows the comparator.

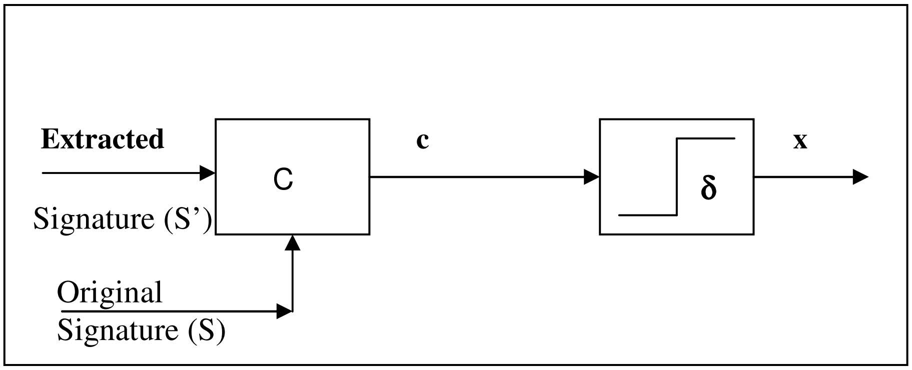


Fig. 1.3 Comparator

Where C is the correlator and x = C_{δ}(S', S). Without loss of generality, watermarking scheme can be treated as a three-tuple (E, D, C_{δ}).

A watermark must be detectable or extractable to be useful [20]. Depending on the way the watermark is inserted and depending on the nature of the watermarking algorithm, the method used can involve very distinct approaches. In some watermarking schemes, a watermark can be extracted in its exact form, a procedure we call **watermark extraction**. In other cases, we can detect only whether a specific given watermarking signal is present in an image, a procedure we call **watermark detection**. It should be noted that **watermark extraction can prove ownership** whereas **watermark detection can only verify ownership**. [21]

1.4.TYPES OF DIGITAL WATERMARKS

Watermarks and watermarking techniques can be divided into various categories in various ways.

Watermarking techniques can be divided into four categories according to the type of document to be watermarked as follows: [16]

- **Text Watermarking**
- **Image Watermarking**
- **Audio Watermarking**
- **Video Watermarking**

In the case of imagery, several different methods enable watermarking in the **spatial domain**. An alternative to spatial watermarking is **frequency domain** watermarking.

In other way, the digital watermarks can be divided into three different types as follows: [16], [21-23], and [32]

- **Visible watermark**
- **Invisible-Robust watermark**
- **Invisible-Fragile watermark**

Visible watermark is a secondary translucent overlaid into the primary image. The watermark appears visible to a casual viewer on a careful inspection. The invisible-robust watermark is embed in such a way that alternations made to the pixel value is perceptually not noticed and it can be recovered only with appropriate decoding mechanism. The invisible-fragile watermark is embedded in such a way that any manipulation or modification of the image would alter or destroy the watermark.

From application point of view digital watermark could be: [61]

- **source based** or
- **destination based**.

Source-based watermark are desirable for ownership identification or authentication where a unique watermark identifying the owner is introduced to all the copies of a particular image being distributed. A source-based watermark could be used for authentication and to determine whether a received image or other electronic data has been tampered with. The watermark could also be destination-based where each distributed copy gets a unique watermark identifying the particular buyer. The destination-based watermark could be used to trace the buyer in the case of illegal reselling.

1.5 APPLICATION OF DIGITAL WATERMARKS

VISIBLE WATERMARK: Visible watermarks can be used in following cases [16,21,23-25,32].

- **Visible watermarking for enhanced copyright protection**. In such situations, where images are made available through Internet and the content owner is concerned that the images will be used commercially (e.g. imprinting coffee mugs) without payment of royalties. Here the content owner desires an ownership mark, that is visually apparent, but which doesn't prevent image being used for other purposes (e.g. scholarly research).

- **Visible watermarking used to indicate ownership originals**. In this case, images are made available through the Internet and the content owner desires to indicate the ownership of the underlying materials (library manuscript), so an observer might be encouraged to patronize the institutions that owns the material.

INVISIBLE ROBUST WATERMARKS: Invisible robust watermarks find application in following cases. [21,23,26]

- **Invisible Watermarking to detect misappropriated images**. In this scenario, the seller of digital images is concerned, that his, fee-generating images may be purchased by an individual who will make them available for free, this would deprive the owner of licensing revenue.

- **Invisible Watermarking as evidence of ownership**. In this scenario, the seller the digital images suspects one of his images has been edited and published without payment of royalties. Here the detection of the seller's watermark in the image is intended to serve as evidence that the published image is property of seller.

INVISIBLE FRAGILE WATERMARKS: Following are the applications of invisible fragile watermarks. [21,23,27]

- **Invisible Watermarking for a trustworthy camera**. In this scenario, images are captured with a digital camera for later inclusion in news articles. Here, it is the desire of a news agency to verify that an image is true to the original capture and has not been edited to falsify a scene. In this case, an invisible watermark is embedded at capture time; its presence at the time of publication is intended to indicate that the image has not been attended since it was captured.

- **Invisible Watermarking to detect alternation of images stored in a digital library**. In this case, images (e.g. human fingerprints) have been scanned and stored in a digital library; the content owner desires the ability to detect any alternation of the images, without the need to compare the images to the scanned materials.

1.6 ATTACKS ON WATERMARKS

A watermarked image is likely to be subjected to certain manipulations, some intentional such as compression and transmission noise and some intentional such as cropping, filtering, etc. They are summarized below [26-29,71].

- **Lossy Compression**: Many compression schemes like JPEG and MPEG can potentially degrade the data's quality through irretrievable loss of data.

- **Geometric Distortions**: Geometric distortions are specific to images and videos and include such operations as rotation, translation, scaling and cropping.

- **Common Signal Processing Operations:** They include the followings.

  - **D/A conversion**
  - **A/D conversion**
  - **Resampling**
  - **Requantization**
  - **Dithering distortion**
  - **Recompression**
  - **Linear filtering such as high pass and low pass filtering**
  - **Non-linear filtering such as median filtering**
  - **Color reduction**
  - **Addition of a constant offset to the pixel values**
  - **Addition of Gaussian and Non Gaussian noise**
  - **Local exchange of pixels**

- **Other intentional attacks**:

  - **Printing and Rescanning**

  - **Watermarking of watermarked image (rewatermarking)**

  - **Collusion**: A Number of authorized recipients of the image should not be able to come together (collude) and like the differently watermarked copies to generate an un-watermarked copy of the image (by averaging all the watermarked images).

  - **Forgery**: A Number of authorized recipients of the image should not be able to collude to form a copy of watermarked image with the valid embedded watermark of a person not in the group with an intention of framing a 3rd party.

  - **IBM attack**: It should not be possible to produce a fake original that also performs as well as the original and also results in the extraction of the watermark as claimed by the holder of the fake original.

  - The **Unzign** [32] and **Stirmark** [40] have shown remarkable success in removing data embedded by commercially available programs.

1.7 DESIRED CHARACTERISTICS OF WATERMARKS

The desired characteristics of the watermarks are listed below.

- **Difficult to notice**: The invisible watermarks should not be noticeable to the viewers nor should the watermark degrade the quality of the content. Ideally, it should be imperceptible [33] and [35]. However, if a signal is truly imperceptible, then perceptual based lossy compression algorithm should, in principle, remove such signal. Of course, a just noticeable difference (JND) is usually observed by comparing two signals, e.g. compressed and uncompressed or watermarked and original.

- **Robustness**: In general, a watermark must be robust to transformations that include common signal distortions as well as D/A and A/D conversions and loss compression. Moreover, for images and video, it is important that the watermark survive geometric distortions such as translation, scaling and cropping etc. It has been argued [58] and [71] that robustness can only be attained if watermark is placed perceptually significant regions of an image. But it has been already mentioned that watermark should be imperceptible, which is possible if watermark is plated in perceptually insignificant regions of an image. They are two conflicting requirements. It should be noted **robustness actually comprises two separate issues**:

  - whether or not the watermark is still present in the data after distortion and

  - whether the watermark detector can detect it.

  It should also be noted that ability to embed robust watermarks in digital images does not necessarily imply the ability to establish ownership, unless certain requirements are imposed legally on the watermarking scheme [19]

- **Tamper-resistance**: As well as requiring the watermark to be robust to legitimate signal distortions, a watermark may also be subjected to signal processing that is solely intended to remove the watermark. It is important that a watermark be resistant to such tampering. There are a number of possible ways this may be achieved:

  - **Private Watermark**: A private watermark where either the decoder requires knowledge of the un-watermarked content or the pseudo-random noise sequence that constitutes the watermark is only known to sender and receiver, are inherently more tamper resistant than public watermarks in which everybody is free to decode the watermark

  - **Asymmetric encoder/decoder**: If removal of a public watermark requires inverting the encoding, then it is highly desirable to make the encoder as complex as possible, especially if the watermark is only to be applied once. However if decoders must run in real time, then it is necessary for the decoding process to be simpler than encoding.

- **Bit-rate**: The bit rate of a watermark refers to them amount of information a watermark can encode in a signal. This is especially important for public watermarks. Low bit-rate watermarks are more robust [36].

- **Modification and Multiple Watermarks**: In some circumstances, it is desirable to alter the watermark after insertion. For example, in the case of digital video discs, a disc may be watermarked to allow only a single copy. Once this copy has been made, it is then necessary to alter the watermark on the original disc to prohibit further copies. Changing a watermark can be accomplished either (a) removing the 1st watermark and then adding a new one or (b) inserting a 2nd a watermark such that both are readable, but are overrides the other.

- **Scalability**: It is well known that computer speeds are approximately doubling every eighteen months, so that what looks computationally unreasonable today may very quickly become a reality. It is therefore, very desirable to design a watermark whole decoder is scalable with each generation of computers. Thus for example, the first generation of decoder might be computationally inexpensive but might not be as reliable as next generation decoders that can afford to expend more computation to deal with issues such as geometric distortions.

- **Unambiguous**: Retrieval of watermark should unambiguously identify the owner. The watermark should not need any interpretation as looking into the database of codes to interpret the watermark unless a standard body maintains it internationally.

- **Universal**: The same digital watermark should apply to all three media under consideration. This is potentially helpful in the watermarking of multimedia products. Also this feature is conducive to implementation of audio/image/video watermarking algorithm on common hardware.

- **Minimum alternation of pixels**: While watermarking high quality image and art works the amount of pixel modification should be minimum.

- **Minimum Human intervention**: Insert of watermark should require little human intervention or labor.

1.8 CONTRIBUTIONS AND ORGANIZATION OF THE REPORT

We have developed four different Watermarking algorithms (Visible and Invisible) for protection of Digital Images. Two of them are in Spatial Domain are in and other two are in DCT Domain.

Chapter#2 gives the details of the technical challenges of the Watermarking problem. Information theory has been used to analyze the amount of data that can be embedded so and the locations where they can be embedded so that it is not perceptible. Different aspects of Human Visual System (HVS) and different properties of Visual Signals have been discussed. The use of Spread Spectrum Communications in Watermarking is also discussed. Chapter#3 reviews the existing literature on Watermarking. Chapter#4 gives the details of a Visible Watermarking Technique in Spatial Domain. Chapter#5 discusses the proposed DCT Domain Visible Watermarking Technique. Chapter#6 is an Invisible Watermarking Technique in Spatial Domain. Chapter#7 elaborates an Invisible Watermarking Technique in DCT Domain. Chapter#8 concludes the report and gives the future research directions.

CHAPTER#2

TECHNICAL CHALLENGES FOR WATERMARKING

2.1 How much to add and where?
2.2 Spread Spectrum Communications
2.3 Properties of Visual Signals
2.4 Just Noticeable Distortion (JND)
2.5 Properties of Human Visual System (HVS)

Data hiding, a form of steganography embeds data into digital media for various purposes. The technical challenges of data hiding are formidable. Any holes to fill with data in a host signal, either statistical or perpetual, are likely targets for removal for lossy signal compression**. The key to successful data hiding is the finding of holes that are not suitable for exploitation by compression algorithms.** A further challenge is to fill these holes with data in a way that remains invariant to a large class of host signal transformations.

2.1 HOW MUCH TO ADD AND WHERE?

Reliable communication was proven by Shannon [89] to be theoretically possible providing the information rate does not exceed a threshold known as **channel capacity.** With an idealized assumption regarding the form of the noise **n** corrupting a watermark, information theory can be used to derive the rules to decide about the strength of the watermark required and location of the watermark.

Let us write,

$$x_i + n_i = y_i \; ; \quad 1 \le i \le N \qquad (2.1)$$

where x_i is one element of a watermark vector of length N, n_i is an element of a noise vector and y_i is an element of a watermark distorted by image processing noise. Assuming the noise is additive, white, Gaussian:

$$p(y_i \mid x_i) = p(n_i) = (1 / \sigma \sqrt{2\pi}) \exp \left[-(y_i-x_i)^2 \; / 2\sigma^2 \right] \qquad (2.2)$$

Assuming that the n_i are uncorrelated and that

$$p(y_1, y_2,\ldots.,y_N|x_1,x_2,\ldots x_N) = \Pi_i^N \, p(y_i|x_i) \qquad (2.3)$$

Channel capacity [90] may be defined as

$$C = \max_{p(x)} I \, (X_i Y) \qquad (2.4)$$

where the watermark probability density function p (x) is chosen to maximize the average mutual information I(X;Y).

According to Proakis [91] the capacity is maximized with respect to distribution p(x) if

$$p(x_i) = (1/(\gamma\sqrt{2\pi})) \exp. [-x_i^2/(2\gamma^2)] \qquad (2.5)$$

which is a zero mean Gaussian density with variance γ^2 . In this case,

$$I_{max} = ½ N \log_2 (1+\gamma^2/\sigma^2) \quad (2.6)$$

In image watermarking we might expect that the transmission of information is functioning under quite extreme conditions, in which case $\sigma^2 >> \gamma^2$ which implies

$$\ln(1+\gamma^2/\sigma^2) \cong \gamma^2/\sigma^2 \quad (2.7)$$

Substituting eqn. (2.7) into eqn. (2.6) we obtain the following condition for reliable communication:

$$(\gamma^2/\sigma^2) > (2\ln 2)\ J/\ N \quad (2.8)$$

Where the N is the number of sites used to hide watermark information bit and J is the information rate. It should be noted that the noise power can be considerably greater then the signal power and, in theory at least, the message may still be transmitted reliably.

The strategy for communicating the watermark is now clear. Because a watermark should be imperceptible the signal to noise ratio (SNR), is severely limited. Reliable communication can only be assured by increasing bandwidth B to compensate poor SNR. Hence in the case of watermarking the maximum number N of suitable transform domain coefficients should be exploited for hiding information in the image. Watermarking may be considered as being an application of spread spectrum communications [83]. The Shannon limit may be approached by applying error control codes. Robust error correction techniques can be employed if necessary.

To answer the second part of the question "Where to embed ?" we again take recourse to information theory concepts. Let us assume that the image may be considered as a collection of parallel uncorrelated Gaussian channels which satisfy eqn. (2.1) above with the constraint that the total watermark energy is limited:

$$\sum_i^N \gamma_i^2 <= E \quad (2.9)$$

Using eqn. (.2.2) and assuming the noise variances are not necessarily the same in each channel, Gallger [90] shows that the capacity is,

$$C = ½ \sum_i^N \log_2 (1+\gamma_i^2/\sigma_i^2) \quad (2.10)$$

where σ_i^2 is the variance of the noise corrupting the watermark and γ_i^2 is the average power of the watermark signal in the i^th^ channel. This is a mere general form of eqn. (2.6). Capacity is achieved when

$$\gamma_i^2 + \sigma_i^2 = T_h \qquad \text{if} \quad \sigma_i^2 < T_h \quad (2.11)$$

where the threshold T_h is chosen to maximize the sum on the left-hand side of en. (2.9) and thus maximize the energy of the watermark. This result shows clearly that the watermark should be placed in those areas where local noise variance σ_i^2 is smaller than threshold T_h and not at all in those areas where local noise variance exceeds the threshold.

It should be noted that the simple analysis presented here assumes that the noise corruption suffered by the watermarks a result of common forms of image processing is Gaussian. This is not an accurate assumption to make in many cases. However, the Gaussian assumption is not a bad choice given that the aim is to derive the rules and heuristics that apply in general to a number of fundamentally different image processing scenarios.

2.2 SPREAD SPECTRUM COMMUNICATIONS

It is clear that the watermark should not be placed in perceptually insignificant regions of the image or its spectrum since many common signals and geometric processes attack these components. For example, a watermark placed in the high frequency spectrum of an image can be easily eliminated with little degradation to the image by any process that directly or indirectly performs lowpass filtering. The problem then becomes how to insert a watermark into the most perceptually significant regions of a spectrum without such alternations becoming noticeable. Clearly, any spectral coefficient may be altered, provided such modification is small. However, very small changes are very susceptible to noise.

To solve this problem, the frequency domain of the image or sound is viewed as a communication channel, and correspondingly, the watermark is viewed as a signal that is transmitted through it. Attacks and unintentional signal distortions are thus treated as noise that the immersed signal must immune to.

Thus, the watermarking can be considered as an application of **spread spectrum communications.** In spread spectrum communication, one transmits a narrow band signal over a much larger bandwidth such that the signal energy present in any single frequency is imperceptible. Similarly, the watermark is spread over very many frequency bins so that the energy in any one bin is very small and certainly undetectable. Nevertheless, because the watermark verification process knows the location and context of the watermark, it is possible to concentrate these many weak signals with a high signal to noise ratio (SNR). However, to considerably destroy such a watermark would require noise of high amplitude to be added to all frequency bins.

Spreading of the watermark throughout the spectrum of an image ensures a large measure of security against unintentional or intentional attack. First the spatial location of the watermark is not obvious. Furthermore, frequency regions should be selected in a fashion that ensures severe degradation of the original data following any attack on the watermark.

Cox et al [71,58] have used a technique analogous to spread spectrum communications. Hartung and Girod [73] have developed the relevant mathematical framework for spread spectrum watermarking technique.

2.3 PROPERTIES OF VISUAL SIGNALS

Visual signals are generally recognized as amplitude plots, intensity versus space displays of image information and intensity versus space and time displays of video scenes. These waveforms reveal a lot of information of the properties of the signals. Some of the properties are listed below.

- **Nonstationarity:** Common to all waveforms is the property of nonstationarity. image and video signals contain a wealth of segments of flat or slowly changing intensity, as well as edges and textured regions.

- **Periodicity:** There exits a line to line and frame to frame periodicities in image and video signals. They are not exactly periodic but there exits redundancy between frames and lines.

- **Power Spectral Density:** In a global or longtime average sense, visual signals tend to have lowpass frequency spectra. Short-term frequency analysis i.e. in local sense, say in particular region of the image, however reveals parts of signals that are either all-pass or high-pass.

- **Properties Of Color Signals:** In typical inputs, the UV or IQ components have lower energy and lower bandwidth compared to the luminance component Y. this is the reason why these components are subsampled and use coarser quantization for data compression. Perceptual criteria relate to lower sensitivities to coarse quantization, and to the related observation that additional liberties in chroma quantization are possible in the context of a strong change in the luminance component.

2.4 JUST NOTICEABLE DISTORTION

The properties of visual signals are frequency, intensity, texture, and temporal activity. The properties can be extracted after performing short time or spatio-temporally local analysis of the input signal. These properties then can be used to derive a perceptual distortion threshold. This threshold can be a function of time, space or frequency. It expresses a critical distortion profile in the sense that if the distortion caused by watermarking or some compression algorithm is at or below the threshold at all points of the time, space or frequency, the degradation in the signal quality is imperceptible. The critical distortion profile is called **Just Noticeable Distortion (JND)**. Another related term that could be defined is a supra-threshold generalization of it, which is not transparent (but still perceptually optimum) **Minimally Noticeable Distortion (MND)**.

2.5 PROPERTIES OF HUMAN VISUAL SYATEM

- **Brightness sensitivity:** The sensitivity of the human eye is to perceive a low intensity signal (watermark) in the presence of backgrounds of different intensity. When mean value of the Noise Square is the same as that of the background, the Noise Square tends to be most visible against a mid-grey background. The characteristic is known as Weber's law, means that the eye has high sensitivity at low intensity levels and greatly reduced sensitivity at high intensity levels. Superimposed on this is a dependence on the intensity of the region surrounding the region under test. As the surrounding region intensity is increased, the relative intensity in dark areas is reduced and the sensitivity in the light areas is increased.

- **Frequency sensivity:** Psychovisual studies have shown that the human visual system (HVS) has a general bandpass characteristic with peak sensitivity between 3 and 4 cycles per degree and reduced sensitivity at higher and lower spatial frequencies. One of the sensitivity functions is proposed in [85]. The strength of the watermark levels in a particular spatial frequency has to therefore be inversely proportional to the relative sensitivities of the corresponding spatial frequencies.

- **Texture sensitivity:** The visibility of distortion depends on the background texture. The distortion visibility is low when the background has a strong texture. In a highly textured image block, energy tends to be more evenly distributed among the different DCT coefficients. In a flat-featured portion of the image the energy is concentrated in the low frequency components of the spectrum.

- **Spatial masking:** The phenomena of distortion masking, no noise masking is a complex result of transuding of natural components of perception. It is highly adaptive and refers to the perceptibility of one signal in the presence of another in its space or frequency vicinity. The changing visibility of a single stimulus in an area of varying spatial activity leads to the reduction in the visibility of the pixel errors in the areas of high-detail luminance changes (high activity).

CHAPTER # 3

REVIEW OF EXISTING WATERMARKING/ DIGITAL SIGNATURE ALGORITHMS

3.1 Algorithms in spatial domain
3.2 Advantages of frequency domain
3.3 Algorithms in frequency domain
3.4 Algorithms for video

3.1.ALGORITHMS IN SPATIAL DOMAIN

Bender et al. [36] propose patchwork in which a watermark is embedded into the image by modifying the statistical property of the image. The difference between any pair of randomly chosen pixels is Gossip distributed with a mean zero. This mean can be shifted by selecting pair of points and incrementing the intensity of one of the points and decrementing the intensity of the other. The resulting watermark is predominantly high frequency. However the authors recognize the importance of placing the watermark in perceptually significant regions and consequently modify the approach so that pixel patches rather then individual pixels are modified, thereby shaping the watermark more to significant regions of the human visual system. Patchwork is robust to cropping but suffers from the disadvantage of being highly sensitive to affine transformation, JPEG compression & very low bit rate i.e. one bit per image. The inventors provide data that the recovery rate is 85% after JPEG compression, with quality parameter 75%, which is not likely stand up as credible evidence beyond a reasonable doubt in a course of law.

Bender et al. [36] have also proposed texture block coding in which a block from a region with a random texture is copied and placed in a region with similar texture. Detection of hidden blocks is easy and can be done as follows:

- The image is autocorrelated with itself. This will produce peaks at every point in the autocorrelation where identical regions of the image overlap. If large enough areas of an image are copied, this will produce an additional autocorrelation peak at the correct alignment for coding.

- The image is shifted as indicated by the peaks in previous step. Now, the image is subtracted from the shifted copy, padding the edges with zeros as needed.

- The result is squared and threshold to recover only those values quite close to zero. The copied region will be visible at these values.

The method requires a human operator to choose the source and destination regions and to evaluate visual impact of the modifications on the image. The technique will not work on the images that lack moderately large areas of continuous texture from which to draw.

P.G.Van Schyndel et al. [42] discuss two methods. The first is based on bit-plane manipulation of the LSB, which offers easy and rapid decoding. The second method utilizes linear addition of the watermark to the image data and is more difficult to decode, offering inherent security. The first method involves the embedding of the m-sequence on the LSB of the image data. The second method uses LSB addition for embedding the watermark. The decoding process makes use of the unique and optimal auto-correlation function of m-sequences. The process requires the examination of the complete bit pattern and its current implementation, must therefore be performed off-line which is principal disadvantage. However, it is intrinsically more secure, since a potential code breaker has to perform the same operation, without any a priori knowledge. The main problem found with adding the watermark is in retaining the dynamic range of the original image and the auto-correlation output. The watermark is robust to averaging, and potentially compatible with JPEG compression.

R.B.Wolfgang and E.J.Delp [43] present a watermark, which is a two dimensional extension of [42]. Their first watermark is robust the mean and median filtering and the second watermark is robust to JPEG compression. The first watermark uses a much longer m-sequences than its counterpart [42], which is, arranged row by row into two-dimensional blocks. Then a zero is appended to the entire m-sequences, instead of using an extended m-sequence. One advantage of a two-dimensional watermark is the ability to more effectively locate where an image has been changed. They define the spatial cross-correlation function of images X and Y as:

$$R_{xy}(\alpha,\beta) = \sum_i \sum_j X(i,j)Y(i-\alpha,j-\beta) \quad (3.1)$$

Let X be the original image block, W be the watermarked block, Y be the water marked image block and Z be the watermarked image block that might be forged. The test statistics for the block, is defined as:

$$\delta = R_{yw}(0,0) - R_{zw}(0,0) \quad (3.2)$$

If the watermarked image is unchanged, then $\delta = 0$. When is larger then a defined tolerance the block fails the watermark test. A larger threshold provides more robustness but increases the probability of missing a forgery the authors revised this watermarking technique to improve security and localization. Localization is the ability to identify where in the image any changes have occurred. The block size is 8x8 pixels and each block is formed as follows:

- A large span m-sequence (n = 96) is generated with the first 128 bits skipped.
- The next 64 bits are inserted in the first block of the watermark column by column. The next m bits are skipped.
- The procedure repeats for the remaining blocks.

