A PROJECT REPORT
ON

A METHODOLOGY FOR DIGITAL WATER MARKING USING DCT&DWT AND PBFO

A Project Report submitted to

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY, Kakinada.

In the partial fulfillment of the requirements for the award of the degree of

BACHELOR OF TECHNOLOGY

IN

ELECTRONICS AND COMMUNICATION ENGINEERING

Submitted by

Y. BHARGAVI	(17A71A0452)
N.ANANTHA LAKSHMI	(18A75A0409)
SK.SAYYED BAJI	(17A71A0440)
B.BHASKAR RAO	(17A71A0404)

Under the Esteemed Guidance of

DR.CH.SRINIVASA KUMAR,M.E,Ph.D,ISTE,DBMA,PROFESSOR,HOD.

Department of Electronics and communication Engineering

NALANDA INSTITUTE OF ENGINEERING AND TECHNO LOGY

(An ISO9001-2000)Certified Institution, Approved by AICTE New Delhi& Affiliated to JNT University, Kakinada

Siddhartha Nagar, Kantepudi(V), Sattenapalli(M), Guntur Dist -522438,08641-23786/64

2017-2021

NALANDA INSTITUTE OF ENGINEERING AND TECHNOLOGY

(An ISO 9001-2000 Certified Institution, Approved by AICTE New Delhi & Affiliated to JNT University, Kakinada) Siddhartha Nagar, Kantepudi(V), Sattenapalli(M), Guntur Dist – 522438, 08641-237863/64

BONAFIDE CERTIFICATE

This is to certify that the main project report entitled "A METHODOLOGY FOR DIGITAL WATER MARKING USING DCT&DWT AND PBFO" as the part of academic fulfilment according to JNTU-KAKINADA done by Y.BHARGAVI(17A71A0452),N.ANANTHA LAKSHMI(18A75A0409), SK.SAYYED BAJI(17A71AO440)& B.BHASKER RAO(17A71A0404) under the guidance and supervision of A PROF, CH.SRINIVASA KUMAR,M.E,PH.D,ISTE,DBMA,HOD at the Department of Electronics and Engineering , for the degree of Bachelor of Technology in ELECTRONICS AND COMMUNICATION ENGINEERING of Jawaharlal Nehru Technological University,

Kakinada, A.P, INDIA.

The project viva-voce exam is held on_____of_____, 2021.

INTERNAL GUIDE **EXTERNAL GUIDE**

HEAD OF THE DEPARTMENT **PRINCIPAL**

DECLARATION

I hereby declare that this thesis entitled **"A METHODOLOGY FOR DIGITAL WATER MARKING USING DCT&DWT AND PBFO"** submitted to Jawaharlal Nehru Technological University, Kakinada for the award of degree of **Bachelor of Technology** in **ELECTRONICS AND COMMUNICATION ENGINEERING** is based on the original work carried out in the laboratories of **NALANDA INSTITUTE OF ENGINEERING AND TECHNOLOGY,** kantepudi (V), Sattenapalli (Md),

Guntur (Dt), AP., INDIA and has not been submitted earlier in part or in full for any degree or diploma of any university.

Y.BHARGAVI	17A71A0452
N.ANANTHA LAKSHMI	18A75A0409
SK.SAYYED BAJI	17A71A0440
B.BHASKAR RAO	17A71A0404

ACKNOWLEDGEMENT

The Almighty has been bestowing us with his blessings throughout our life. I thank thou force for all that he has done for me and my friends. We all are his disciples .Words are few to express the feeling of thanks and gratitude to the following persons

I am extremely thankful to my honorable and enthusiastic FOUNDER CHAIRMAN **Dr. A. VARA PRASAD REDDY.** Nalanda Group of Institutions, Sattenapalli, thereby making my dream of higher education come true.

I express my grateful attitude to SECRETARY **Dr. A.VIJAYA SARADA REDDY**. Nalanda Group of Institutions, Sattenapalli, for providing necessary facilities for the graduation studies and dissertation work by being behind the screen.

I am extremely thankful to my honorable and enthusiastic CHAIRMAN **Mr. A. SIDDHARTH REDDY.** Nalanda Group of Institutions, Sattenapalli, thereby making my dream of higher education come true.

I express my heart-felt gratitude to our PRINCIPAL Prof. CH. SRINIVASA KUMAR, M.E,(Ph.D),ISTE,DBMA.NALANDA INSTITUTE OF ENGINEERING AND TECHNO LOGY, Sattenapalli for his encouragement, constructive suggestions and constant inspiration throughout the entire course of study.

I am extremely grateful to our **PROF.CH.SRINIVASA KUMAR,M.E,Ph.D,ISTE,DBMA.**Head of the Department of Electronics and communication Engineering, NALANDA INSTITUTE OF ENGINEERING AND TECHNOLOGY, Sattenapalli, for her valuable guidance, affectionate encouragement and moral support throughout the course of this investigation. I am greatly indebted to his guidance.

I would like to gratefully acknowledge my project guide, **PROF.CH.SRINIVASA KUMAR,M.E,Ph.D,ISTE,DBMA**. has been abundantly helpful and has assisted me in numerous ways. I specially thank him for his infinite patience.

My sincere thanks to all my teaching and non-teaching staff, Nalanda Institute of Engineering & Technology,, who had helped me directly or indirectly for the successful completion of our dissertation work.

I express my feelings and gratitude to my beloved parents without whose selfless help and moral support and boundless enthusiasm, I am nothing. They helped me in every possible way and the love bestowed on us deserves endless praise.