To make it JPEG compatible new statistics was defined:

$$\delta = R_{yjw}(0,0)-R_{zjw}(0,0) \quad (3.3)$$

where Yj is the watermarked image after JPEG compression and decompression and Zj be possibly forged water marked image after JPEG processing.

R.B.Wolfgange and E.J.Delp [44] elaborated watermarking techniques introduced in [43]. They describe how their techniques withstand random errors. Here they find the mean of δ for all blocks as follows:

$$E\,[|\delta|] = 1/N\ \sum_i^N \delta_k \tag{3.4}$$

where δ_k is the value of δ for the kth block and N is the number of 8x8 blocks in the mage. The test statistics E [|δ|] is not robust to small attenuation as it is very small. This is a potential problem. They give the range of E [|δ|] for an image to be fully authentic but forged, possibly authentic and completely in authentic (or water marked by a different owner).

I. Pitas and N.Nikolaids and Kaskali [45-48] use an approach that allows slightly more information to be embedded. A binary signature that consists of equal no of zeros and ones is embedded in an image by assigning pixels into one of the two sets. The intensity levels of pixels in one of the sets are altered. The intensity levels are not changed in the other set. Signature detection is done by comparing mean intensity value of the marked pixels against that of the not marked pixels. Statistical hypothesis testing id used for this purpose. The signature can be designed in such a way that it is resistant to JPEG compression and low pass filtering. According to the authors, the degree of certainty can be as low as 84% and as high as 92%, which would likely not stand up as evidence in a court of law for copyright protection.

G.Voyatris and I.Pitas [49] use toral automorphism to chaotically mix binary logos or signatures, which are added to a secret region in the image. The embedding algorithm is robust to noise filtering and compression. The reconstructed watermark is recognized visibly if the watermarked is affected by JPEG compression up to 6:1. By using detection methods we can get a reliable answer about the existence or not of a watermark even if the watermarked image has been affected quite strangely by filtering and JPEG compression, greater then 10:1.

J.Zhao and K.Koch [50] develop the product **Syscop** is compatible with JPEG compression quality factor 50%. An image is partitioned into 8x8 blocks and eight coefficients in the blocks are used for marking. The blocks are pseudo randomly selected to minimize detection. The method is still weak against physical damages (e.g. cut a pixel live, grab an area etc.).

M.Scheinder and S.F.Chang [41] present a variation on J.Zhao and K.Koch [50] method for image authentication. The general procedure for generating a constant based signature is given as follows:

- The content of interest C_o is extracted from the original image I_o using extraction function F_o.
- The content is hashed using a hash function F_h to reduce the amount of data.
- The hash H_o is then encrypted using the private key K_{pr} of the signing entity to produce the final signature S.

Mathematically it can be written as follows:

$$\left.\begin{aligned} C_o &= F_c\,(I_o) \\ H_o &= F_h\,(C_o) \\ S &= H_o + K_{pr} \end{aligned}\right\} \qquad (3.5)$$

To verify the authenticity of an questionable image I_t , the following steps are followed:

- The signature is decrypted using the public key K_{pu}
- Then it is compared with the hashed content extracted from the questionable image.
- If the distance between the feature vectors is less then a threshold value τ, then the questionable image is declared un-manipulated.

Mathematically we can write the step as below:

$$\left.\begin{aligned} C_t &= F_c\,(\,I_t\,) \\ H_t &= F_h\,(\,I_t\,) \\ H_o &= S + K_{pu} \\ \| H_o - H_t \| &< \tau \end{aligned}\right\} \qquad (3.6)$$

The algorithm is compatible with certain types of image modification (e.g. lossy compression).

K.Hirotsugu [51] presents a digital signature system to assert copy right of image data. The outline of the signature method is shown as follows:

- The original image is divided into 8x8 blocks.
- The region graph is generated.
- A random permutation is generated as secret information of the owner of the original image.

- The concealed graph is generated.
- The graph data is concealed in the original image.

The verification process is given as follows.

- The region graph is generated.
- The concealed graph is decoded from the concealed information.
- The isomorphism between the two graphs is shown using ZKIP (zero knowledge interactive proof).

This technique has a very good advantage that the secret information is not disclosed even during the authentication process. The author has not mentioned about robustness of the technique for various attacks.

M.M.Yeung and F.Mintzer [52] have proposed an invisible image watermarking technique for image verification, where one is interested in knowing whether the content of the image has been altered since some earlier time, perhaps because of the act of a malicious party. That means that this is an invisible fragile watermarking algorithm. In the watermarking process, a binary map B (i, j) of a watermarked image W (i, j), is embedded into the source image I (i, j), to produce a stamped image I' (i, j). in the image verification processing, a watermark image, B(i,j), is extracted from a stamped image I'(i,j). The watermarking process does not introduce visual artifacts and retain quality of the images. A verification key is produced together with a stamped image. The embedded watermark image can be extracted from the stamped image using this verification key. Alternations to an image introduce artifacts on the extracted image, which can be visually and automatically identified. The technique offers fast image verification to detect and localize unauthorized image alterations. The technique provides a means of ensuring data integrity, adds to security of digital content and allows the recipients of an image to verify the image as well as to display the ownership information on the image.

J.F.Delaigle et al. [53] present an additive watermarking technique for grey-scale images. It contains in secretly embedding a binary code into the image without degrading its quality. Those bits are encoded through the phase of maximal length sequences (MLS). The core of the embedding process is underlaid by a masking criterion that guaranties the invisibility of the watermark. It combined with an edge and texture discrimination to determine the embedding level of the MLS, where bits are actually spread over 32x8 pixel blocks. The watermarking method is resistant to white noise, JPEG compression, lowpass filtering and forgery.

Kutter et al. [54] has presented a spatial domain method which does not need the original for the purpose of extraction of the watermark. Signal bits are multiplied and embedded by modifying the pixel values in the blue channel, the color that the eye is least sensitive to. Further the modifications are additive, subtractive depending on the value of bit, the proportional to the luminance. For extraction the prediction of the original pixel value is used in place of the original. A cross-shaped neighborhood is chosen to predict the same. The sign of the difference of the predicted value and the pixel value of the watermarked copy is used in decision making. Random locations are selected for embedding. Two bits are always maintained as 0 and 1 which define a geometric reference used for countering geometrical attacks. An adaptive threshold is also used to improve decision making. The scheme is robust to blurring, JPEG compression (75% quality factor), and geometrical operation.

J.R.Hernandez et al. [64] model and analyze a watermarking scheme for copyright protection. In this scheme a signal following a key-dependent 2-D multiple modulation is added to the image for ownership enforcement purpose. They derive bound and approximations to the receiver operating characteristic. The results can be used to determine the threshold associated to a required probability, false probability of detection. They model the data-hiding process as communication channel.

3.2 ADVANTAGES OF FREQUENCY BASED METHODS

We have already discussed various attacks that a watermark may encounter in Sec.1.6. We will discuss here the effect of those attacks on the frequency spectrum of a signal, which will show the advantages of a frequency based method [71].

Lossy compression is an operation that usually eliminates perceptually nonsalient components of an image or sound. If one wishes to preserve watermark in the face of such an operation, the watermark must be placed in the perceptually significant region of the data. Most processing of this sort takes place in the frequency domain. In fact, data loss usually occurs among the high frequency components. Hence the watermark must be placed in the significant frequency components (low frequency component) of the image (or sound) spectrum.

Geometric distortions are specific to images and videos. By manually determining a maximum of four or nine corresponding points between the original and distorted watermark, it is possible to remove any two or three dimensions affine transformation. However, an affine scaling (shrinking) of the image leads to loss of data in the high frequency regions of the image. Cropping may be a serious threat to any spatially based watermark but it is less likely to affect frequency based scheme.

Common signal distortions, which are nonlinear particularly, it is difficult to analyze their effects in either a spatial or frequency based method.

3.3 ALGORITHMS IN FREQUENCY DOMAIN

J.J.K.O'Runaidh et al. [55] present a perceptual watermarking method operating in the transform domain. They argue that water marking needs to be adaptive in order to be robust and place the watermark in the perceptually most significant components of the image. A watermark is non-intrusive if it resembles the image that it is designed to protect. That means less information should be hidden on flat featureless regions of the image & more information in the parts of the image that contain more texture or around edges, provided edge integrity is maintained. Transform domain methods is preferred as it is felt that it is possible to mark according to perceptual significance of different transform components and the watermark gets regularly distributed over the entire image sub-block, making it more difficult for attackers in possession of independent copies of the image to decode and read the mark. The watermark survived 20:1 JPEG compression on the standard 256x256 Lena image.

J.J.K.O'Runaidh et al. [56] prepare a discrete Fourier transform phase based method of conveying watermark information. They used the fact that phase is more important than magnitude of the DFT values. The watermark survived 15:1 JPEG image compression.

M.D.Swason et al. [57] introduce a watermarking scheme for image which exploits the human vision system (HVS) to guarantee that embedded watermark is imperceptible. The insertion of watermark involves following steps:

- The image is segmented into blocks.
- DCT of each block is found.
- A frequency mark of each block is computed.
- The resulting perceptual mark is scaled and multiplied by the DCT of a minimal length pseudo-noise sequence (author id).
- The watermark is then added too the corresponding DCT block.
- The watermark image is obtained by assembling the inverse DCTs of each block.

They use a model for frequency masking. Spatial masking is used to verify that the watermark designed with the frequency-masking model is invisible for local spatial regions. Detection of the watermark is accomplished via hypothesis testing. Experimental results show that the watermark is robust to several distortions including white and colored noise, JPEG coding at different qualities and cropping.

I.J. Cox et al. [58and71] propose to insert a watermark into the spectral components of the data using techniques analogous to spread spectrum communication. The argument is that the watermark must be perceptually significant components of a signal if it is to be robust to common signal distortions and malicious attack. However, the modification of these components can lead to perceptually degradation of the signal. The watermark insertion consists of following steps:

- DCT of the image is computed
- The perceptually significant regions of the image are found out.
- The watermark X = $x_1, x_2, \ldots, x_n$ is constructed where each x_i is chosen according to N (0,1), where N(0,1) denotes a normal distribution with mean 0 and variance 1.
- The watermark is inserted in the DCT domain of the image by setting the frequency components v_i in the original image to VI' using eqn. (3.7).

  $$v_i' = v_i (1+\alpha x_i) \qquad (3.7)$$

  where α is a scalar factor.

The author chose $\alpha = 0.1$. A Gaussian type of watermark is used because it is more robust to tampering then uniform embedding. Extraction of watermark consists of following steps:

- DCT of watermark image is computed.
- DCT of the original image is computed.
- The difference of the two is the watermark X*.

The extracted watermark X^* is compared with the original watermark X using similarity function given in eqn. (3.8).

$$\mathrm{sim}\,(X,X^*) = (X\cdot X^*) / \mathrm{sqrt}(X^*\cdot X^*) \qquad (3.8)$$

The watermark is robust to common signal and geometric distortion such as A/D and D/A conversion, resampling, quantization, compression, rotation, translation, crapping and scaling. The watermark is universal in the sense that it can be applied to all three media. Retrieval of the watermark unambiguously identifies the owner and the watermark can be constructed to make counterfeiting almost impossible.

C.T.Hsu and J.L.Wu [59] propose an image authentication technique by embedding each image with a signature so as to discourage unauthorized copying a DCT based algorithm is used to implement the middle band embedding. The proposed technique could actually survive several kinds of image processing and the JPEG lossy compression.

A.G.Bors and I. Pitas [60] propose an algorithm for image copyright protection. The algorithm proposed selects certain blocks in the image based on a Gaussian network classifier. The pixel values of the selected blocks are modified such that their DCT coefficients fulfill a constraint imposed by the watermark code. Two different constraints are considered. The first approach consists of embedding a linear constraint among selected DCT coefficients and second one defines circular detection regions in the DCT domain. The watermark detection is based on the probability detection theory. The proposed algorithm is resistant to JPEG compression.

C.Podilchuk and W.Zeng [61] propose a watermarking technique for digital images that is based on utilizing visual models, which have been developed in the context of image compression. The visual models give a direct way to determine the maximum amount of watermark signal that each portion of an image can tolerate without affecting the visual quality of the image. The scheme is best suited for destination faced. The watermark encoding scheme consists of a frequency decomposition based on an 8x8 framework followed by JND calculation and watermark insertion. Watermark detection is based on classical detection theory. The original image is subtracted from the received image and the correlation between the signal difference and specific watermark sequence is determined. The maximum correlation value is compared to a threshold to determine whether the recovered contains the watermark in question. The watermarking scheme is extremely robust to JPEG compression, cropping, scaling, additive noise, gamma correction and the combination of printing/Xeroxing/rescanning.

A. Piva et al. [62and70] propose a method in which watermark casting is performed by exploiting the masking characteristics of HVS and the embedded sequence is extracted without reporting to the original image. The watermark insertion process involves the following steps:

- N x N DCT of an N x N image is computed.
- DCT coefficients are recorded into a zigzag scan.
- The first L + M coefficients are selected to generate a vector T = {t_1, t_2,…………..,t_L,t_{L+1},…………,t_{L+m}}.
- In order to obtain a trade off between perceptual invisibility and robustness to image procuring techniques, the lowest L coefficients are

skipped and a watermark X = {x_1, x2,..........,x_m} is embedded in the last m members to obtain a new vector T' = {t_1', t_2', ...t_L', t_{L+M}'} according to the following rule:

$$t_{L+i}' = t_{L+i} + \alpha .|t_{L+i}| .x_i \qquad (3.9)$$

where i = 1,2,................M. The vector T' is then reinserted in the zigzag scan and inverse DCT algorithm is performed obtaining the watermarked image I'.

- In order to enhance the robustness of the watermark characteristics of the HVS is exploited to adapt the watermark to the image being signed. The original image I and the watermarked image I' are added pixel by pixel according to the local weighting factor b_{ij}, obtaining a new watermarked image I", i.e.

$$\begin{aligned} y''_{ij} &= y_{ij}(1-b_{ij}) + b_{ij}y'_{ij} \\ &= y_{ij} + b_{ij}\,(y'_{ij}-y_{ij}) \qquad (3.10) \end{aligned}$$

The b_{ij} takes into account the characteristics of the HVS.

The watermark detection process consists of following process:

- Given a possibly corrupted image I^*, the N x N DCT is applied to I^*.
- The DCT coefficients are recorded into a zigzag scan.
- The coefficients from the $(L+1)^{th}$ to the $(l+M)^{th}$ are selected to generate a vector T* = {t*L+1,t*L+2,.........t*L+M}
- The correlation between the marked and the possibly corrupted coefficients T* and the mark itself is taken as a measure of mark presence.

The watermark is robust to JPEG compression, lowpass and medium filtering, histogram equalization and stretching, Gaussian noise addition, nesting cooping and multiple watermarking.

J.J.K.O'Ruanaidh and T.Pun [63and69] propose that Fourier transform based invariants can be used for digital image watermarking. The watermark takes the form of a two-dimensional spread spectrum signal in the RST transformation invariant domain.

The watermark survives lossy image compression using JPEG at normal setting (75% quality factor). The watermark is also reasonably resistant to cropping and could be recovered from a segment approximately 50% of the size of the original image.

J.R.Smith and B.O.Comisky [65] use the concepts of communication theory to characterize information-hiding schemes. They introduce a framework for quantifying the tradeoffs among the conflicting figures of merit useful for characterizing information-hiding schemes:

- capacity (the number of bits that may be hidden and then recovered),
- robustness to accidental removal and
- imperceptibility.

They also introduce a technique called “predistortion’’ for increasing resistance to JPEG compression. They pointed out that frequency hopping spread spectrum is superior perceptually and in terms of robustness to accidental removal, to direct sequence spread spectrum.

D.J.Fleet and D.J.Heeger [66] describe method for embedding information in color images. A model of human color vision is used to ensure that the embedded signal is invisible. Sinusoidal signals are embedded so that they can be detected without use of original image. The embedded information is robust enough to be reliably extracted after being printed and scanned on common place equipment.

G.W.Braudway [67] presents a method for marking high quality digital image with a robust and invisible watermark. The watermark is imparted into an image as a random but reproducible, small modulation of its pixel brightness and becomes a permanent of the marked image. Watermark detection can be done without using the original image. The detection method presented exploits the not all understood but superb ability of the human visual system to recognize a correlated pattern in a scattered diagram called a “visualizer-coincidence image”. The watermarking scheme is robust to JPEG compression, printing and rescanning of the image.

C.I.Podilchuk and W.Zeng [68] have proposed two watermarking techniques for digital images that are based on utilizing visual models which have been developed in the context of image compression. One technique is based on frequency decomposition consists of block based DCTs and the second technique is based on frequency decomposition consists of a wavelet decomposition. First technique is same as already described in [61]. The second technique based on a wavelet decomposition uses almost similar insertion and detection procedure, but has got lots of advantages over its DCT counterpart as discussed here. Due to the hierarchical decomposition, this approach has an advantage of constructing watermark components that have varying spatial support providing the benefits of both spatially local and spatially global watermark. The watermark components with local spatial support are suited for local visual masking effects. And robust to signal processing such as cropping. The watermark components with global spatial support are robust to operations such as lowpass filtering. DCT faced framework produces watermarks wit only local spatial support and the spread spectrum approach produces watermarks with global spatial support.

Tao and Dickinson [72] propose an additive watermarking techniques which assigns each spatial region a noise sensitive level and embeds the watermark using block DCT according to this sensitivity level. NAC coefficients having the smallest quantization step sizes in the JPEG quantization tables are selected and modulated. The authors have arrived at a formula based on the noise sensitivity of the block for the extent of perturbation possible to the ac coefficients. The blocks are classified into 6 perceptual classes basing on gradient and variances in the particular blocks. The watermark generated is a function of image itself. The Neyman-Pearson theorem is used to design the detector to achieve a desired low false alarm probability. This needs original imager for watermark detection.

3.4 ALGORITHMS FOR VIDEO

F.Hartung and B.Girod [73-77] present a scheme for robust interoperable watermarking of MPEG–2 encoded video. The watermarking is either embedded into the encoded video or into the MPEG-2 bit streams and can be retrieved from the codec video. The basic idea of watermarking for raw video is addition of a pseudo-random signal to the video that is below the threshold of perception that can't be identified and thus removed without knowledge of the parameters of the watermarking algorithm. The approach to accomplish this is a direct extension from direct-sequence spread spectrum communications (already discussed in chapter 2). The marking of raw video data v_i to produce a modified signal $v_i^{'}$ is described by eqn. (3.11).

$$v_i^{'} = v_i + \alpha b_i . p_i \qquad (3.11)$$

Where p_i is the pseudo-noise sequence, b_i is the embedded bit and α is amplitude-scaling factor. The information bit is recovered by a matched filter. Given several sequences with different watermarks, it is easier to figure out the watermarked pixel values if the watermark consists only of the –1's and 1's. The amplitude factor α can be used to exploit spatial and temporal masking effects of the human visual system (HVS). Several watermarks can be superimposed, if different pseudo-noise sequences are used for modulation. This is due to the fact that different pseudo-noise sequences are in general orthogonal to each other and do not significantly interfere. In the bit stream domain if it is more difficult to embed a watermark into video, especially when the requirement is imposed that the bit rate may not be increased. For each signal block, the watermarking procedure consists of the following steps:

- The DCT of the watermark data (of the spread information bits modulated by the pseudo-noise sequence) is calculated for 8x8 block. A zigzag scan is done to get a 1x64 vector of rescanned DCT coefficients. The DCT coefficients are denoted by W_n with W_o being DC coefficients and W_{63} being the highest frequency AC coefficients. The DCT coefficients of the unwatermarked signal are denoted by V_n and that of the watermarked signal by $V_n^{'}$.

- For DC coefficients, $V_o^{'} = V_o$ + Wo that is the mean value of the watermark block is added to the mean value of the signal block.

- For the AC coefficients, the bit stream of the coded signal is searched for the next VLC codeword, the (run-level) pair (r_m, lm) belongs to that codeword is identified and thus the position and amplitude of the ac DCT coefficients V_m represented by the VLC codeword.

- $V_m^{'} = V_m + W_m$ is the candidate DCT coefficients for the watermarked signal. However $V_m^{'}$ should not increase the bit-rate.

- Let R be the number of bits used for transmitting the codeword for (r_m,l_m) (i.e. for V_m) and $R^{'}$ be the number of bits used for transmitting the codeword for (r_m,$l_m^{'}$)(i.e. for $V_m^{'}$).

- If R >= $R^{'}$ the codeword for (r_m,$l_m^{'}$), is transmitted else the code word (r_m,$l_m^{'}$) is transmitted.

- Steps 3-6 are repeated until end of block (EOB) codeword is encountered.

Due to bit rate constraint, usually only few DCT coefficients of the watermark can be incorporated per 8x8 block. As a result, the watermarking scheme in bit stream domain is less robust then its counterpart in the pixel domain. But the scheme working on encoded video is of much lower complexity then a complete decoding process followed by watermarking in the pixel and recording. Although an existing MPEG-2 bitstream is partly altered the scheme avoids drift problems. The authors have suggested schemes for drift compensation in [76]. The embedded watermark can be retrieved from the watermarked video without knowledge of the original video. The watermark is robust against the linear and non-linear operations like further transform coding, filtering, quantization, modest rotation etc.

I.J.Cox et al. [58and71] has proposed watermarking techniques analogous to spread spectrum communications has already been discussed in Sec.3.3. This technique can be extended to video.

M.D.Swanson et al. [78] give a scheme for hiding high bit rate supplementary data such as secondary video, into a digital video stream by directly modifying the pixels in the video frames. The technique requires no separate channel or bit interleaving to transmit the extra information. The hidden data may include real time video and speech, text, hypertext, image data etc. the image data remains intact as the host video is compressed, stored and transmitted etc. upon receiving the video, the intended audience may extract the information. The data-hiding algorithm exploits frequency masking to embed data. The data hiding approach is based on two steps:

- Linear projection, a common linear algebra operation and
- Quantization and Perturbation.

The scheme is robust to lossy compression and Gaussian noise addition.

M.D.Swanson et al. [79] propose an object based watermarking technique. Individual watermarks are created for objects within the video. Each watermark is created by shaping an author and video dependent pseudo-random sequence according to the perceptual masking characteristics of the video. The insertion procedure has following steps:

- The spatial (S) and frequency masking (M) values for the current frame are computed. The frequency masking values are obtained from DCT coefficients of 8x8 blocks in the frame.
- The frame segmented to block (B) to ensure that masking estimates are localized.
- Each block of frequency masking values is then multiplied by part of the pseudo-random author representation.
- The inverse DCT of the product (P) is computed.
- The result is multiplied by the spatial masking values for the frame, creating the perceptually shaped pseudo-noise W.
- The pseudo-noise is added to the blocks of the frame to get watermarked block B’
- The watermark for a macroblock in the current frame is replaced for the watermark for the macroblock from the previous frame if the distortion D (V) is less than threshold T.

Detection of watermark is accomplished via generalized likelihood ratio test. The watermark is statistically undetectable. The watermark also resolves multiple ownership claims. The watermark algorithm may be easily incorporated in to the MPEG-4 object based coding framework. The watermarking procedure is robust to video degradations that result from noise, MPEG compression, cropping, printing and scanning.

C.T.Hsu and J.L.Wu [80] present a DCT based watermarking technique for video sequences. The steps for watermark insertion are given below:

- The original image is divided into 8x8 blocks and the 2-D DCT is applied independently to each block.
- The middle frequency range coefficients are picked up.
- A 2-D sub-block is used in order to compute the residual pattern from the chosen middle frequency coefficients.
- The watermark is a binary image. A fast 2-D pseudo-random number traversing method is used to permute the watermark so as to disperse its spatial relationship.
- Both variances of image block and watermark blocks are sorted and mapped accordingly so that the invisibility of the watermarked image will improve.
- After binary residual patterns of the transform intraframe are obtained, for each marked pixel of the permuted watermark, the DCT coefficients are modified according to the residual mask so that corresponding polarity of the residual value is reversed.
- Inverse DCT value of the associated result is calculated to obtain the watermarked image. For P-frame, modifying then temporal relationship between the current P-frame and its reference frame embeds the watermarks.
- For B frame, the residual mask is designed between the current B frame and its past and future reference frame. The polarity of the residual frame is also reversed to embed the watermark.

The extraction procedure is simply the reverse operation of insertion procedure. This requires the original frame, then watermarked frame and also the digital watermark, which is a disadvantage of this watermarking scheme. The scheme is robust to cropping operation and MPEG compression.

M.D.Swanson et al. [81] presents a scene based and video dependent watermarking scheme. It directly exploits the spatial masking, frequency masking and temporal properties to embed a robust, invisible watermark. The watermark consists of static and dynamic temporal components that are generated from a temporal wavelet transform of the video scenes generating a multiresolution temporal representation of the video. The lowpass frame consists of static component in the video scene. The high pass components capture the motion components and changing nature of the video sequence. The watermark embedded in the lowpass frames exist throughout the entire video scene due to wavelet localization properties. The watermark detection is done by the help of hypothesis testing. The watermark is robust to several robust degradations and distortions.

T.Y.Chung et al. [82] propose a watermarking technique which is appropriate for MPEG-2 video coding system by extending the direct sequence spread spectrum. The method embeds the hiding information into coefficients after DCT or quantisation. The insertion procedure has following steps:

- Original I picture is divided into 8x8 blocks and each block is transformed DCT domain.
- Each block is classified with respect to its energy distribution by using classification masks.
- After block classification, embedding area for each class is assigned to each of the blocks and adaptive embedding strength is obtained.
- DCT of the hiding information (modulated with PN code) is calculated (block wise).
- Picture blocks and watermark blocks are added up using adaptive strength.
- IDCT is found that gives watermarked image.

The watermark can be extracted following the reverse insertion procedure but using watermarked image. The scheme is robust to various attacks.

CHAPTER # 4

AN ADAPTIVE VISIBLE WATERMARKING TECHNIQUE FOR IMAGE DATA

(This work was presented in International Conference on Information Technology, 1998,CIT’98, Bhubaneswar, Orissa, India)

ABSTRACT

With the advances in networked multimedia technology, reproduction of multimedia data has become easier. This has created a need for the copyright protection of the data. **Digital Watermarking** is the technique in which a visible / invisible signal (watermark) is embedded in the data for copyright protection. Here, we describe a visible watermarking scheme

4.1 INTRODUCTION

Digital watermarking is defined as a process of embedding data (watermark), into a multimedia object to help to protect the owner's right to that object. The embedding data (watermark) may be either visible or invisible. In visible watermarking of images, a secondary image, the watermark, is embedded on a primary image such that the watermark is intentionally perceptible to a human observer; whereas in the case of invisible, the embedded image data that is not perceptible, but may be extracted by a computer program.

Some of the desired characteristics of visible watermarks are listed below [21,23].

- A visible watermark should be obvious in both color and monochrome images.
- The watermark should spread in a large and important area of the image in order to prevent its deletion by clipping.
- The watermark should be visible yet must not significantly obscure the image details beneath it.
- The watermark must be difficult to remove, rather removing a watermark should be more costly and labor intensive than purchasing the image from the owner.
- The watermark should be applied automatically with little human intervention and labor.

There are very few visible watermarking techniques available in current literature. The IBM Digital Library Organization has used a visible watermarking technique to mark digitized pages of manuscript form the Vatican archive [25]. Rajmohan [84] proposes a visible watermarking technique in DCT domain. He divides the image into different blocks, classifies these blocks by perceptual classification methods as proposed in [5] and modifies the DCT coefficients of host image as follows.

$$X'_n = \propto_n X_n + \beta_n W_n \qquad (4.1)$$

The $\propto_n$ and β_n coefficients are different for different classes of blocks. X_n are the DCT co-efficient of the host image blocks and W_n are the DCT co-efficients of the watermark image block.

Here, we propose a visible watermarking scheme that modifies gray values of each pixel of the host image. The modification is based on the local as well as global statistics of the host image. The characteristics of the Human Visual System (HVS) are taken into consideration so that the perceptual quality of the image is not very much affected.

4.2 PROPOSED WATERMARKING TECHNIQUE

The steps for watermark insertion are discussed below.

- The original image I (one to be watermarked) and the watermark image W are divided into blocks (both the images may not be of equal size, but blocks should be of equal size).

- μ and σ , the global mean and variance of the image I are computed.

- For each block the local statistics mean μ_n and variance σ_n are computed.

- Let $\mathbf{i}_n$ denote the nth block of original image I ,and $\mathbf{w}_n$ denote the nth block of watermark image W. Denoting the nth block of watermarked image by $\mathbf{i}_{n}$',
  we have,

  $$\mathbf{i}_{n}' = \alpha_n . \mathbf{i}_n + \beta_n \mathbf{w}_n \qquad n = 1,2, \ldots\ldots \qquad (4.2)$$

  where $\propto_n$ and β_n are scaling and embedding factors respectively for each block computed as described below.

Fig.4.0 gives the schematic representation of the insertion process.

The choice of α_n's and β_n's are governed by certain characteristics of Human Visual System (HVS) which for watermark images can be translated into following requirements [72,84-88].

- The edge blocks should be least altered to avoid significant distortion of the image. So one can add only small amount of watermark gray value in the edge block of host image. This means that scaling factor α_n should be close to α_{max} , (the maximum value of the scaling factor) and embedding factor β_n should be close to β_{min} (the minimum value of the embedding factor).
- Its also pointed out in [72,84-88] that blocks with uniform intensity (having low variance) are more sensitive to noise than the blocks with non-uniform intensity (having high variance). So one can add less to the blocks with low variance and

add more to the blocks with high variance. We assume the scaling factor α_n is inversely proportional to variance whereas β_n directly proportional to variance.

- Yet another characteristic of HVS is that the blocks with mid-intensity are more sensitive to noise than that of low intensity blocks as well as high intensity blocks. This means that the α_n should increase with local mean gray value upto mid gray value and again decrease with local mean gray value. The variation of α_n with mean block gray value is assumed to be gaussian in nature. The variation β_n with mean gray value is reverse to that of α_n .

Basing on the above discussion we propose the following mathematical model.

$$\alpha_n = \begin{cases} \alpha_{max} , & \text{for edge blocks} \\ \alpha_{min} + (\sigma_{min} (\alpha_{max} - \alpha_{min})/\sigma_n) \ \exp(- ((\mu_n - \mu)/\sigma)^2 / 2), \\ \qquad\qquad \text{for other blocks} \end{cases} \tag{4.3}$$

$$\beta_n = \begin{cases} \beta_{min} , & \text{for edge blocks} \\ \beta_{min} + (\sigma_n (\beta_{max} - \beta_{min}) / \sigma_{max}) \ [1 - \exp(- ((\mu_n - \mu)/\sigma)^2 / 2)], \\ \qquad\qquad \text{for other blocks} \end{cases} \tag{4.4}$$

Where,
α_{min} and α_{max} are respectively minimum and maximum values of scaling factor,
β_{min} and β_{max} are respectively minimum and maximum values of embedding factor,
σ_{min} and σ_{max} are respectively minimum and maximum values of block variances,
μ_n and σ_n are respectively normalized mean and variance of each block, and
μ and σ are respectively normalized mean & variances of the image.

The above expressions have been validated by experiments. Fig.4.1-Fig.4.4 show the curves for “lena” image.

4.3.IMPLEMENTATION AND RESULTS

The following steps are followed to implement the above proposed algorithm.

- The global mean and variance of the image are found out.

- The image is divided into blocks; block mean and variance are found out. If the watemark size is smaller than the host image then the portion of the image in which the watermark is to be embedded is divided into blocks.

- The block means are properly scaled to range the 0.1 to 1.0.

- The log of the block variances are taken and scaled to the range 0.1 to 1.0.

- The edges of the image are found out using sobel operator. Then the major edge blocks are identified.

- α_n and β_n are found out using (4.3) and (4.4)

- α_n are properly to the range α_{min} to α_{max} and β_n are properly scaled to the range β_{min} to β_{max}. The final values of α_n and β_n are shown in Fig.4.5 & Fig.4.6.

- One can start with any value of α_{min} ,α_{max}, β_{min} , β_{max}. The typical value of α_{min} ,α_{max}, β_{min} and β_{max} are 0.95,0.98,0.05 and 0.17 respectively.

- If needed the values of α_{min} ,α_{max}, β_{min} , β_{max} can be changed after a simple visual inspection or using SNR.

Fig.4.7 shows the watermark image. Fig.4.10 - Fig.4.22 show different watermarked images with different sizes of watermark at different locations.

4.4. MODIFICATIONS TO THE ABOVE TECHNIQUE

One of the drawbacks of the proposed algorithm and also that of the classification schemes proposed in [72,84,87,88] is that they fail for the images that has very less objects and has more uniform area as that of shown in Fig.4.27. In [72,84,87,88] most of the blocks will be classified as one class for this type of images. If our algorithm is applied then for most of the blocks we will have same α_n and β_n as clear from Fig.4.23 and Fig.4.24. So in both the cases it is easy for a digital thief to remove the watermark from the watermarked image. We propose a modification to our above technique as follows.

If α_n values are same for more than 1/3 of the blocks then we generate Gaussian random numbers (Gn) with mean μ (image mean) and variance σ(image variance), and scale to the range 0 to (α_{max} -- α_{min}) /4. Then the random numbers are added to (subtracted from) α_n if they are close to α_{min} (α_{max}). If β_n values are same for 1/3 of the blocks then we scale (1- Gn) to the range 0 to (β_{max} - β_{min})/2. Then the numbers are added to (subtracted from) β_{min} (β_{max}). The modified α_n and β_n are shown in Fig.4.25 and Fig.4.26.The watermarked image is shown in Fig.4.28 and Fig.4.29.

4.5. CONCLUSIONS

A visible watermarking technique has been proposed here. A mathematical model is developed for this purpose exploiting the HVS. We have also proposed a modification to increase the robustness of the watermark when used for images with very few objects. For more robustness watermark should not be publicly available, the watermark should be used in different sizes and should be put in different portions for different images. The watermark may find application in future digital TV, digital libraries and e-commerce.

Proposed Watermarking Technique

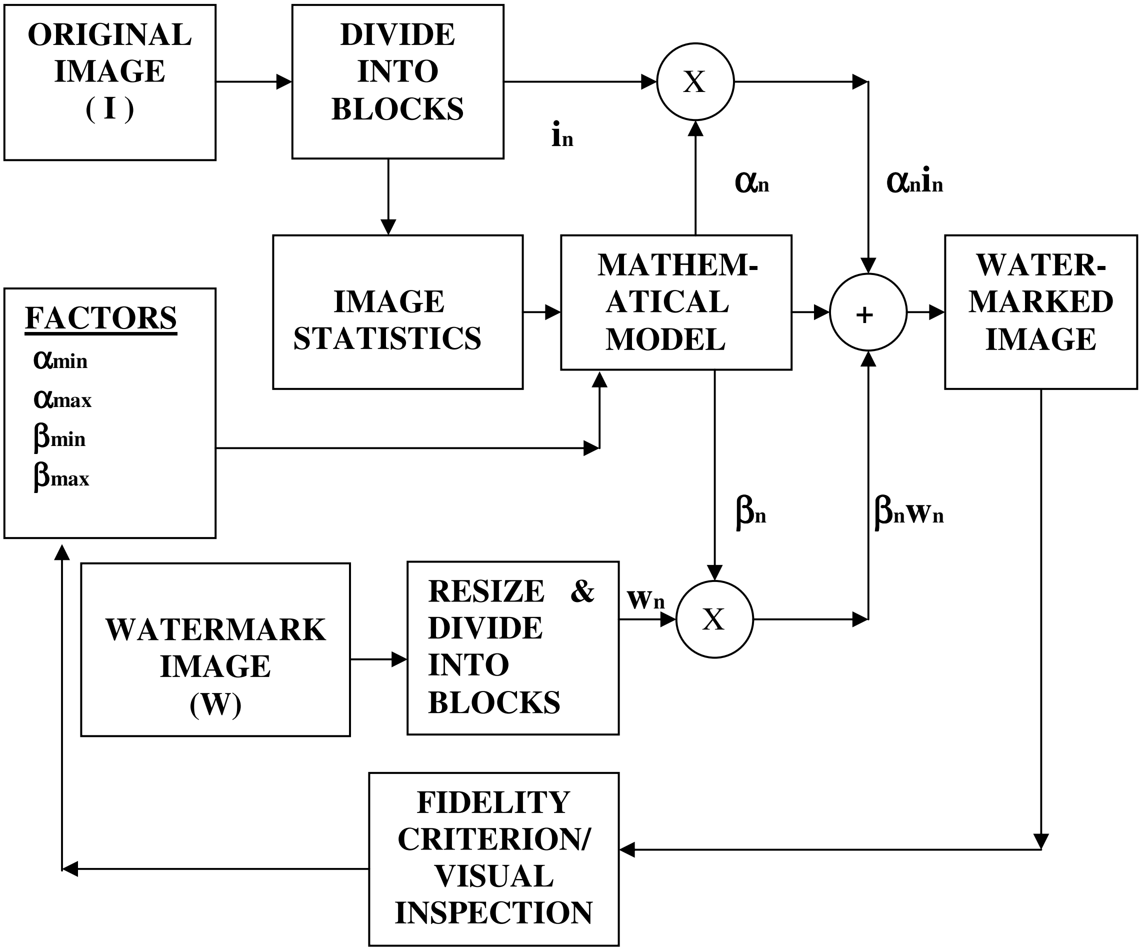


Fig.4.0 Schematic Representation

Fig.1 Variation of embedding factor "beta" with mean for "lena" image

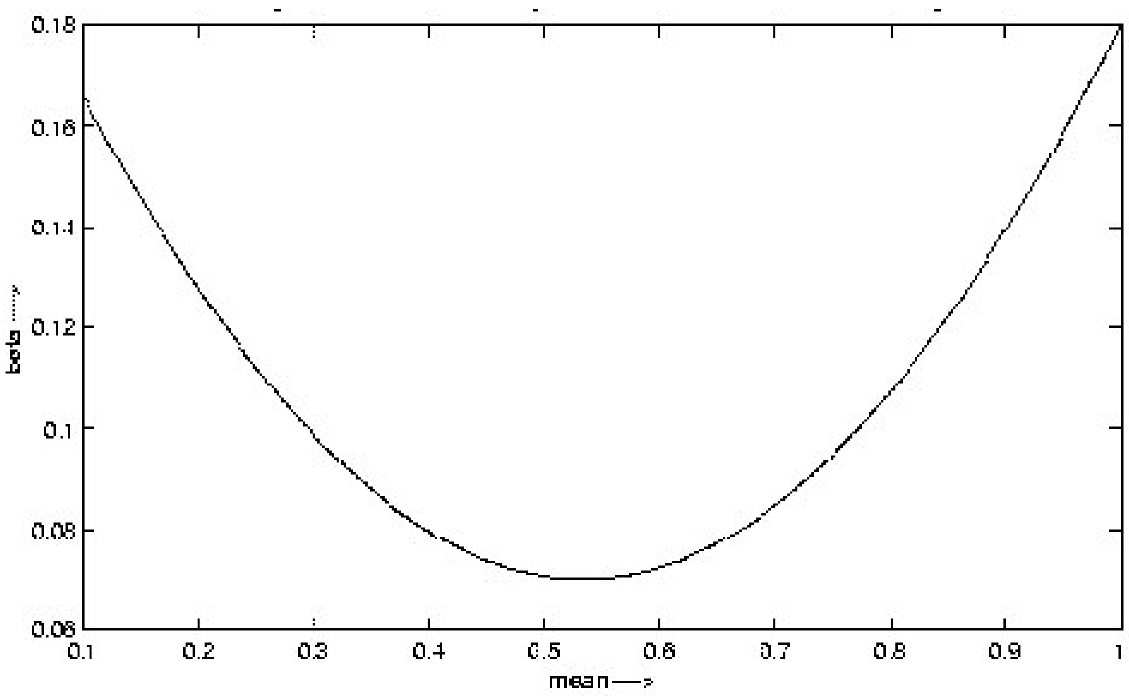


Fig.2 Variation of embedding factor "beta" with variance for "lena" image

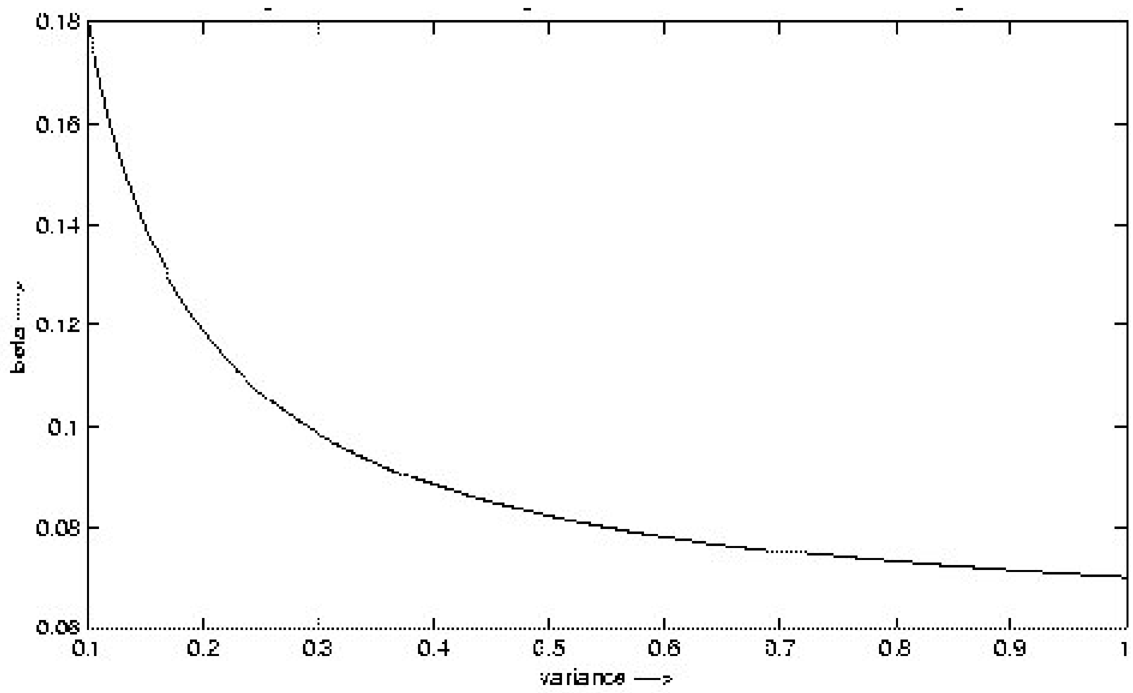


Fig.3 Variation of scaling factor "alpha" with mean for "lena" image

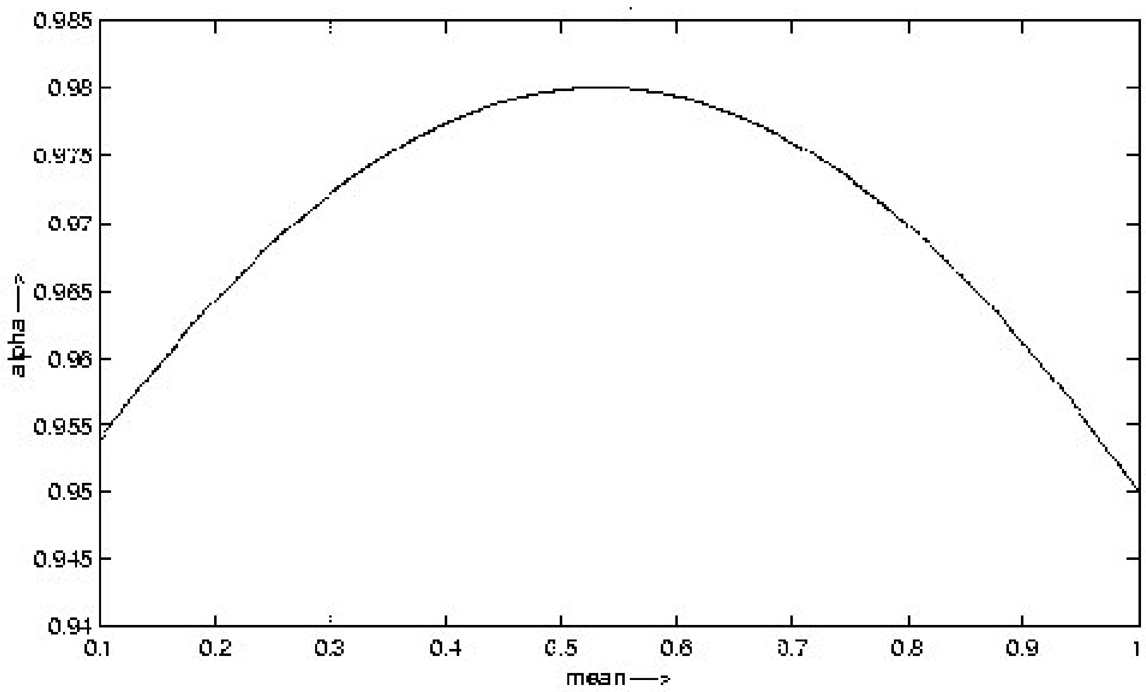


Fig. 4 Variation of scaling factor "alpha" wit variance for "lena" image

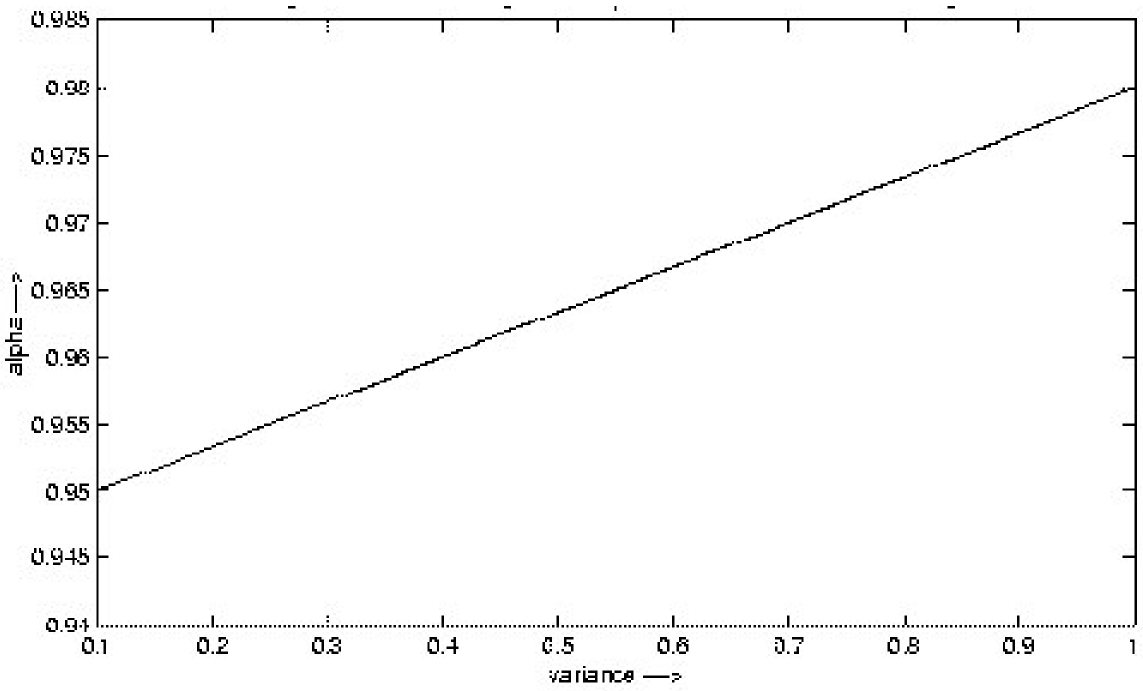


Fig.5 Scaling factor “alpha” for different blocks

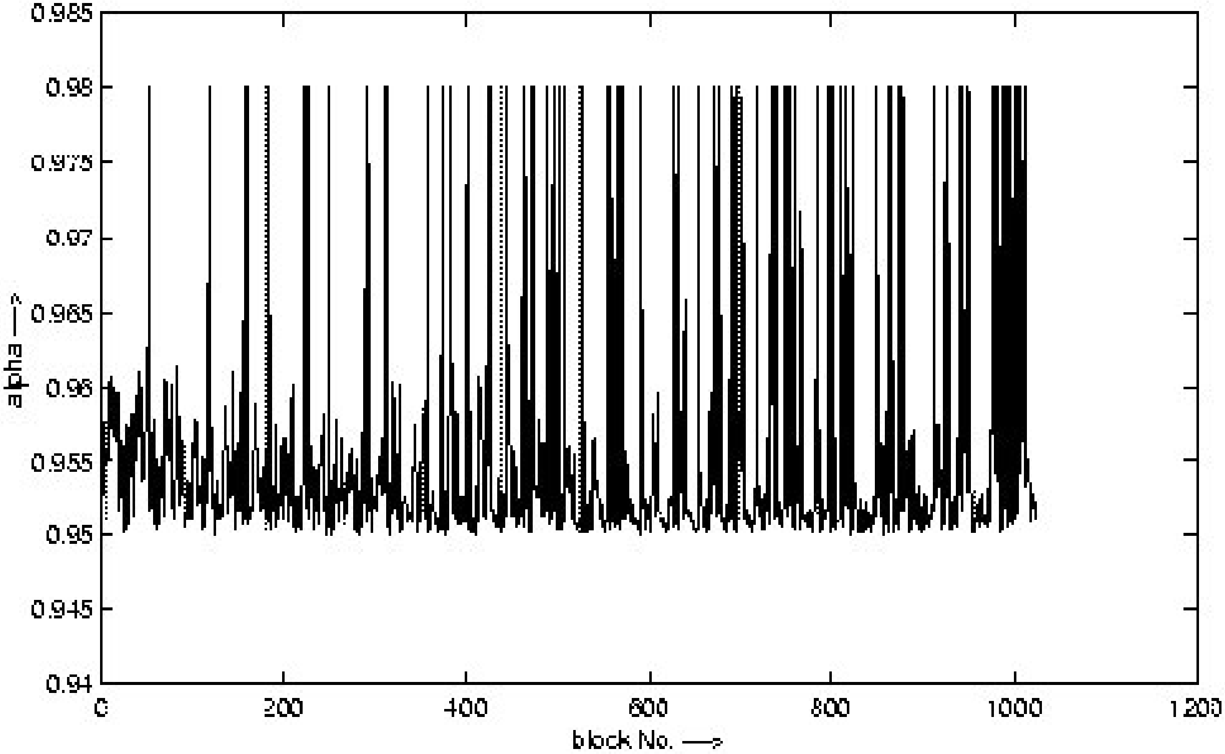
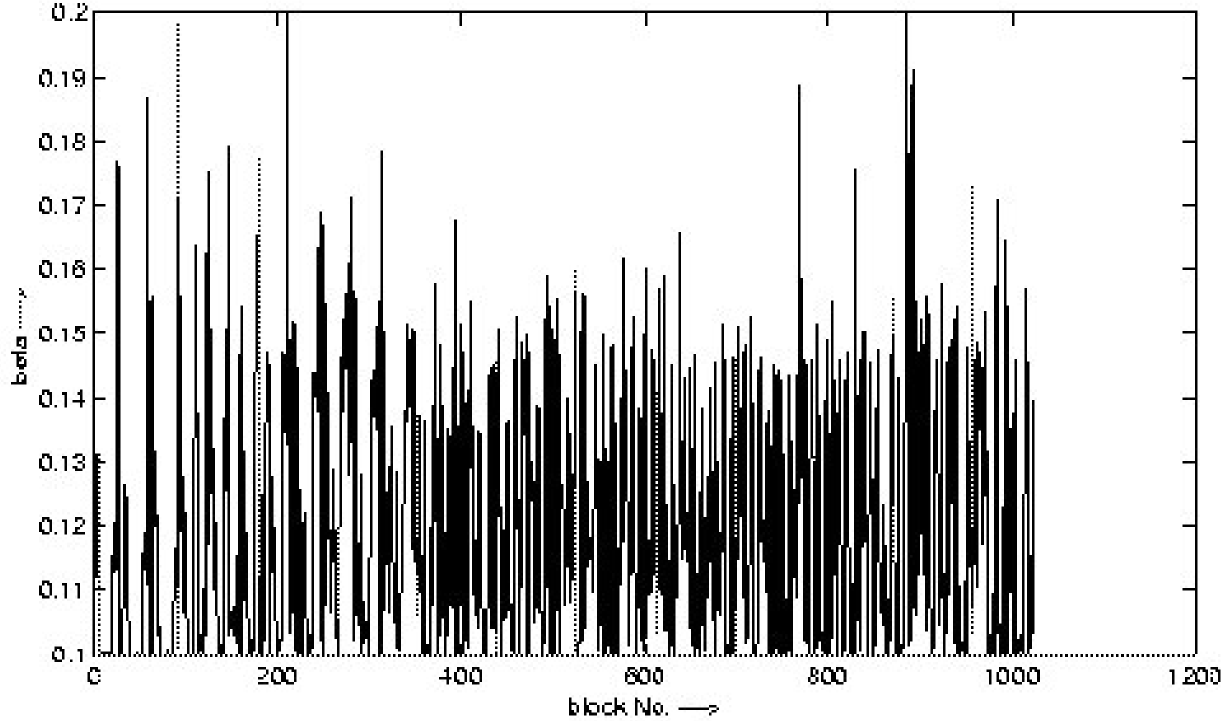


Fig. 6 Embedding factor “beta” for different blocks



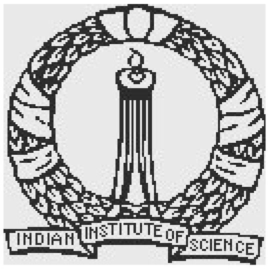


Fig. 4.7 Watermark Image

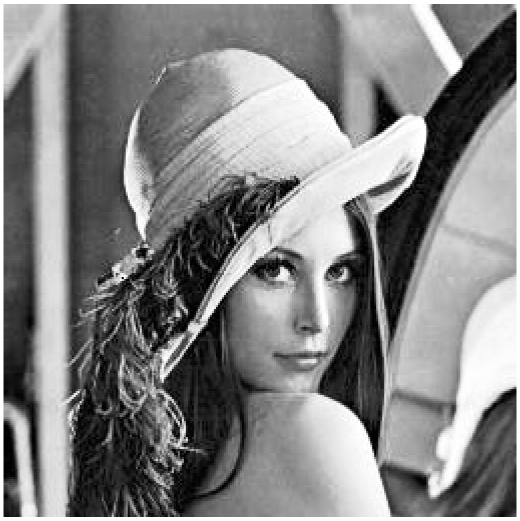


Fig. 4.8 Original "lena" Image

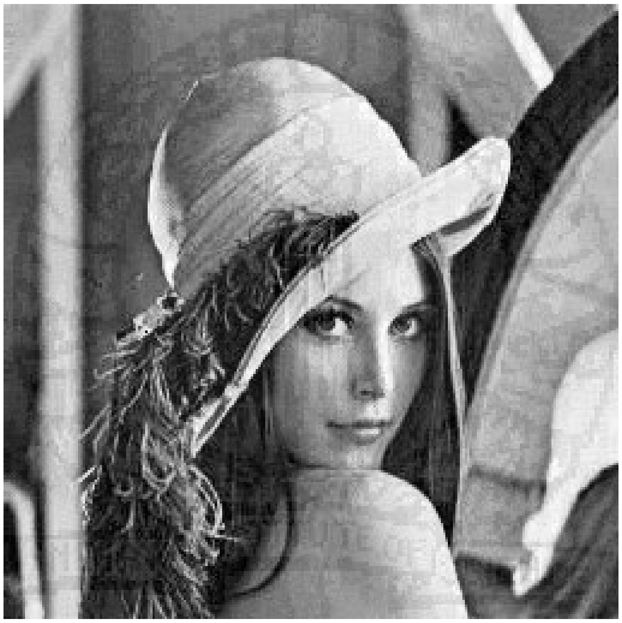


Fig. 4.9 Watermarked "lena" image (Watermark over the whole image)

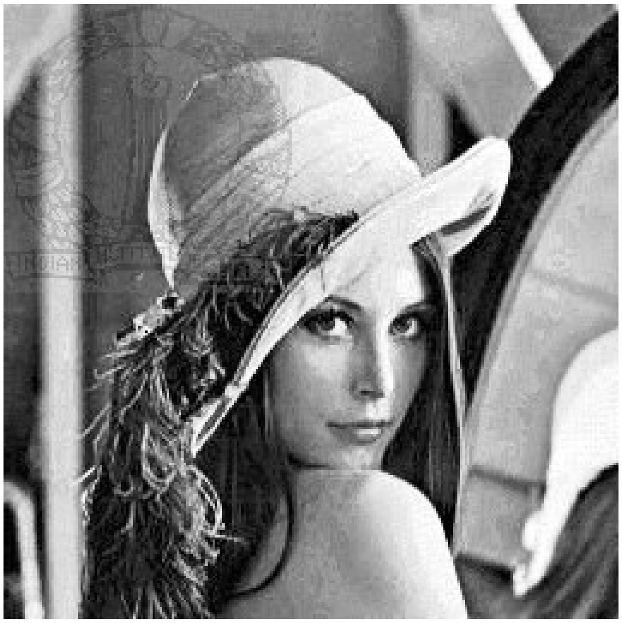


Fig. 4.9 Watermarked "lena" image (Watermark at the corner)

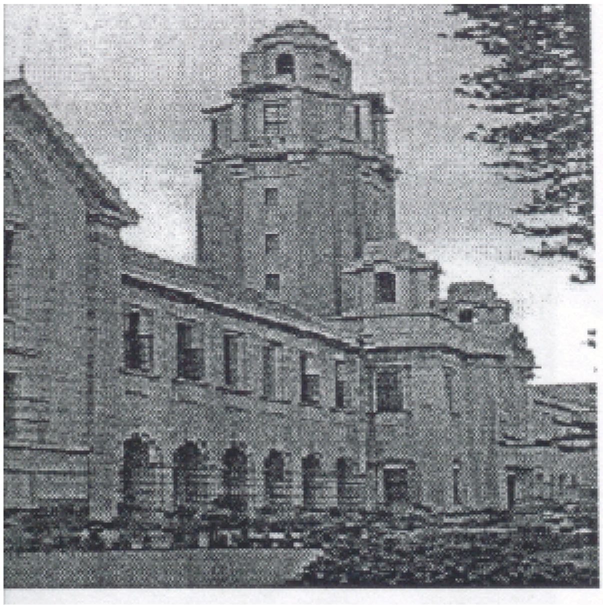


Fig. 4.11 Original “tower” image
***scanned from hardcopy**

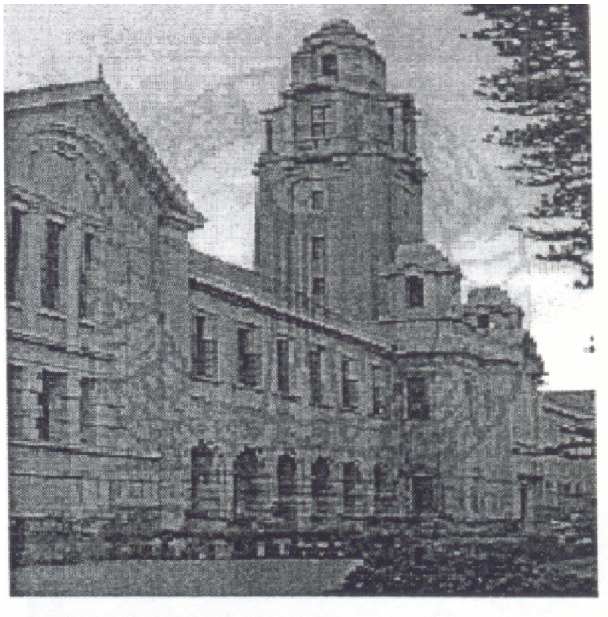


Fig. 4.12 Watermarked “tower” image
(watermark of smaller size)
***scanned from hardcopy**

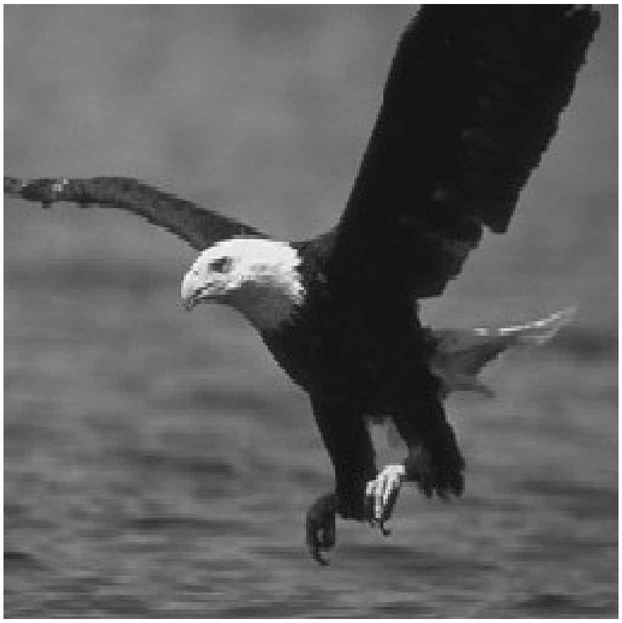


Fig. 4.13 Original “bird” image

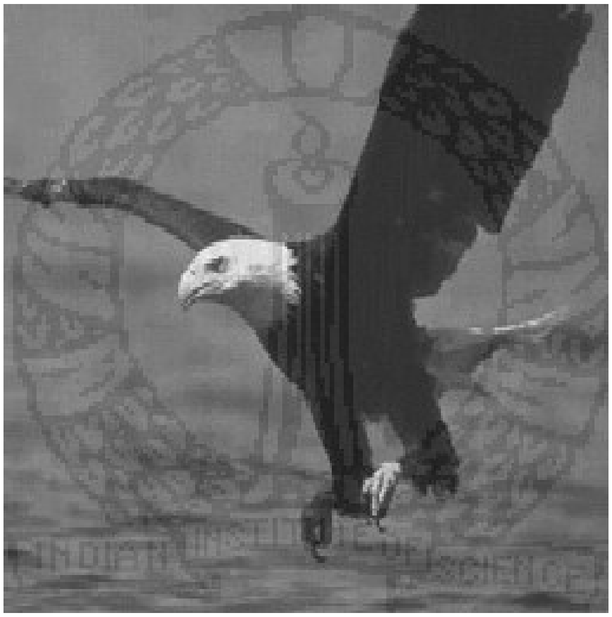


Fig. 4.14 Watermarked “bird” image

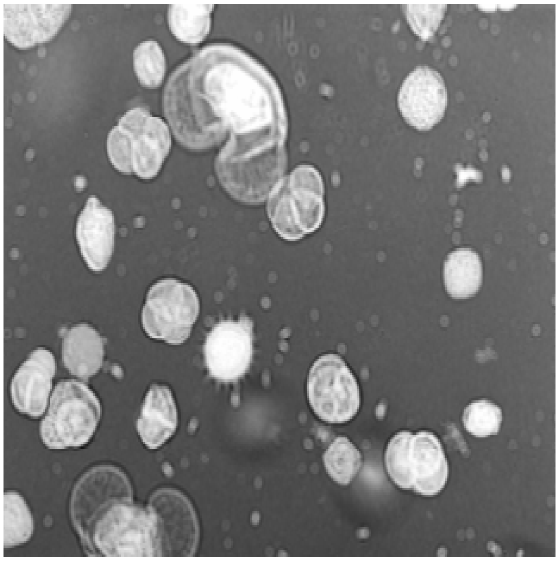


Fig. 4.15 Original "pollen" image

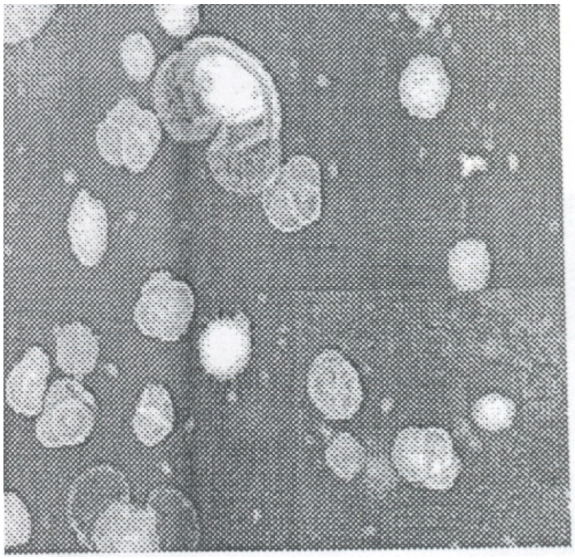


Fig. 4.16 Watermarked "pollen" image
***scanned from hardcopy**

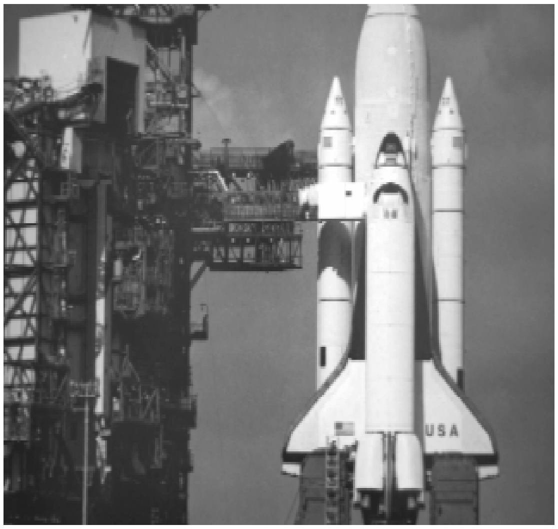


Fig. 4.17 Original "shuttle" image

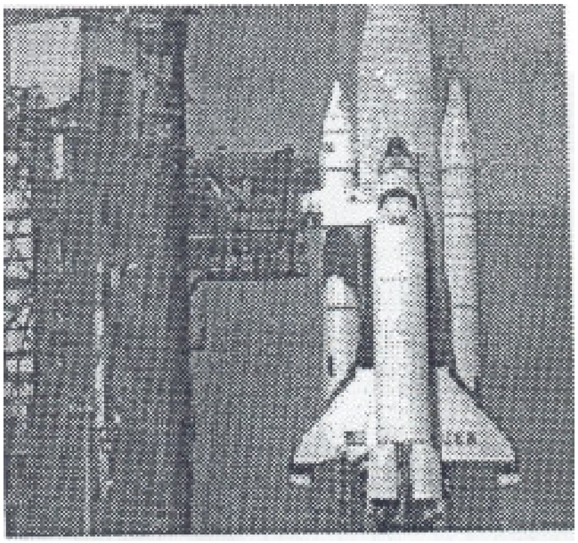


Fig. 4.18 Watermarked "shuttle" image
***scanned from hardcopy**

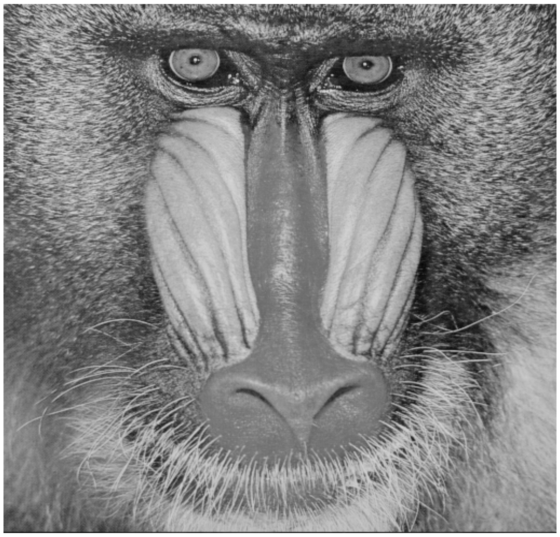


Fig. 4.19 Original “mandrill” image

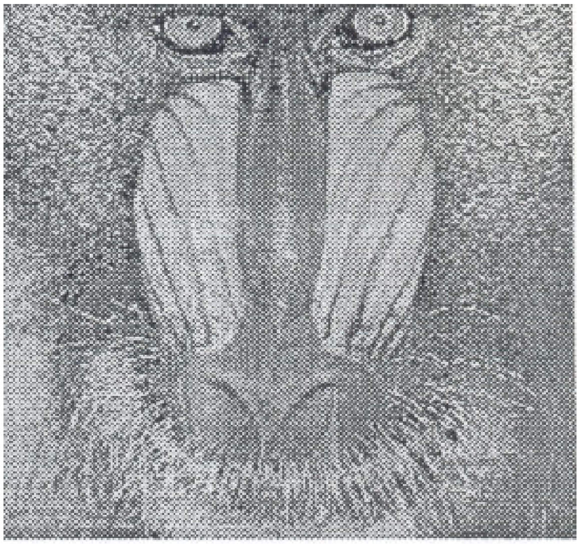


Fig. 4.20 Watermarked “mandrill” image
*scanned from hardcopy

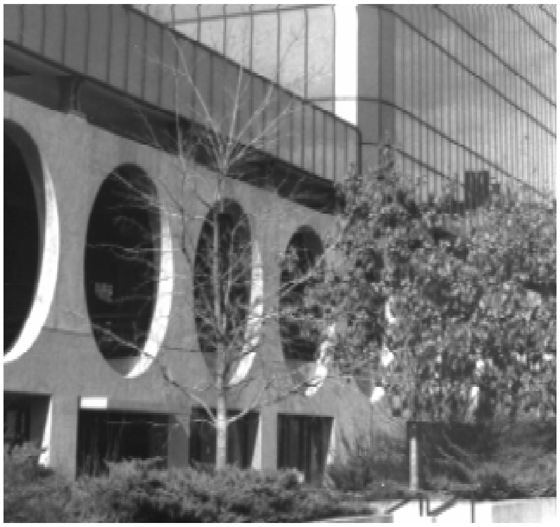


Fig. 4.21 Original “building” image

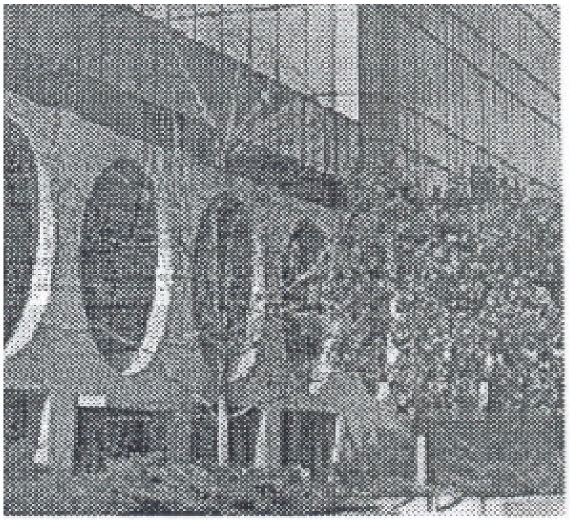


Fig. 4.22 Watermarked “building” image
*scanned from hardcopy

Fig. 4.23 Scaling factor "alpha" for different blocks
***scanned from hardcopy**

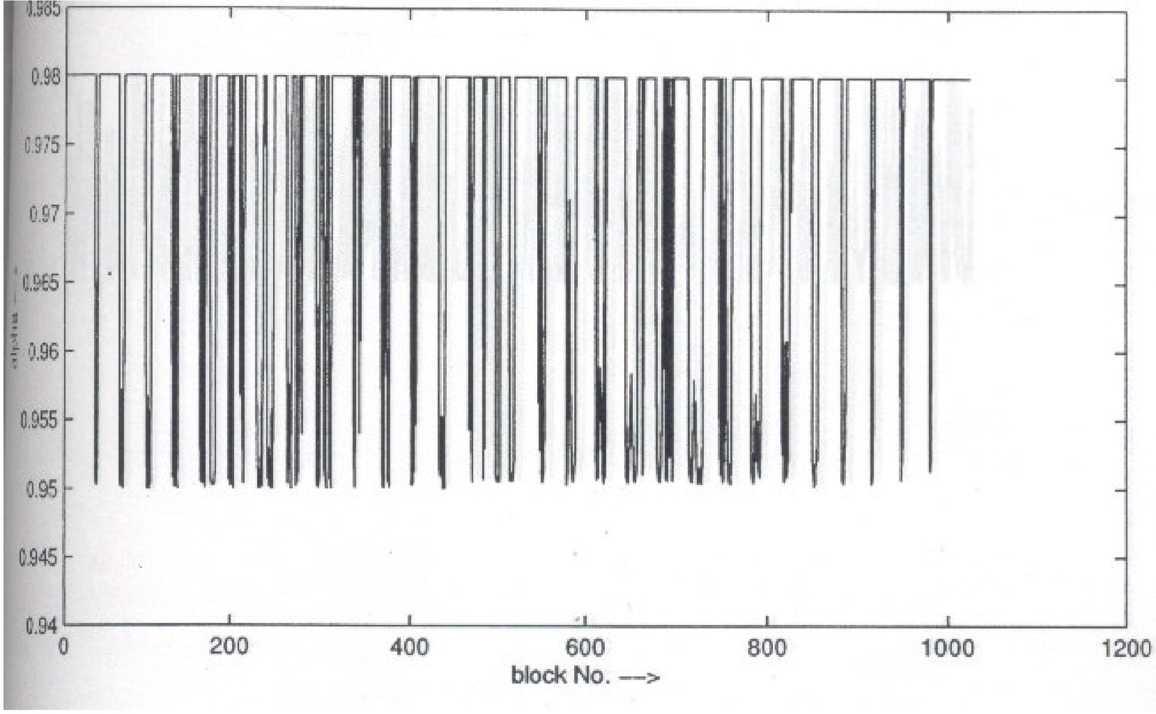


Fig. 4.24 Embedding factor "beta" for different blocks
***scanned from hardcopy**

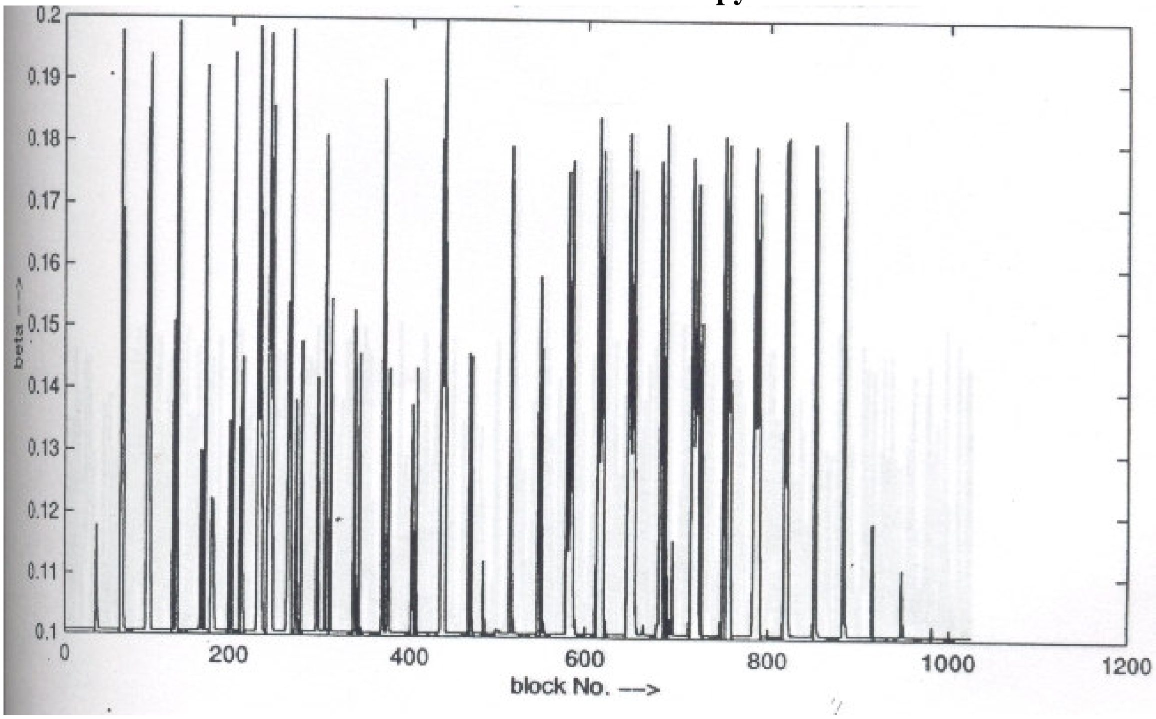


Fig. 4.25 Modified Scaling factor "alpha" for different blocks
***scanned from hardcopy**

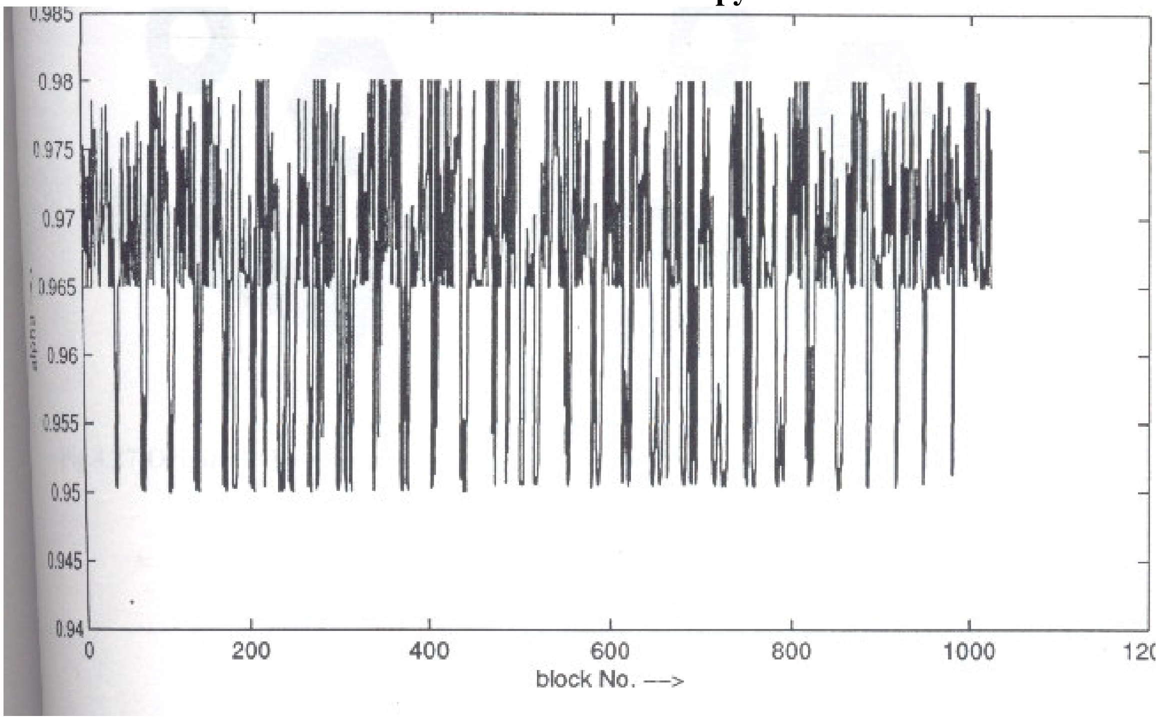
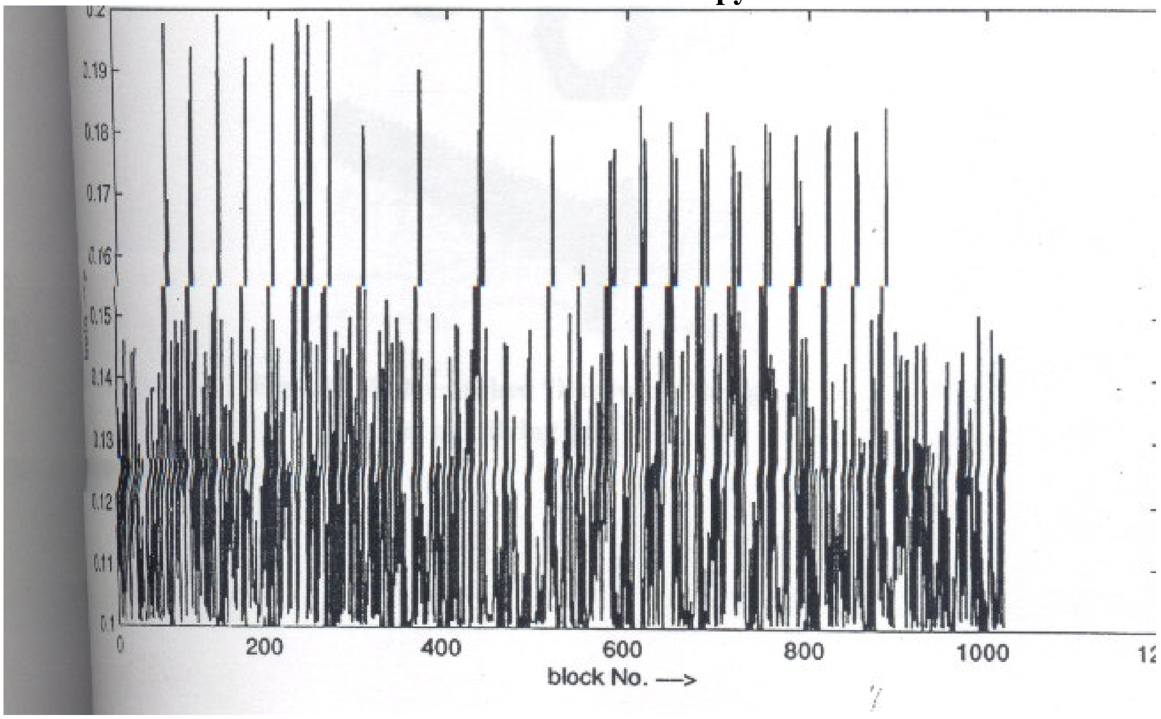


Fig. 4.26 Modified Embedding factor "beta" for different blocks
***scanned from hardcopy**



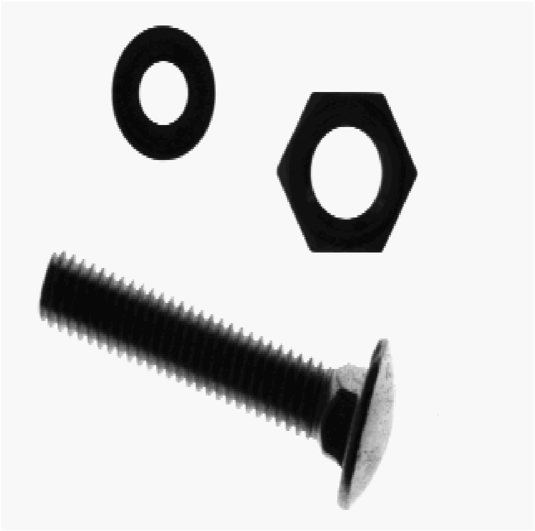


Fig. 4.27 Original "hardware" image

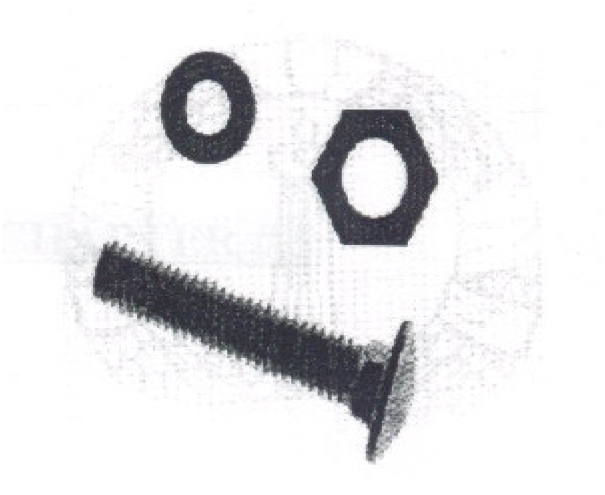


Fig. 4.28 Watermarked "hardware" image (before modifying beta) *scanned from hardcopy

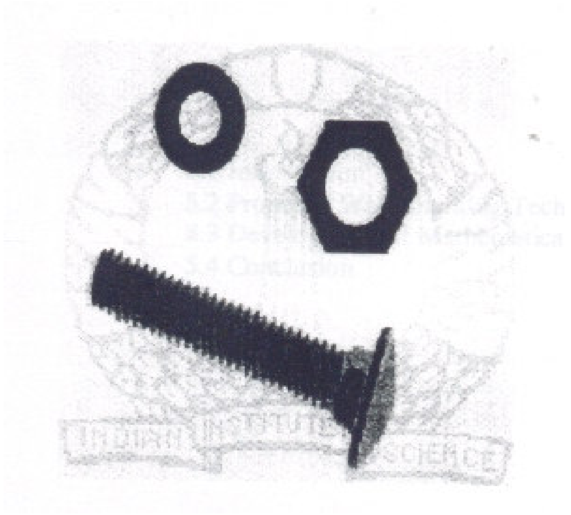


Fig. 4.29 Watermarked "hardware" image (after modifying beta) *scanned from hardcopy

CHAPTER # 5

AN ADAPTIVE VISIBLE WATERMARKING TECHNIQUE FOR IMAGE DATA IN DCT DOMAIN

5.1 INTRODUCTION

We have already discussed in previous chapters, “What is Visible Watermarking?” and “What are the characteristics of it?”. Here, we propose a Visible Digital Watermarking scheme, which may be thought of as an extension of algorithm proposed in chapter # 4 to the DCT domain.

5.2 PROPOSED WATERMARKING TECHNIQUE

The steps for watermark insertion are discussed below.

- The original image I (one to be watermarked) and the watermark image W are divided into blocks of size 8*8. (both the images may not be of equal size).
- For each block of the original image I the mean gray value μ_n is computed.
- The DCT for each block of the original image are found out.
- The DCT of watermark image blocks are found out.
- For AC DCT co-efficient of each original image block, variance σ_n is found out.
- The block means μ_n scaled to the range 0.1 to 1.0.
- The log of the variance σ_n are scaled to the range 0.1 to 1.0.
- The image mean μ is found out which is the mean of block means μ_n.
- Let $\mathbf{i}_n$ denote the nth DCT block of original image I ,and $\mathbf{w}_n$ denote the nth DCT block of watermark image W. Denoting the nth block of watermarked image by $\mathbf{i}_{n'}$, we have,

  $$\mathbf{i}_{n'} = \alpha_n . \mathbf{i}_n + \beta_n \mathbf{w}_n \qquad n = 1,2, \ldots\ldots \qquad (5.1)$$

  where $\propto_n$ and β_n are scaling and embedding factors respectively for each block computed as described. They are computed using eqn. (5.2) and (5.3).
- The $\propto_n$ and β_n are classified and Gaussian random numbers are added (if required) as described in Sec4.4.
- The IDCT of $\mathbf{i}_{n'}$ are found out which give the watermarked image I’.

Fig.5.0 gives the schematic representation of the insertion process.

5.3 DEVELOPMENT OF THE MATHEMATICAL MODEL

The choice of α_n's and β_n's are governed by texture sensitivity of Human Visual System (HVS) as discussed in Sec.2.5. The following factors are considered to develop mathematical model.

.

- The edge blocks should be least altered to avoid significant distortion of the image. So one can add only small amount of watermark gray value in the edge block of host image. This means that scaling factor α_n should be close to α_{max} , (the maximum value of the scaling factor) and embedding factor β_n should be close to β_{min} (the minimum value of the embedding factor).

- The distortion visibility is low when the background has a strong texture In highly textured block, energy tend to be more evenly distributed among the different AC DCT That means AC DCT co-efficient of highly textured blocks have small variances and we can add more to those blocks. So, we assume α_n to be directly proportional to variance σ_n and β_n to be inversely proportional to variance σ_n.

- The blocks with mid-intensity are more sensitive to noise than that of low intensity blocks as well as high intensity blocks. This means that the α_n should increase with local mean gray value upto mid gray value and again decrease with local mean gray value. The variation of α_n with mean block gray value is assumed to be gaussian in nature. The variation β_n with mean gray value is reverse to that of α_n .

Basing on the above discussion we propose the following mathematical model.

$$\alpha_n = \begin{cases} \alpha_{max}\ , & \text{for edge blocks} \\ \alpha_{min} + (\sigma_n\,(\alpha_{max} - \alpha_{min})/\sigma_{max})\ \exp.(\ -(\mu_n - \mu)^2\ /\ 2\ ), & \text{for other blocks} \end{cases} \tag{5.2}$$

$$\beta_n = \begin{cases} \beta_{min}\ , & \text{for edge blocks} \\ \beta_{min} + (\sigma_{min}\,(\beta_{max} - \beta_{min})\ /\ \sigma_n)\ [\ 1 - \exp(-\ (\ \mu_n - \mu)^2 /\ 2)\ ], & \text{for other blocks} \end{cases} \tag{5.3}$$

Where,

α_{min} and α_{max} are respectively minimum and maximum values of scaling factor,
β_{min} and β_{max} are respectively minimum and maximum values of embedding factor,
μ_n is normalized mean of each block,
σ_n are normalized variances of each DCT blocks,
σ_{min} and σ_{max} are respectively minimum and maximum values of DCT block variances,
μ is the normalized image mean.

The above expressions have been validated by experiments. Fig.5.1-Fig.5.4 show the curves for “lena” image.

Fig.5.5 and Fig.5.6 respectively show the α_n and β_n values for different blocks of "lena" image.

5.4 CONCLUSIONS

A visible watermarking technique has been proposed here in DCT domain. A mathematical model is developed for this purpose exploiting the texture sensitivity of the HVS. The typical values of $\alpha_{min,}$ $\alpha_{max,}$ $\beta_{min,}$ and β_{max} are 0.95, 0.98, 0.05 and 0.17 respectively (same as the chapter # 4 algorithm). It is observed that the quality of the watermarked imageis better in this case as compared to the chapter # 4 algorithm. Fig.5.7 – Fig. 5.14 show the different watermark images. For more robustness watermark should not be publicly available, the watermark should be used in different sizes and should be put in different portions for different images. The watermark may find application in digital TV, digital libraries and e-commerce.

Proposed Watermarking Technique

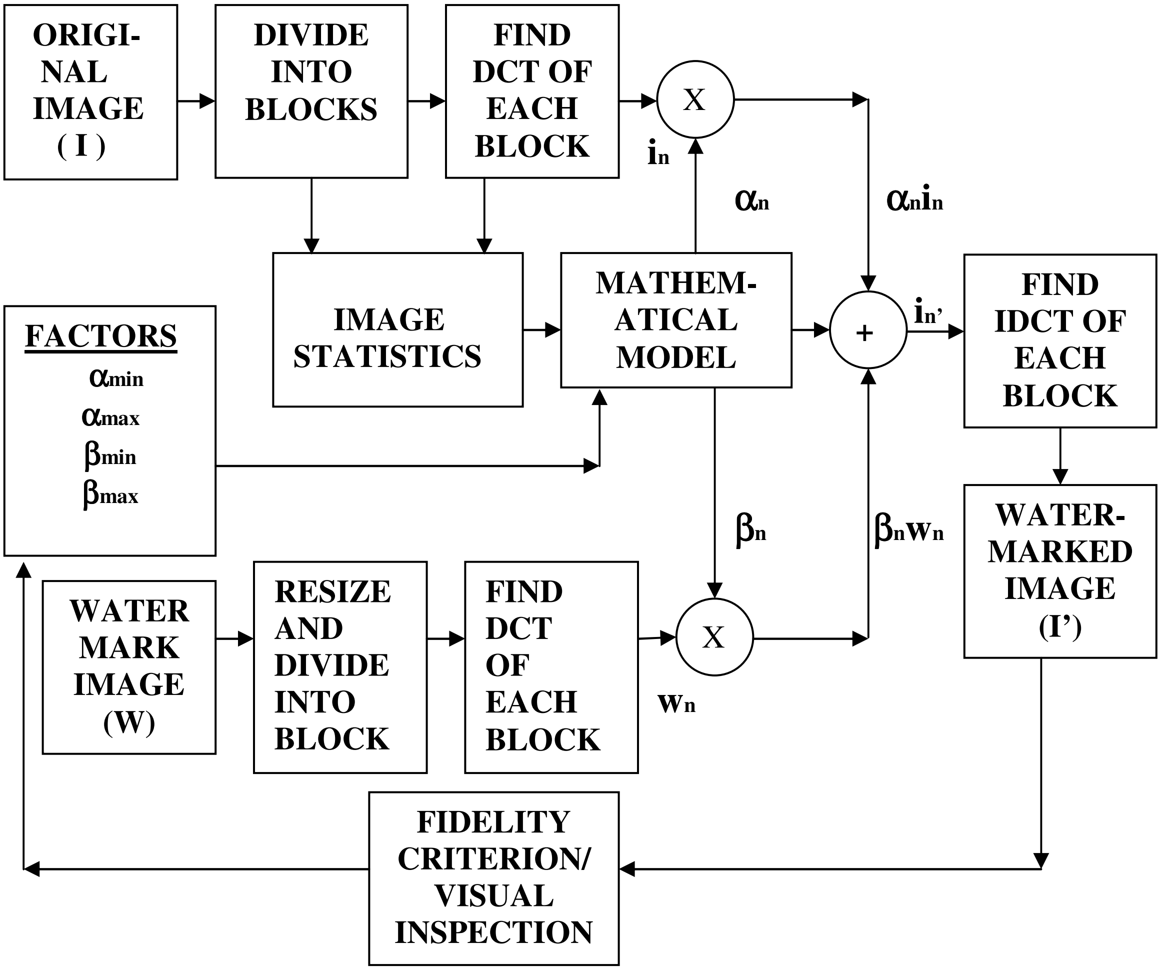


Fig.5.0 Schematic Representation

Fig. 5.1 Variation of scaling factor “alpha” with mean for “lena” image

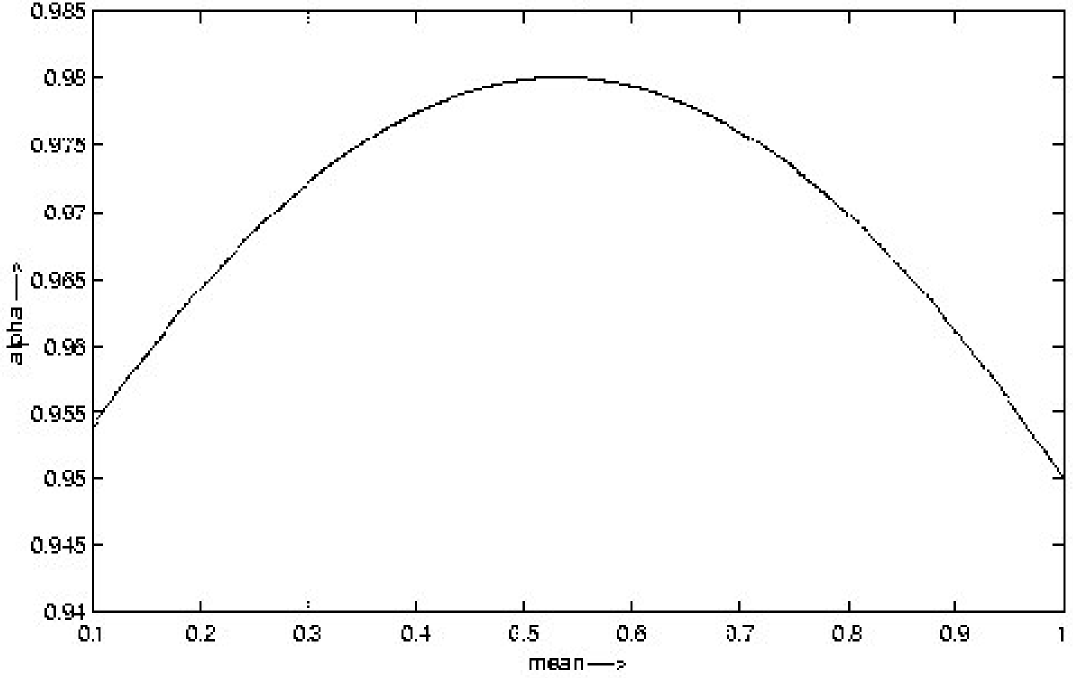


Fig. 5.2 Variation of scaling factor “alpha” with variance for “lena” image

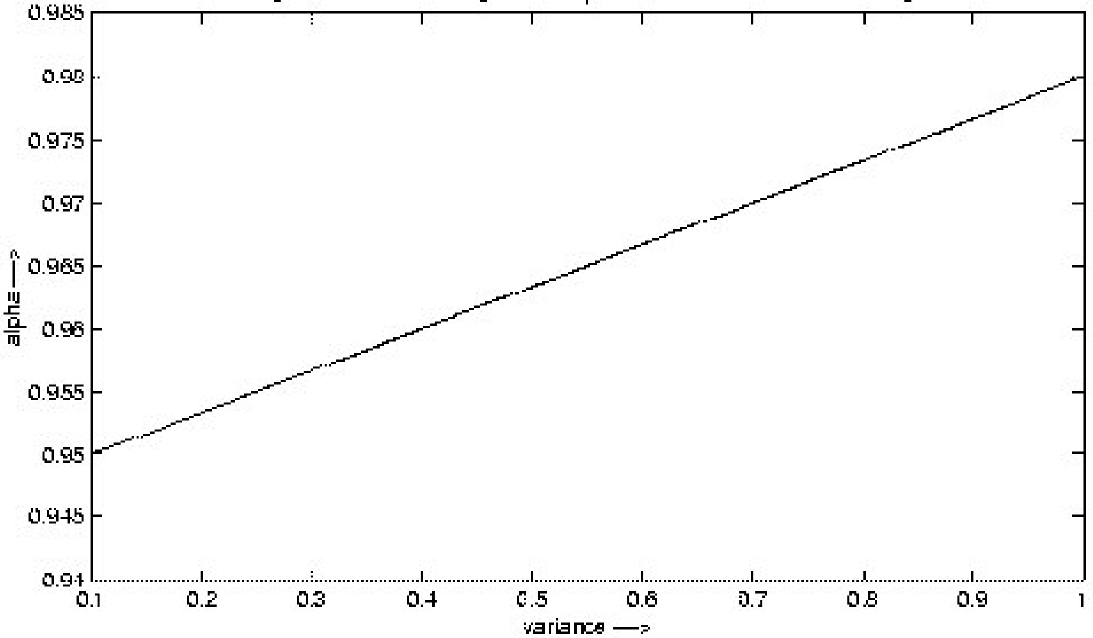


Fig.3 Variation of embedding factor "beta" with mean for "lena" image

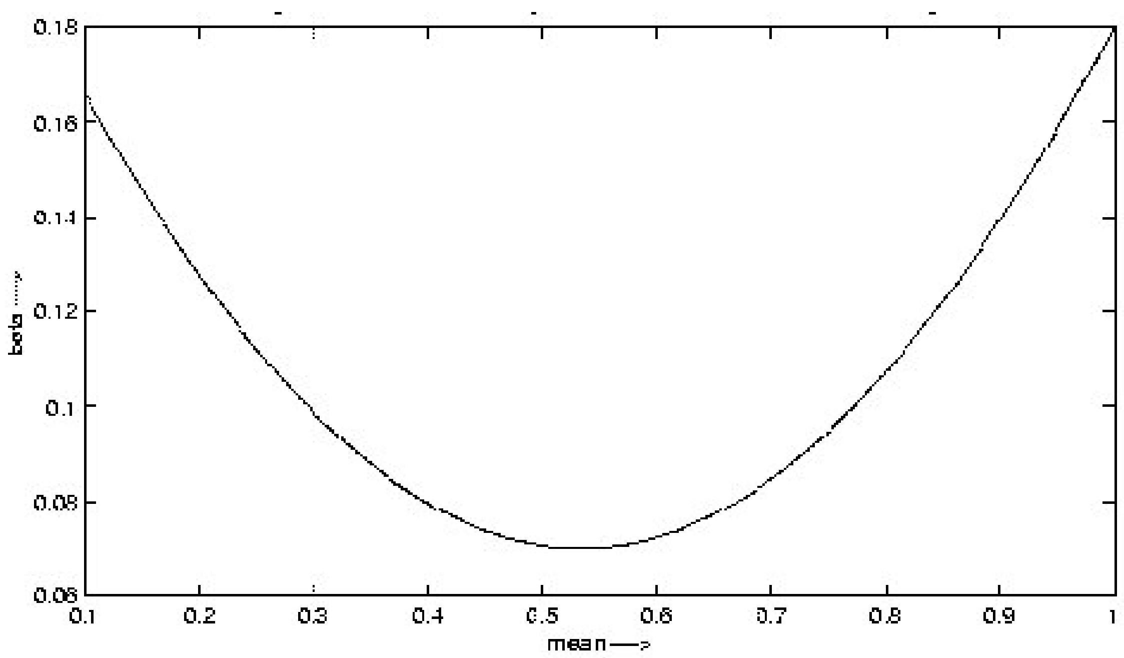


Fig. 4 Variation of embedding factor "beta" with variance for "lena" image

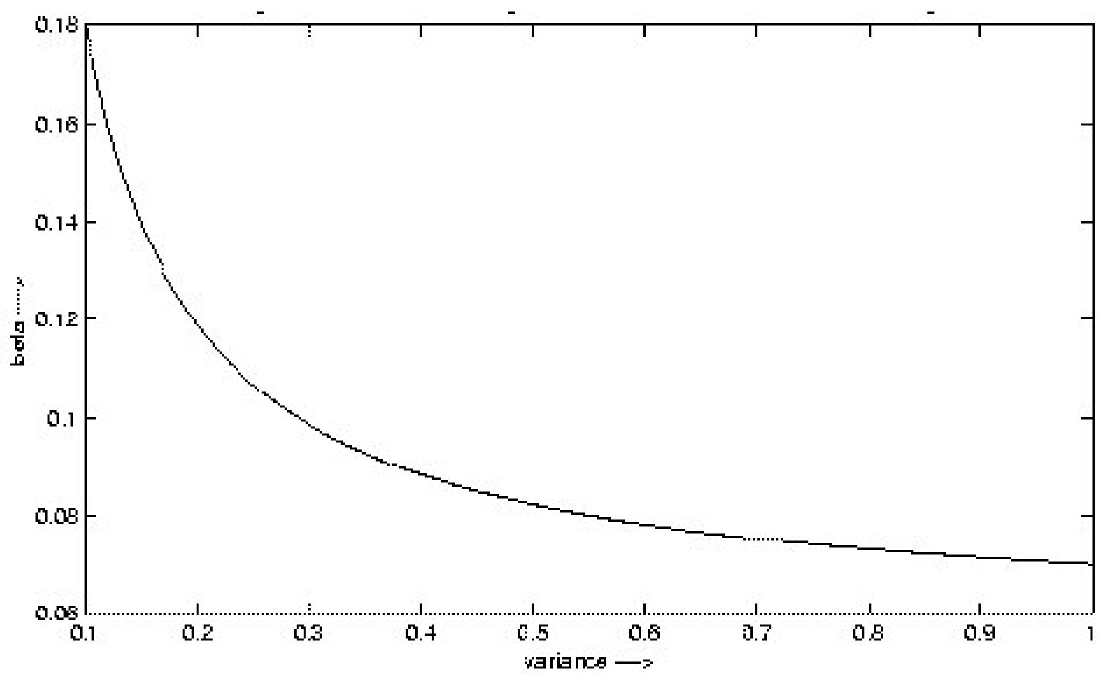


Fig. 5.5 Scaling factor “alpha” for different blocks for “lena” image
***scanned from hardcopy**

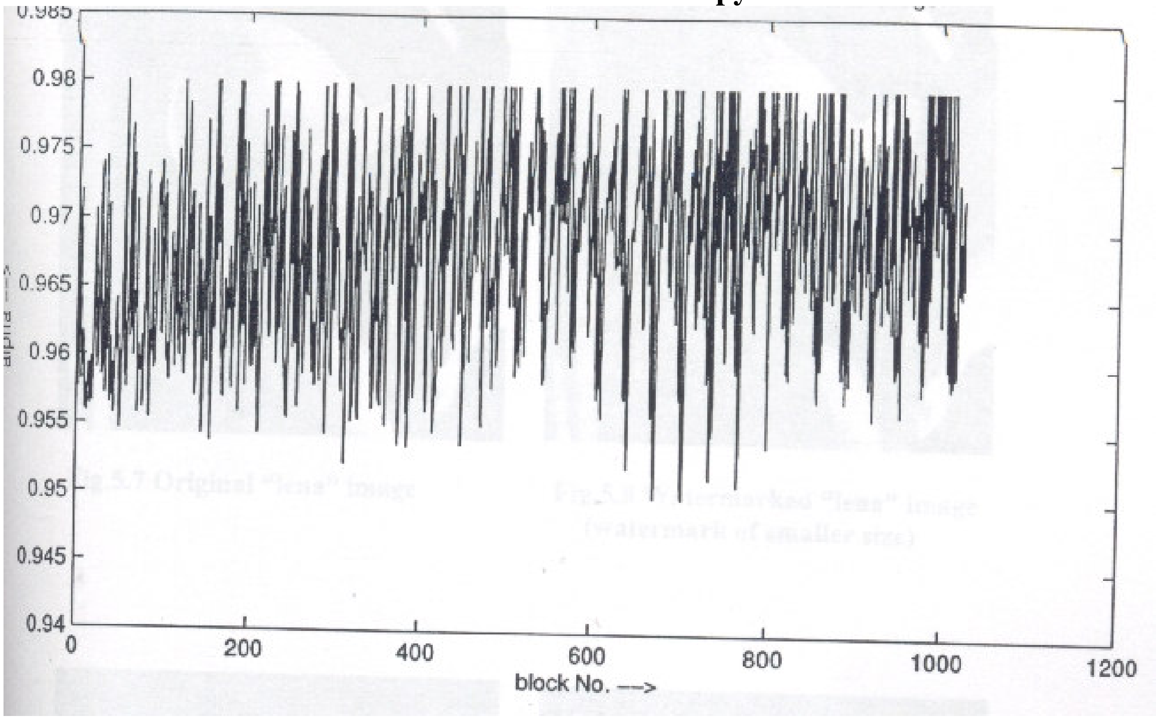
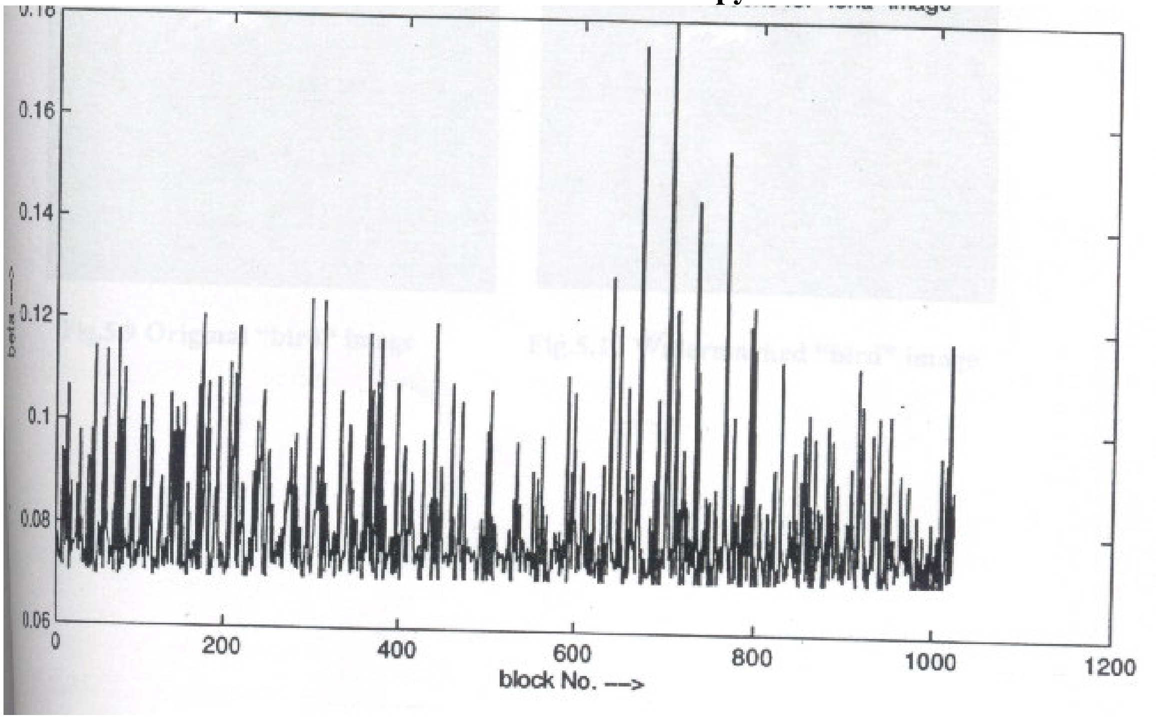


Fig. 5.6 Embedding factor “beta” for different blocks for “lena” image
***scanned from hardcopy**



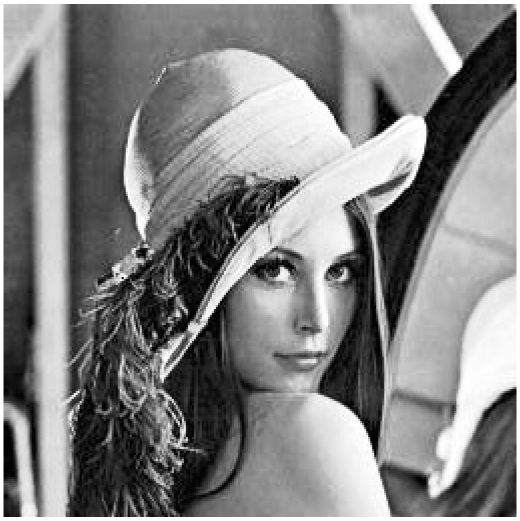


Fig. 5.7 Original “lena” image

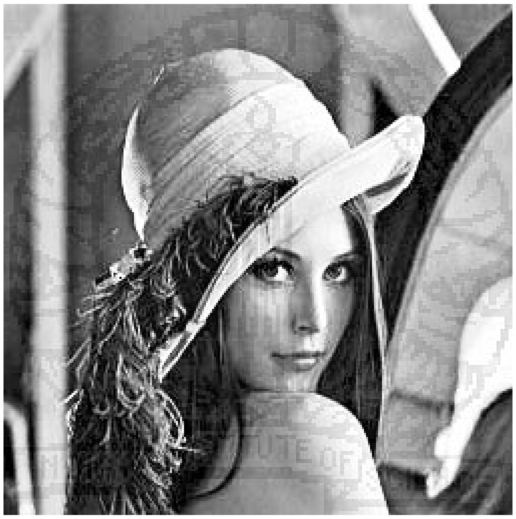


Fig. 5.8 Watermarked “lena” image

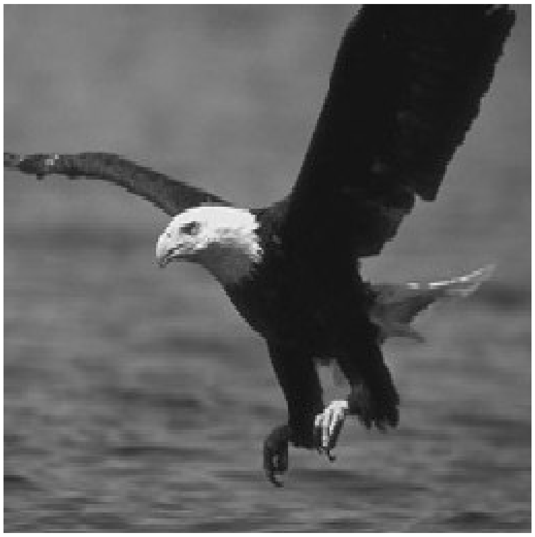


Fig. 5.9 Original “bird” image

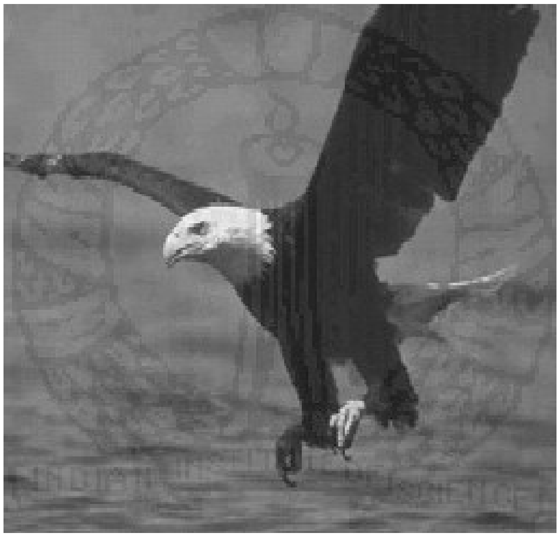


Fig. 5.10 Watermarked “bird” image

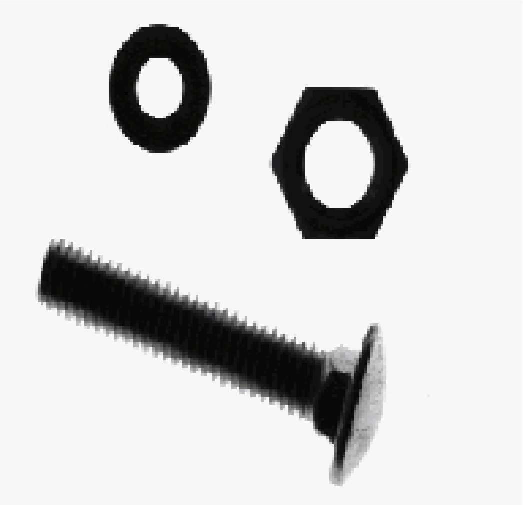


Fig. 5.11 Original "hardware" image

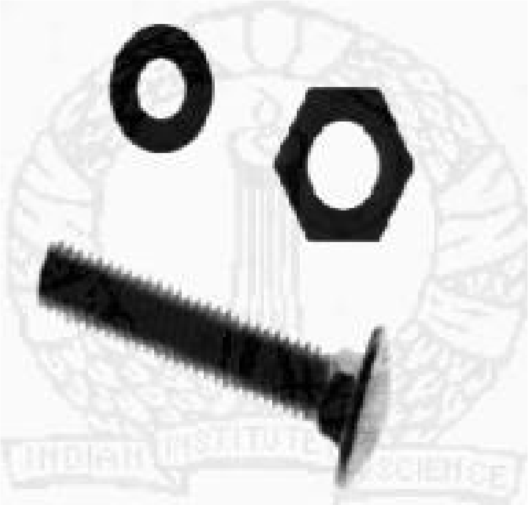


Fig. 5.12 Watermarked "hardware" image

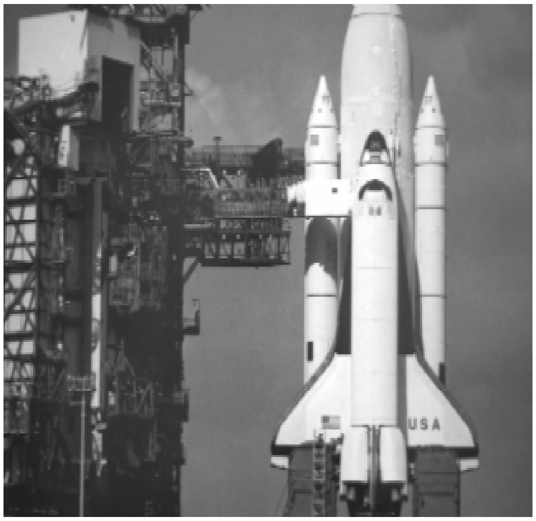


Fig. 5.13 Original "shuttle" image

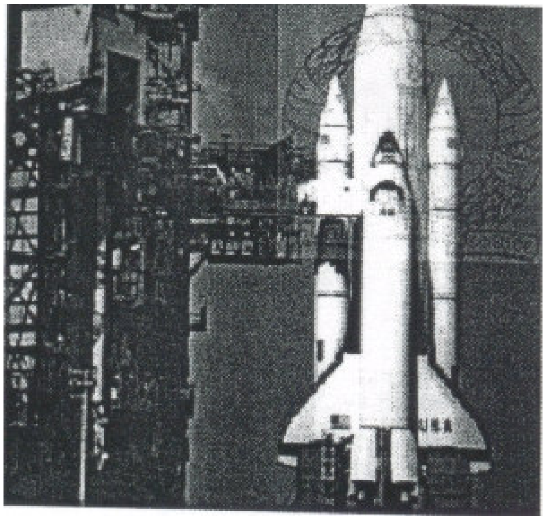


Fig. 5.14 Watermarked "shuttle" image
*scanned from hardcopy

CHAPTER # 6

AN INVISIBLE IMAGE WATERMARKING TECHNIQUE IN SPATIAL DOMAIN

6.1 INTRODUCTION

We have already discussed (in Chapter #1) "What is invisible watermarking?" and "What are the desired characteristics of Invisible Watermarking?" We have also discussed (in Chapter #3) different watermarking algorithms proposed for digital images in spatial domain. Here, we propose an invisible watermarking algorithm. The algorithm can be thought of as extension of [42] or [43] or [44]. The scenario is like this: Schyndel et. al [42] add m-sequence on the LSB of the image data and identify the watermark by computing the spatial cross-correlation function of the sequence and the watermarked image. Wolfgang et. al [43] and [44] propose the watermark, which is a 2-dimensional extension of [42].

6.2 WATERMARK INSERTION

Following are the steps for watermark insertion:

(1) The image bit planes are found out.

(2) Pseudo-random binary sequences or m-sequences {0,1} of period n are generated using a linear feedback shift register. The period n is equal to the number of pixels of the image. It should be noted that $n = 2^m - 1$, m being number of bits, cells or flip-flops of the shift register.

(3) The watermark is generated by arranging the binary sequence into suitable blocks of size 4x4 or 8x8. The size of the watermark is same as the size of the image.

(4) We start from bit-plane i = 0 (for MSB plane) of the image.

(5) The watermark is EXCLUSIVE-ORed with this bit-plane i of the image. This gives a bit-plane for watermarked image.

(6) The watermarked bit-plane found above and the remaining unwatermarked bit-planes of the original image are merged to find the watermarked image.

(7) The SNR is found out.

(8) If, SNR > 20dB, then we stop; otherwise we go to the next lower bit-plane with i incremented by 1. Then we go to (5).

(9) If, i = 7 (for LSB Plane) we stop. But it has been found out that for most of the images i= 4.

Fig6.1 - Fig6.8 show different watermarked images.

6.3 m-SEQUENCES AS WATERMARK

The m-sequences with large periods have excellent randomness and correlation properties [33], [35], [83] and [91].

The watermark using m-sequences has certain advantages [43].

- If an authorized (who doesn't try to tamper the watermark) user knows the watermark, the exact original image can be obtained.
- If an attacker tries to tamper the watermark, he only succeeds in swapping the m-sequence without affecting the correlation properties.
- The techniques used are all compatible with hardware implementation. Such implementation would be capable of on-line, real-time algorithm execution.

6.4 WATERMARK DETECTION

For watermark detection we use the same technique that has been suggested in [43] and [44]

.

The spatial cross-correlation function of images X and Y is defined as:

$$R_{xy}(\alpha,\beta) = \sum_i \sum_j X(i,j)\, Y(i-\alpha,j-\beta) \qquad (6.1)$$

Let X be the original image block, W be the watermark block, Y be the watermarked image block and Z be the watermarked image block that might be forged. The test statistic for the block, δ is defined as:

$$\delta = R_{yw}(0,0) - R_{zw}(0,0) \qquad (6.2)$$

The average δ for all blocks is obtained as given below.

$$E[|\delta_k|] = 1/N \sum_k \delta_k \qquad (6.3)$$

where, δ_k is the value of δ for kth block, and N is the number of blocks.

After tampering the watermarked image in various ways using the algorithm given in XV software and MATLAB. We establish a testing paradigm. The value of $E[|\delta|]$ after different operations is given in Table6.1. The data are for "lena" image with watermark block size 4x4, SNR = 24dB. The watermark is being inserted in 5th bit-plane. (The watermarked was initially snapped using "Capture-Screen" software of HP workstation and was saved in "tif" format.)

TABLE 6.1

SL. No.	OPERATIONS	E[|δ|]	REMARKS
1	JPEG Compression, Q.F – 100%	6.33789	Identical
2	JPEG Compression, Q.F – 50%	12.6685	Identical
3	JPEG Compression, Q.F – 25%	16.7988	Identical
4	3 x 3 blur, JPEG Compression, Q.F – 25%	24.5310	Identical
5	5 x 5 blur, JPEG Compression, Q.F – 25%	35.5872	Heavily blurred
6	25% sharp, JPEG Compression, Q.F – 25%	17.2371	Identical
7	50% sharp, JPEG Compression, Q.F – 25%	27.8308	Identical
8	75% sharp, JPEG Compression, Q.F – 25%	43.1770	Too sharp
9	3 x 3 spread, JPEG Compression, Q.F – 25%	71.3774	Unrecognizable
10	Pixel size 2 x 2, JPEG Compression, Q.F – 25%	21.7539	Identical
11	Pixel size 4 x 4, JPEG Compression, Q.F – 25%	32.1846	Almost unreco.
12	Pixel size 6 x 6, JPEG Compression, Q.F – 25%	65.1899	Unrecognizable
13	3 x 3 Median filter, JPEG Comp., Q.F. – 25%	22.4087	Identical
14	5 x 5 Median filter, JPEG Comp., Q.F. – 25%	28.5247	Blurred
15	7 x 7 Median filter, JPEG Comp., Q.F. – 25%	35.9729	Too blurred
16	11 x 11 Median filter, JPEG Comp., Q.F – 25%	51.6985	Unrecognizable
17	Gaussian Noise, Mean = 0.0, Variance – 0.01	40.1984	Identical
18	Gaussian Noise, Mean = 0.0, Variance – 0.02	56.2318	Too noisy
19	Gaussian Noise, Mean = 0.0, Variance – 0.04	79.2969	Too noisy
20	JPEG Compression , Q.F. – 100% in MATLAB	8.80591	Identical

The testing paradigm can be established as follows:

- If E[|δ|] < 9.0 watermarked image under test is perceptually identical to the original watermarked image. It is fully authentic.

- If 9.0 <= E[|δ|] < 50, watermarked image under test is forged. It is authentic.

- If 50.0 <= E[|δ|] <= 70, watermarked image under test is heavily forged. It is authentic.

- If E[|δ|] > 70.0, watermarked image under test doesn’t belong to owner or severely tampered.

6.5 COMPARISION WITH OTHER ALGORITHMS

We have already mentioned in Sec.6.1 that the algorithm proposed here may be thought of as an extension of [42] or [43] or [44]. The comparison data of E[|δ|] values are tabulated in Table6.2.

TABLE 6.2

SL. No	$E[\|\delta\|]$ for proposed algo.	$E[\|\delta\|]$ for [44]	Remarks
1	< 9.0	< 10.0	Fully authentic
2	9.0 – 50	10.0 – 100.0	Authentic, forged
3	50.0 – 70.0	100.0 – 200.0	Authentic, heavily forged
4	> 70.0	> 200.0	Severely forged or doesn’t belong to the owner

It is clear from Table 6.2 that the ranges of values of $E[|\delta|]$ for the proposed algorithm is smaller than that proposed in [44]. This shows that the proposed algorithm is robust than that proposed in [44].

6.6 CONCLUSIONS

We propose here an invisible, robust watermarking scheme for copyright protection of the digital images. The algorithm works for both gray and color images. It is capable of authenticating the watermarked image as well as determining if it has been tampered. The algorithm is robust to various signal processing applications like JPEG compression, linear as well as median filtering, sharpening and addition of noises.

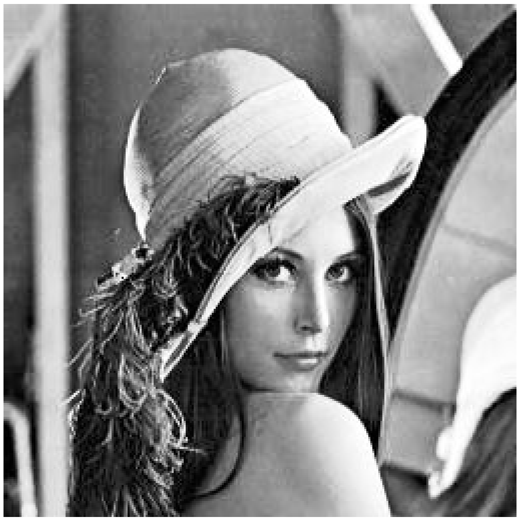


Fig. 6.1 Original “lena” image

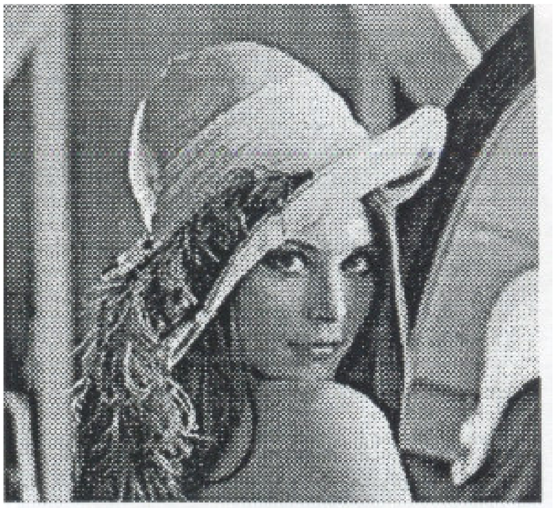


Fig. 6.2 Watermarked “lena” image
(block size = 4x4, i=4, SNR = 24dB)
*scanned from hardcopy

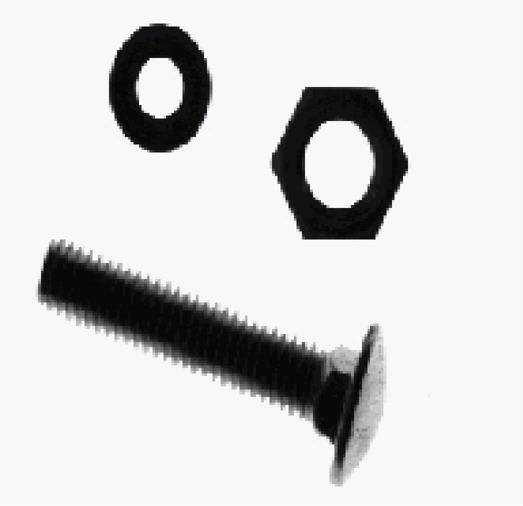


Fig. 6.3 Original “hardware” image

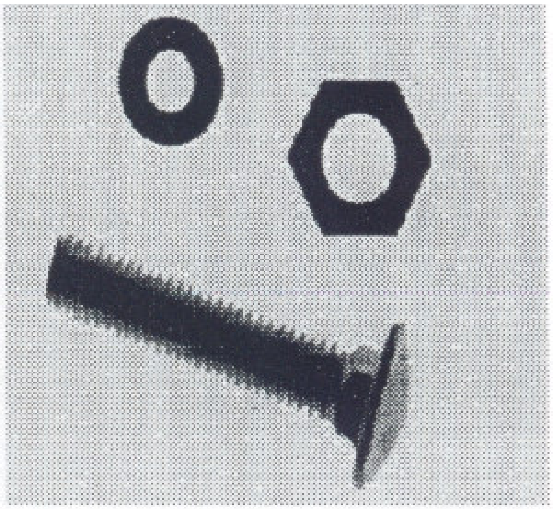


Fig. 6.4 Watermarked “hardware” image
(block size = 4x4, i=4, SNR = 25dB)
*scanned from hardcopy

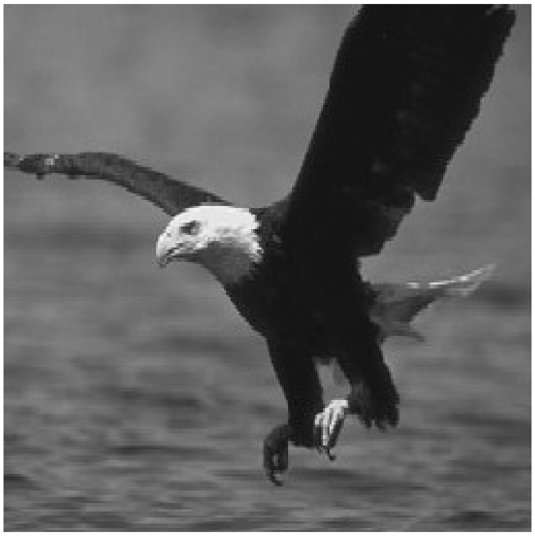


Fig. 6.5 Original "bird" image

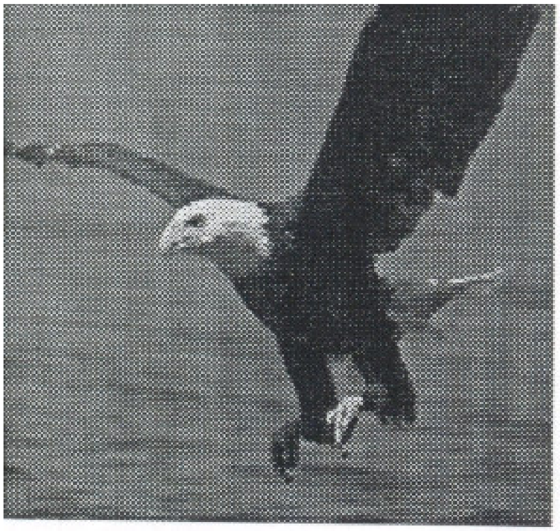


Fig. 6.6 Watermarked "bird" image (block size = 4x4, i=4, SNR = 24dB) *scanned from hardcopy

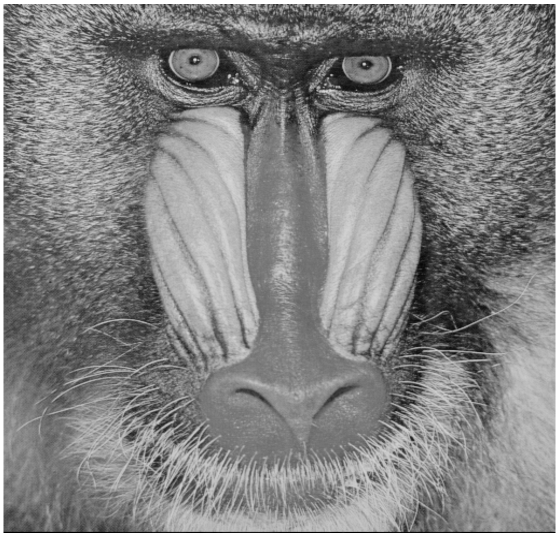


Fig. 6.7 Original "mandrill" image

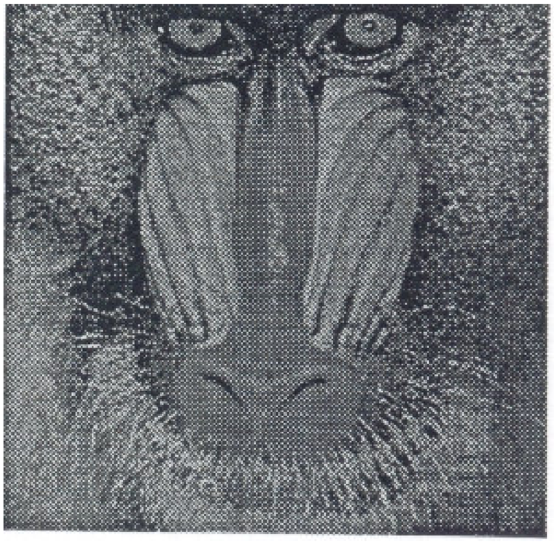


Fig. 6.8 Watermarked "mandrill" image (block size = 4x4, i=4, SNR = 20dB) *scanned from hardcopy

CHAPTER # 7

A SPREAD SPRECTRUM WATERMARKING TECHNIQUE FOR DIGITAL IMAGES

7.1 INTRODUCTION

We have already discussed what an invisible watermark is and what are its desired characteristics. We have also reviewed various invisible watermarking algorithms proposed in frequency domain (Chapter # 3). The watermarking technique proposed in the chapter is analogous to spread spectrum communication (already discussed in Sec.2.2). The algorithm can be thought of as an extension of [58 and 71].

Cox et.al. in [58 and 71] add a watermark X consisting of a sequence of real numbers to the perceptually significant frequency components of the image. For extraction, they follow the reverse of insertion process. The sequence of real numbers is $X = \{x_1,x_2, \ldots\ x_n\}$, where x_i is chosen independently according to N (10,1) (Gaussian distribution with usual notations). The choice of n depends on the degree to which the watermark is inserted among the relevant frequency components of the image. The addition of this type of watermark is defended by Ruanaidh [55]. The watermark is robust to various types of attacks as claimed by the authors.

We propose a watermarking algorithm, which is a modification over the above algorithm [58 and 71]. In [58 and 71] the watermark consists of Gaussian Random numbers chosen according to N (10,1). The watermark is added to the perceptual significant frequency components that makes it robust. The authors didn't take the distribution of DCT coefficients into consideration. As pointed out by Reininger [92], for most of the images, the DCT coefficients of each block of image is Gaussian distributed and AC DCT coefficients follow Laplace distribution. So, we feel that instead of adding a Gaussian type watermark if we construct a watermark consisting of both Gaussian distribution (for DC coefficients) and Laplace distribution (for AC coefficients), then the watermark will be more robust and at the same time image quality will be maintained. Further, instead of only adding the watermark to the significant frequency components we can add to some components and subtract from some components as suggested by Craver[26]. This will further enhance the robustness of the watermark.

The authors [58 and 71] have used same scaling factor α for all frequency components. They have also suggested the use of multiple scaling factors α_i for different frequency components v_i. In this case choosing α_i poses a new problem. So we propose using two scaling factors, α_{dc} for DC DCT coefficients and α_{ac} for AC DCT coefficients.

7.2 WATERMARK CREATION

The watermark is created as follows: We find the DCT coefficients of the image I with 8x8 block sizes. The data for a given coefficient "ij" consists of points c_{ij} (k), k = 1,2, ………M, where k represents the position of block in the image (if we transverse the image in a horizontal manner). M is the total number of 8×8 blocks in the image and is given by (row*col/64), “row” is the number of rows and “col” is the number of columns of the image. For these data points the sample mean μ_{ij} and variance σ_{ij}^2 are calculated as:

$$\mu_{ij} = 1/M \sum c_{ij}(k) \tag{7.1}$$

$$\sigma_{ij}^2 = 1/M \sum (c_{ij}(k) - \mu_{ij})^2 \tag{7.2}$$

Suppose we will modify only the DC component c_{00} and 3 low frequency components c_{01},c_{10} and c_{11}(actual number of components to be modified can be chosen using some perceptual analysis). We create a watermark of blocksize 2×2 but number watermark blocks should be same as number of image blocks. Let us denote the watermark asW and its value at position “ij” as w_{ij}. The $w_{00}(k)$ are generated using Gaussian distribution of mean μ_{00} and variance σ_{00}^2. The rest w_{ij} (k) are generated using Laplace distribution of mean μ_{ij} and variance σ_{ij}^2. In mathematical form we have the followings.

$$w_{00} (k) = \exp. [-1/2 ((c_{00}(k) - \mu_{00}) / \sigma_{00})^2] \tag{7.3}$$

$$w_{ij} (k) = \exp. [-|c_{ij}(k) - \mu_{ij}| / \lambda_{ij}] \tag{7.4}$$

where, $$\lambda_{ij} = \sqrt{} (\sigma_{ij}^2 / 2) \tag{7.5}$$

The watermark values are scaled to the range 0-1.0.

7.3 WATERMARK INSERTION

Following are the steps followed for watermark insertion

- The image is divided into 8×8 blocks and block DCT coefficients are found out.
- The watermark is created as described in the last section.
- The perceptual significant DCT coefficients c_{ij} of the original image is modified to c'_{ij} as follows

$$c'_{ij} = \begin{cases} c_{ij} (1 + \alpha w_{ij}), bi = 0 \\ c_{ij} (1 - \alpha w_{ij}), bi =1 \end{cases} \tag{7.6}$$

where b_i is a pseudo-random sequence generated using a linear shift register as in chapter#6. The scaling factor $\alpha = \alpha_{dc}$ when both i and j are 0 (for DC coefficients) whereas $\alpha = \alpha_{ac}$ for other values of i and j (for AC coefficients).

- The IDCT of c'_{ij} values give the watermarked image I'.

- The values of α_{dc} and α_{ac} can be chosen such that image quality is not degraded. For that propose SNR can be found out. We have taken $\alpha_{dc} = 0.02$ and $\alpha_{ac} = 0.1$.

Fig.7.1 shows the schematic representation of insertion process. Fig.7.3–7.10 show different watermarked images.

7.4 WATERMARK EXTRACTION

Given an original image I and a possibly forged watermarked image I^* (may or may not be same as I'), we can extract a possibly distorted watermark W^* by following the reverse of insertion operation. The schematic representation of the process of extraction is given in Fig.7.2. If I^* differs from I' because of some unintentional or intentional attacks, then W^* may not be identical to W. We measure the similarity for W and W^* as proposed by Cox et al. [58 and 71]. The similarity is evaluated using the following.

$$\mathrm{sim}\ (W,W^*) = (W^*.W) / \surd\ (W^*.W) \qquad (7.7)$$

Where $W^*.W$ may be computed as $\sum w_{ij}^*.w_{ij}$, N being the total no of frequency components modified for watermarking (N equals size of watermark).

The detector responses for different attacks are tabulated in Table 7.1. The image was captured using "Capture-Screen" software of HP workstation, then saved in "tif" format. Then using XV software the watermarked image was subjected to various attacks. Basing on detector responses we can say if the response is in the range of 6.0 – 9.0, then the watermark image under-test, passes watermark test.

7.5 CONCLUSION

In this chapter, we proposed a Spread Spectrum Watermarking technique. This can be thought of as a modification of [58and71]. We claim that our technique is more robust as the detection response in our case is in the range 6.0 – 9.0 in comparison to 7.0 – 14.0 in case of [58and71]. In addition in our case, the image quality is better preserved. The drawback in our case as well as in case [58and71] is that in both cases original image is required for watermark extraction.

TABLE 7.1

Sl. No.	**Various Attacks**	Responses
1	JPEG Compression, QF-100%	7.87344
2	JPEG Compression, QF-75%	7.91917
3	JPEG Compression, QF-50%	7.30222
4	JPEG Compression, QF-25%	7.10314
5	3x3 blur, JPEG Compression, QF-25%	6.63185
6	5x5 blur, JPEG Compression, QF-25%	6.22863
7	7x7 blur, JPEG Compression, QF-25%	6.34497
8	25% sharp, JPEG Compression, QF-25%	6.85104
9	50% sharp, JPEG Compression, QF-25%	7.19093
10	Pixel size = 2x2, JPEG Compression, QF-25%	6.87866
11	Pixel size = 4x4, JPEG Compression, QF-25%	8.07584
12	3x3 spread, JPEG Compression, QF-25%	6.92151
13	5x5 spread, JPEG Compression, QF-25%	8.08294
14	3x3 median filter, JPEG Compression, QF-25%	7.79551
15	5x5 median filter, JPEG Compression,QF-25%	7.95514
16	7x7 median filter, JPEG Compression,QF-25%	8.9839

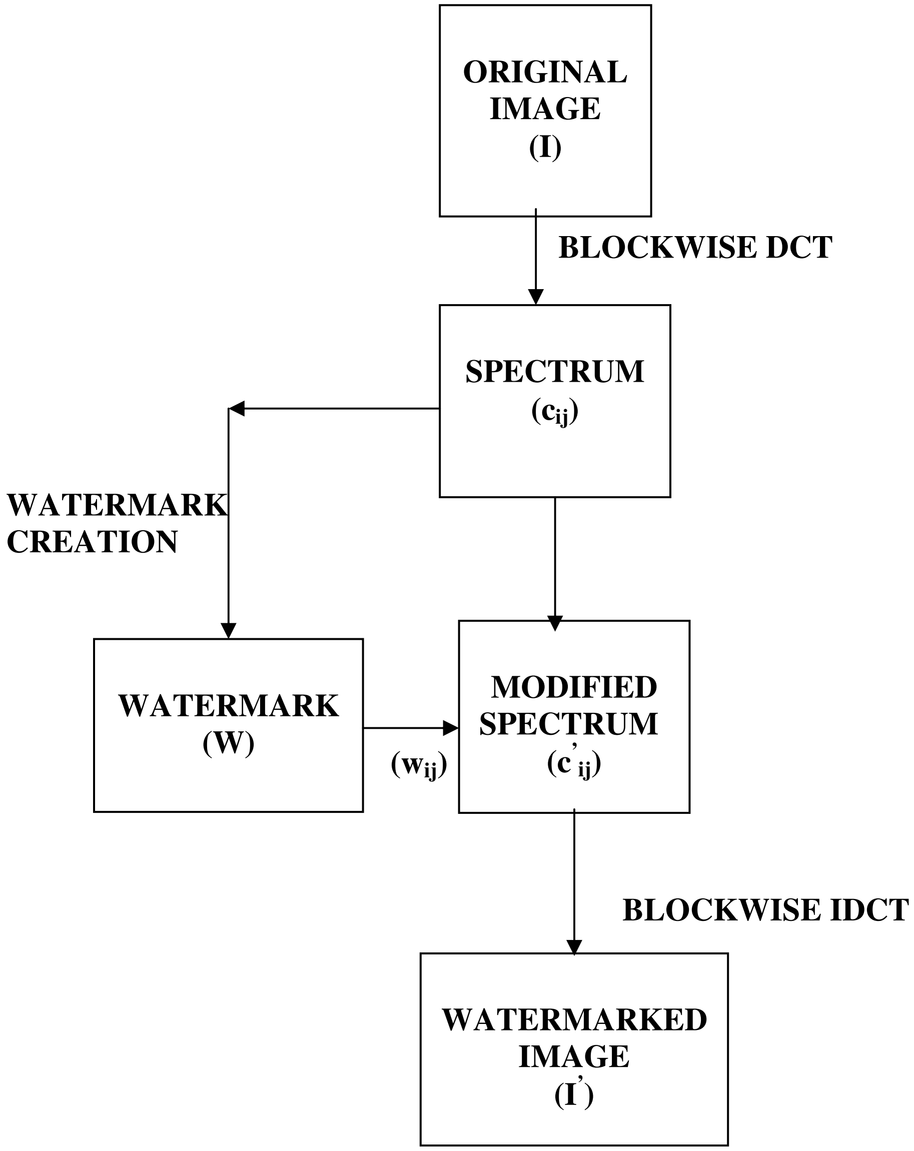


Fig.7.1 Stages of Insertion Procedure

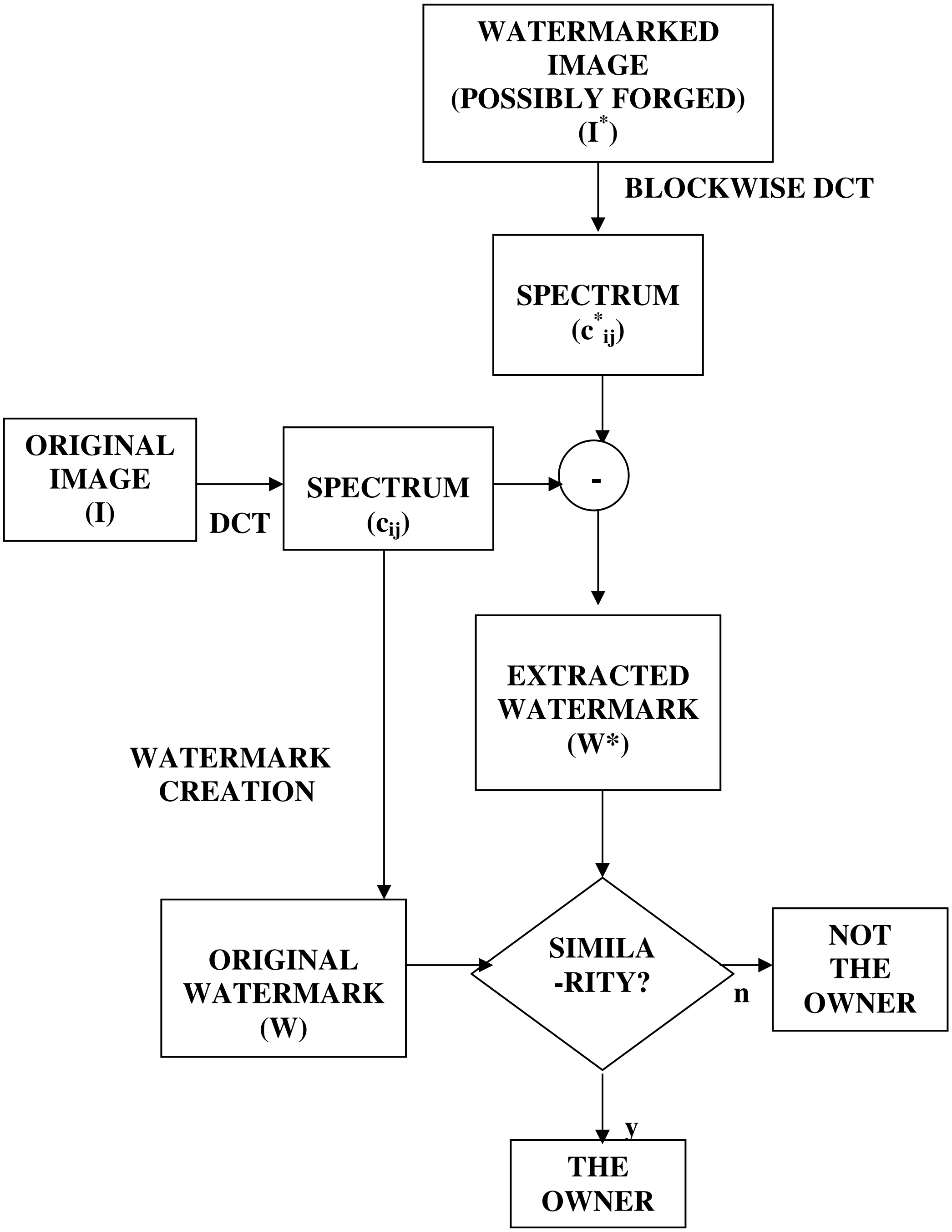


Fig.7.2 Stages Extraction Process

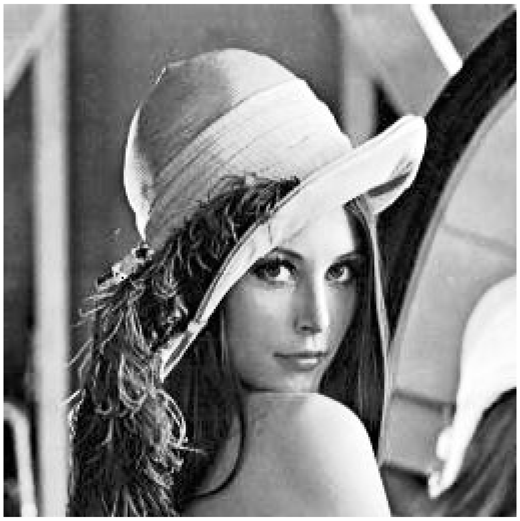


Fig. 7.3 Original “lena” image

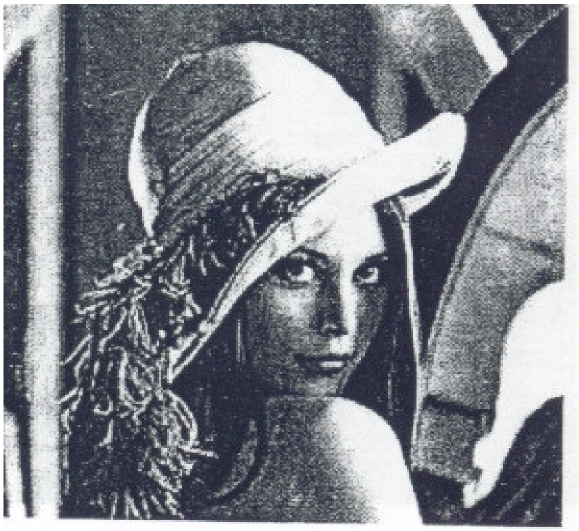


Fig. 7.4 Watermarked “lena” image
(α_{dc} = 0.02, α_{ac} = 0.1 , SNR = 31dB)
*scanned from hardcopy

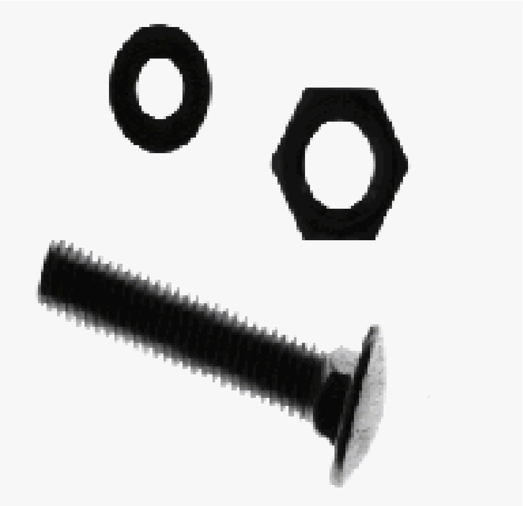


Fig. 7.5 Original “hardware” image

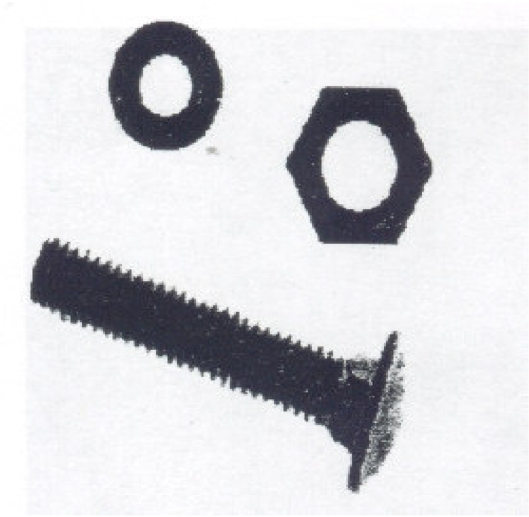


Fig. 7.6 Watermarked “hardware” image
(α_{dc} = 0.008, α_{ac} = 0.08 , SNR = 34dB)
*scanned from hardcopy

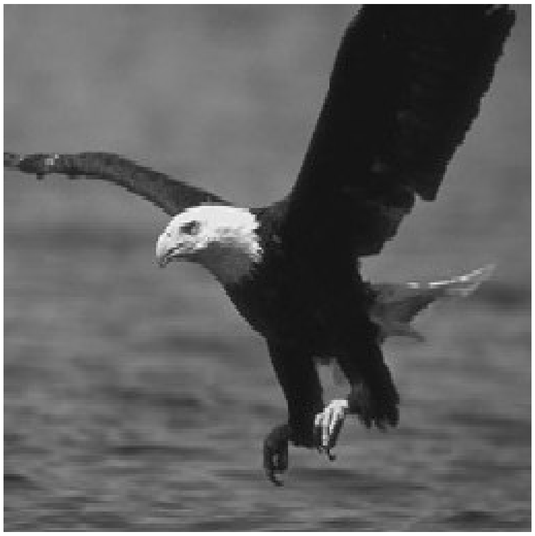


Fig. 7.7 Original "bird" image

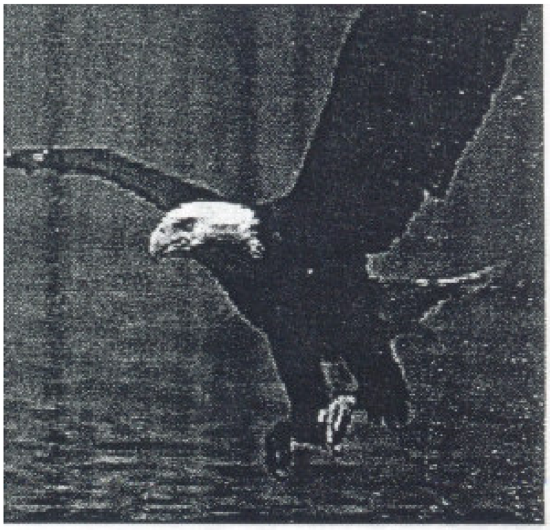


Fig. 7.8 Watermarked "bird" image
(α_{dc} = 0.02, α_{ac} = 0.1, SNR = 27dB)
*scanned from hardcopy

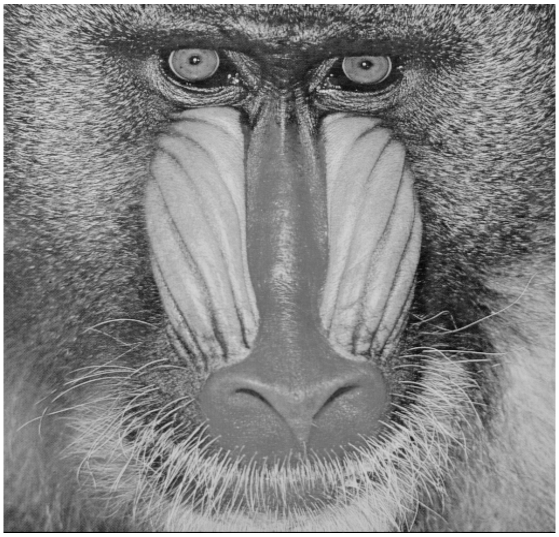


Fig. 7.9 Original "mandrill" image

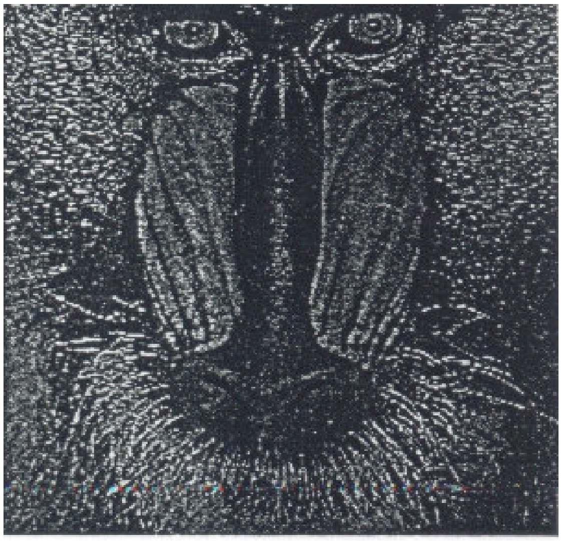


Fig. 7.10 Watermarked "mandrill" image
(α_{dc} = 0.02, α_{ac} = 0.1, SNR = 20dB)
*scanned from hardcopy

CONCLUSIONS AND FUTURE DIRECTIONS OF RESEARCH

Digital watermarking technology is an emerging field in computer science, cryptology, signal processing and communications. The watermarking research is more exciting as it needs collective concepts from all the fields along with Human Psycho-visual analysis, Multimedia and Computer Graphics. The watermark may be of visible or invisible type and each has got its own applications. We have developed two visible and two invisible algorithms as a part of the project work.

There are very few **visible watermarking** algorithms, so far [25] [84]. Out of the two visible watermarking algorithms proposed in this project, one is in spatial domain and the second is in DCT domain. To make the visible watermark visually pleasant, the mathematical models are developed taking the human visual system into consideration. The most significant application of visible watermarking is in Digital Libraries, where the owner wants to make the image available for research purpose but not for commercial use. The IBM Research Center people have used the visible watermarks for Vatican City Library Project.

There are few **fragile invisible algorithms** available in current literature even though it has got its own applications. We think some attention should be given to this area.

The **robust invisible watermarking** has been a topic of considerable interest due to their potential use for copyright protection. We have developed here two robust invisible watermarking algorithms. One of them is in spatial domain and the other one in DCT domain. Both of them are robust to various attacks and have the desired characteristics. As pointed out in [19] the ability to put robust watermarks does not necessarily solve the ownership problem. Still lots of work need are to be done in order to make the robust invisible watermark legally useful.

All the algorithms we have proposed can be extended to video. Only the fourth one can be extended to audio. Further, research is needed to make it work if the insertion/extraction is to be performed in real time. For video watermarking one should also try to exploit the temporal redundancy to make real time algorithms.

BIBLIOGRAPHY

1. A.Papoulis, Probability, Random Variables and Stochastic Processes, McGraw Hill, Inc., 1991, 3rd Edn.

2. R.C.Gonzalez and R.E.Woods, Digital Image Processing, Addison-Wesley Publishing company, Inc., 1993.

3. A.K.Jain, Fundamentals of Digital Image Processing, Prentice-Hall of India Pvt. Ltd., 1995

4. B.Pfitzmann, "Information Hiding Technology", Proc. Of First Int. Workshop on Information Hiding, Cambridge, UK, May30-June1 1996. Lecture notes in Computer Science, Vol.1174, Ross Anderson(Ed.).

5. W.Diffie and M.E.Hellman, "New Directions in Cryptography", IEEE trans. on Information Theory, Vol.IT-22, No.6, Nov.1976.

6. B.M.Macq, J.J.Quisquater, "Cryptography for Digital TV Broadcasting", Proc. of the IEEE, Vol.83, No.6, Jun1995, pp944-957.

7. G.J.Simmons, "The History of Subliminal Channels", IEEE Jou. On selected areas in Communications, Vol.16, No.4, May1998, pp.452-462.

8. G.J.Simmons, "Results Concerning the Bandwidth of Subliminal Channels", IEEE Jou. on selected areas in Communications, Vol.16, No.4, May1998, pp.463-473.

9 Bumster et.al., "A Progress Report on Subliminal-free Channels", Proc. of First Int. Workshop on Information Hiding, Cambridge, UK, May30-Jun1, 1996. Lecture notes in Computer Science, Vol.1174, Ross Anderson(Ed.).

10 Neal Koblitz, A Course in Number Theory and Cryptography, Springer-Verlag.

11 C. Meadow and I.S.Maskowintz, "Covert Channels – A content based view", Proc. of First Int. Workshop on Information Hiding, Cambridge, UK, May30-June1 1996. Lecture notes in Computer Science, Vol.1174, Ross Anderson(Ed.).

12 Homer, The Iliad (trans. R. Fragels), Middlesex, England: Penguin 1972.

13 Herodotus, The Histories (trans. R. Selincourt), Middlesex, England: Penguin 1972.

14 David Kahn, “The History of Steganography”, Proc. of First Int. Workshop on Information Hiding, Cambridge, UK, May30-June1 1996. Lecture notes in Computer Science, Vol.1174, Ross Anderson(Ed.).

15 M.D.Swanson et al., “Multimedia data Embedding and watermarking Technologies”, Proc. of the IEEE, Vol.86, No.6, June1998, pp.1064-1087.

16 Hal Berghel, “Watermarking Cyberspace”, Comm. of the ACM, Nov.1997, Vol.40, No.11, pp.19-24.

17 N.R.Wagner, “Finger Printing”, Proc. of the 1983 Symposium on Security and Privacy, Apr.25-27, 1983, Oakland, California, IEEE Computer Society, pp.18-22.

18 M.M.Yeung, “Digital Watermarking”, Comm. of the ACM, Jul.1998, Vol.41, No.7, pp.31-33.

19 S.Craver et al., “Can Invisible Watermarks Resolve Rightful Ownership?”, IBM Research Report, RC205209, Jul25, 1996. http://www.research.ibm.com/

20 M.Memon and P.W.Wong, “Protecting Digital Media Content”, Comm. of the ACM, Jul.1998, Vol.41, No.7, pp.35-43.

21 M.M Yeung et al. “Digital Watermarking for High-Qulaity Imaging” , 1997 IEEE First Workshop on Multimedia Signal Processing, Jun 23-25, 1997, Princeton, New Jersey, pp 357-362.

22 W. Zeng and B Liu, “On Resolving Rightful Ownership of Digital Images by Invisible Watermarks”, Proc. IEEE 1997 Intl Conference on Image Processing, ICIP-97, Vol. 1, pp 552-555.

23 F. Mintzer, et.al., “Effective and Ineffective Digital Watermarks”, IEEE 1997 Intl. Conference on Image Processing, ICIP-97, Vol. 3, pp 9-12.

24 J. Zhao, et. al., “In Business Today and Tommorrow”, Comm of Acm, July 1998, Vol. 41, No. 7, pp 67-72.

25 F. C. Mintzer, et. al., “Towards Online Worldwide Access to Vatican Library Materials”, IBM Journal of Research and Development, Vol. 40, No. 2, Mar 1996, pp 139-162.http://www.software.ibm.com/is/diglib/vatican.html
http://www.ibm.com/IBM/ibmgives/diglib.html
http://www.research.ibm.com/image_apps

26 S Craver, et. al., “Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks and Implications”, IEEE Jou.. Selected Areas in Communications, Vol. 16, No. 4, May 1998, pp 573-586.

27 G. L. Friedman, “The Trustworthy Digital Camera: Restoring Credibility to the Photographic Image”, IEEE Trans. Consumer Electronics, Vol 39, No. 4, Nov 1993.

28 I. J. Cox and J. P. M. G. Linnartz, “Some General Methods for Tampering with Watermarks”, IEEE Jou.. Selected Areas in Communications, Vol. 16, No. 4, May 1998, pp 587-593.

29 S Craver. et. al., “Technical Trials and Legal Tribulations”, Comm. of ACM, July 1998, Vol 41, No.7, pp 45-54.

30 J. M. Acken, “How Watermarking Value to Digital Content”, Comm. of ACM, July 1998, Vol 41, No.7, pp 75-77.

31 E. Franz, et. al., “Computer Based Steganography”, Proc. First Intl. Workshop on Information Hiding, Cambridge, UK, May 30 – June 1, 1996, Lecture notes in Computer Science, Vol.1174, Ross Anderson(Ed.).

32 G. W. Braudaway, et. al., “Protecting Publicly Available Images with a Visible Image Watermark”, Proc. SPIE Conf. Optical Security and Counterfiet Deterrence Technique, Vol. SPIE- 2659, pp.126-132, Feb. 1996.

33 F. J. MacWilliam and N. J. A. Sloane, "Pseudorandom Sequences and Arrays", Proc. IEEE, Vol. 64, No. 12, Dec 1976, pp 1715-1729.

34 I. J. Cox and M. Miller, "A Review of Watermarking and Importance of Perceptual Modelling", Proc. SPIE Human Vision and Imaging, SPIE-3016, Feb 1997.

35 D.V. Sarwate and M. B. Pursley, "Cross-correlation of Pseudorandom and Related Sequences", Proc IEEE, Vol. 68, No. 5, May 1980, pp 593-619.

36 W. Bendor, et. al., "Techniques for Data Hiding", IBM Systems Jrnl., Vol. 35, No. 3 and 4, pp 313-336.

37 F. Mintzer, et. al., "Opportunities for Watermarking Standards", Comm. ACM, July 1998, Vol. 41, No. 7, pp 57-64.

38 S. Craver, et. al., "On the Invertibility of Invisible Watermarking Techniques", Proc IEEE 1997 Intl. Conf. Image Processing, ICIP-97, Vol. 1, pp 540-543.

39 http://www.altern.org/watermark

40 http://www.cl.cam.ac.uk/~fapp2/watermarking/stirmark

41 M. Schneider and S. F. Chang, "A Content BAsed Approach to Image Generation and Authentication", Proc. IEEE 1996 Intl. Conf. Image Processing, ICIP-96, Vol-3, pp 227-230.

42 R. G. Van Schyndel, et.al., "A Digital Watermark", ICIP-94, Vol. 2, pp 86-90

43 R. G. Wolfgang and E. J. Delp, "A Watermark for Digital Images", ICIP-96, Vol 3, pp 219-222.

44 R. B. Wolfgang and E. J. Delp, "A Watermarking Technique for Digital Imagery: Further Studies", Proc. Intl. Conf.. on Imaging Sciences, Systems and Tech. Los Vegas, Jun 30-Jul 3, 1997. http://dynamo.ecn.purdue.edy/ac/delp-pub.html

45 N. Nikolaids and I. Pitas, "Copyright Protection of Images Using Robust Digital Signatures", ICASSP-96, Vol. 4, pp 2168-2171.

46 I.Pitas, “A Method for signature castion on Digital Images”,Proc. IEEE 1996 International Conf. On Image Processing,ICIP-96,Vol 3,pp215-218

47 N. Nikolaidis and I. Pitas, “Robust Image Watermarking in Spatial Domain” ,Signal Procesing,Vol 66,No. 3,pp 385-403.

48 I.Pitas and T. Kaskalis, “Applying Signature on Digital Images” , Proc IEEE,1995, Workshop on Non-linear Signal and Image Processing, I. Pitas(Ed.), pp. 460-463

49 G. Voyatzis and I. Pitas, “Application of Toral Automorphism in Image Watermarking”, Proc. IEEE 1996, International Conf. On Image Processing,1996,Vol2,pp 237-240

50 J.Zhao and E. Koch, “Embedding Robust Labels into Images for Copyright Protection”, Proc of International Congress on Intellectual Property Rights for Specialized Information Knowledge and New Technologies, Vienna, Austria, Aug 21-25 1995, pp 242-251

51 K. Hirotsugu, “An Image Digital Signature System with ZKIP for the Graph Isomorphism”, Proc IEEE 1996,International Conf. On Image Processing,Vol 3,pp 247-250

52 M.M.Yeung and F. Mintzer, “An Invisible Watermarking technique for Image Verification”, Proc. IEEE 1997, International Conf on Image Processing, Vol. 2, pp 680-683

53 J.F.Delaiglee et. al., “Watermarking Algorithm based on Human Visual Model”, Signal Processing, Vol 66, No 3, pp 319-335, May 1998

54 M.Kutter et. al., “Digital Signature of color Images using Adaptive Modulation”, Proc.SPIE-EI97, 1997, pp 518-526

55 J.J.K O'Ruanaidh et. al. "Watermarking Digital Images for Copyright Protection", IEE Proc. Vision Image and Signal Processing, Vol 143, No 4, Aug. 1996

56 J.J.K. O'Ruanaidh et. al. "Phase Watermarking on Digital Images", Proc. IEEE,1996, International Conf. On Image Processing, ICIP-96, Vol 3, pp 239-242

57 M.D.Swanson et. al., "Transparent Robust Image Watermarking", Proc IEEE 1996, International Conf. On Image Procesing, Vol 3, pp 211-214

58 I.J.Cox et. al., "Secure spread Spectrum Watermarking of Images,Audio and Video", Proc IEEE 1996 International Conf on Image Processing, 1996, Vol 3, pp 243-246 http://www.neci.nj.nec.com/tr/neci_tr_95_10.ps

59 C.T.Hsu and J.L.Wu. "Hidden Sinatures in Images", Proc IEEE 1996 International Conf. On Image Processing, Vol 3, pp 223-226

60 A.G.Bors and I. Pitas, "Image Watermarking using Image Domain Constraints", Proc IEEE 1996 International Conf. On Image Processing, Vol 3, pp 231-234

61 C.Podilchuk and W.Zeng, "Perceptual Watermarking of Still Images", 1997 IEEE, First Worlshop on Multimedia signal Processing, June 23-25 1997, Priceton, New Jersy, USA, pp 363-368

62 A.Piva et. al., "DCT based Watermark Recovery without resorting to the Uncorrupted Original Signal", IEEE 1997 International Conf. on Image Processing, Vol.1, pp 520-523

63 J.J.K O'Ruanaidh and T. Pun , "Rotation , Scale and Translation Invariant Digital Image Watermarking", Proc IEEE 1997, International Conf. On Image Processing , Vol 1,pp 536-539

64 J.R.Hermandez et. al., "Performance Analysis of a 2-D Multipulse Amplitude Modulation Scheme for Data Hiding and Watermarking of Still Images", IEEE Journal on Selected areas in Communications, Vol 16, No 4, May 1998 , pp 520-524

65 J.R.Smith and B.O.Comiskey, "Modulation and Information Hiding in Images", Proc of First International Workshop on Information Hiding, University of Canbridge, UK, May 30-June 1 1996, Lecture Notes in Comp. Sc., Vol 1174, Ross Anderson (Ed.)

66 D.J.Fleet and D.J.Heeger , "Embedding Invisible Information in color Images", Proc IEEE 1997, International Conf. On Image Processing, Vol 1, pp 532-535

67 G.W.Barudaway, "Protecting Publicly available Images with Invisible Watermark", Proc IEEE 1997,International Conf on Image Processing,Vol 1 pp 524-527

68 C.I.PodilChuk and W.Zeng, "Image Adaptive Watermarking Visual Models", IEEE Journal on Selected Areas in Communications ,Vol 16, No 4, May 1998, pp 525-539

69 J.J.K. O'Ruanaidh and T.Pun, "Rotation Scale and Translation Invariant Spread Spectrum Digital Image Watermarking", Signal Processing, Vol.66, No 3, May 1998, pp 303-317

70 M.Barni et al., "A DCT-Domain System for Robust Image Watermarking", Signal Processing, Vol 66, No 3,May 1998, pp 357-372

71 I.J.Cox et. al., "A Secure Robust Watermarking for Multimedia", Proc of First International Workshop on Information Hiding, Lecture Notes in Comp. Sc., Vol.1174, pp 185-206, Speinger-Verlag, 1996

72 B.Tao and B.Dickinson, "Adaptive Watermarking in DCT Domain", Proc IEEE 1997, International Conf on Accoustics, Speech and Signal Processing, ICASSP-97, Vol 4, pp 2985-2988

73 F.Hartung and B.Girod , "Digital Watermarking of Raw and Compressed Video", Digital Compression Technologies and Systems for Video Communications Vol 2952 of SPIE Proc. Series, Oct 1996, pp 205-213

74 F.Hartung and B. Girod, "Copyright Protection in Video Dilevery Networks by Watermarking of pre-compressed Video" , in Multimedia applications, Services and Technologies-ECMAST-97, Lecture Notes in Comp Sc., S.Fadida and M.Morganti(Ed.) , Tokyo, Japan, Springer 1997, Vol 1242, pp 423-436

75 F.Hartung and B.Girod, "Fast Public-Key Watermarking of compressed Video", Proc. IEEE 1997, International Conf. On Image Processing , Vol.1, pp 528-531

76 F.Hartung and B.Girod, "Digital Watermarking of MPEG-2 coded Video in Bitstream Domain", Proc. IEEE 1997, International Conf. On Accoustics, Speech and Signal Processing, Vol. 4, pp 2621-2624

77 F.Hartung and B.Girod , "Watermarking of uncompressed and compressed Video", Signal Processing Vol. 66, No. 3, May 1998, pp 283-301

78 M.D.Swanson et. al. "Data Hiding for Video-in-Video", Proc IEEE 1997 International Conf. On Image Processing, Vol 2, pp 676-679

79 M.D.Swanson et. al. "Object Based Transparent Video Watermarking", 1997 IEEE, First Workshop on Multimedia Signal Processing, June 23-25,1997, Princeton, New Jersey, USA, pp.369-374

80 C.T.Hsu and J. L. Wu, "DCT-Based Watermarking for Video", IEEE Trans Consumer Electronics, Vol. 44, No. 1, Feb 1998, pp 206-216.

81 M. D. Swaun, et. al., "Multiresolution Scene-Based Video Watemarking using Perceptual Models", IEEE Jrnl. Selected Areas in Communications, Vol. 16, No.4, May 1998, pp 540-550.

82 T. Y. Chung, et. al., "Digital Watermarking for Copyright Protections of MPEG-2 Compressed Video", IEEE Jrnl. Consumer Electronics, Vol. 44, No. 3, Aug 1998, pp 895-901.

83 A. J. Viterbi, CDMA Principles of Spread Spectrum Communications, Addison-Wesley Inc., 1995.

84 Rajmohan, Watermarking of Digital Images, ME Thesis Report, Dept. Electrical Engineering, Indian Institute of Science,Banglore, India, 1998.

85 K. N. Ngan, et. al., "Adaptive Cosine Transform Coding of Images in Perceptual Domain", IEEE Trans. Acoustics, Speech and Signal Processing, Vol. 37, No. 11, Nov. 1989, pp 1743-1750.

86 D. J. Granrath, "The Role of Human Visual Models in Image Processing", Proc. IEEE, Vol. 69, No. 5, May 1981, pp 552-561.

87 M. Kankanahalli, et. al., "Content Based Watermarking for Images", Proc. 6th ACM International Multimeda Conference, ACM-MM 98, Bristol, UK, pp 61-70, Sep 1998.

88 M. Kankanahalli, et. al., "Perceptual Content Analysis Based Digital Image Watermarking", Proc. National Seminar on Cryptography, Jul 9-10, 1998, Delhi, India.

89 C. E. Shannon, "A Mathematical Theory of Communication", Bell Systems Technical Journal, 1948, 27, pp 379-423, 623-656.

90 R. G. Gallager, Information Theory and Reliable Communication, Wiley, 1968.

91 J. G. Proakis, Digital Communication, McGraw-hill 1995, 3rd ed.

92 R. C. Reminger and J. D. Gibson, "Distribution of the 2D DCT Coefficients for Images", IEEE Trans. Communication, Vol COM-31, No. 6, Jun 1983.

93 J. L. Mannas and D. J. Sakrison, "The Effects of a Visual Fidelity Criterion on the Encoding of Images", IEEE Trans. Information Theory, Vol. IT-20, No. 4, Jul 1974,

94 V. K. Rohatgi, An Introduction to Probability Theory and Mathematical Statistics, Wiley Eastern Ltd., 1993.