Last but not least, I express my sincere thanks to one and all and also to those whom I might have missed to mention, who gave constant encouragement and help throughout my educational career.

A METHODOLOGY FOR DIGITAL WATER MARKING USING DCT&DWT AND PBFO

ABSTRACT

This paper deals with the development of watermarking schemes for digital images stored in both, spatial and transformed domain. In this we mainly focus on the Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) based development. To increase the undetectability and to increase the claim, gain of embedding algorithm is optimized with the help of bacterial foraging optimization (BFO) and particle swarm optimization (PSO) so that security is increased. For this every watermark is given a unique identification, same as the principle of Code Division Multiple Accessing (CDMA) technique. To prove its commercial usability, we take special care so that at least one attack, having huge financial implications, can be sustained due to the in-built capacity of the watermarking scheme. Apart from this, since JPEG is the most commonly used image format over WWW, we pay special attention to robustness against noise attack. We propose to increase the robustness against some attacks by pre-processing the images. In this thesis, we also present a correlation between the performance of the watermarking scheme against some attacks and the original image characteristics. All presented watermarking schemes are robust against common image manipulations and attacks.

INDEX

LIST OF FIGURES

CHAPTER-1

INTRODUCTION

INTRODUCTION TO IMAGE PROCESSING

1.1 IMAGE

An image is a two-dimensional picture, which has a similar appearance to some subject usually a physical object or a person.

Image is a two-dimensional, such as a photograph, screen display, and as well as a three-dimensional, such as a statue. They may be captured by optical devices—such as cameras, mirrors, lenses, telescopes, microscopes, etc. and natural objects and phenomena, such as the human eye or water surfaces.

The word image is also used in the broader sense of any two-dimensional figure such as a map, a graph, a pie chart, or an abstract painting. In this wider sense, images can also be rendered manually, such as by drawing, painting, carving, rendered automatically by printing or computer graphics technology, or developed by a combination of methods, especially in a pseudo-photograph.

Fig 1.1: The color and gray scale images

An image is a rectangular grid of pixels. It has a definite height and a definite width counted in pixels. Each pixel is square and has a fixed size on a given display. However different computer monitors may use different sized pixels. The pixels that constitute an image are ordered as a grid

(columns and rows); each pixel consists of numbers representing magnitudes of brightness and color.

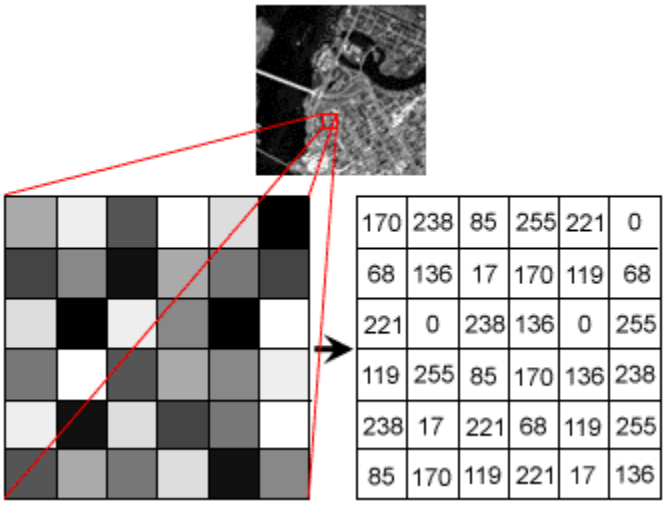
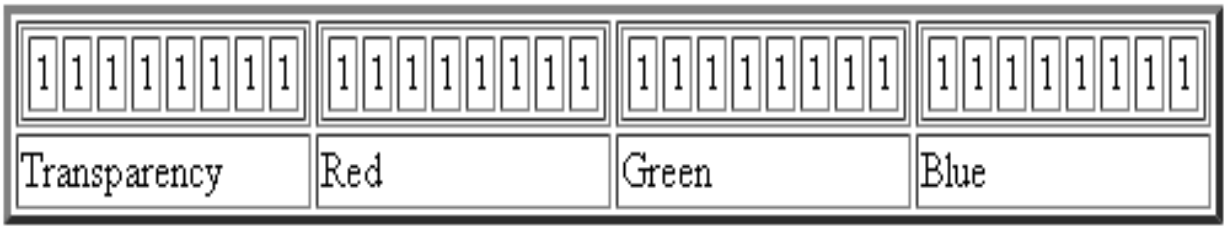


Fig1.2: Pixel Segmentation of image.

Each pixel has a color. The color is a 32-bit integer. The first eight bits determine the redness of the pixel, the next eight bits the greenness, the next eight bits the blueness, and the remaining eight bits the transparency of the pixel.



1.2 IMAGE FILE SIZES

Image file size is expressed as the number of bytes that increases with the number of pixels composing an image, and the color depth of the pixels. The greater the number of rows and columns, the greater the image resolution, and the larger the file. Also, each pixel of an image increases in size when its color depth increases, an 8-bit pixel (1 byte) stores 256 colors, a 24-bit pixel (3 bytes) stores 16 million colors, the latter known as true color. Image compression uses algorithms to decrease the size of a file. High resolution cameras produce large image files, ranging

from hundreds of kilobytes to megabytes, per the camera's resolution and the image-storage format capacity. High resolution digital cameras record 12-megapixel (1MP = 1,000,000 pixels / 1 million) images, or more, in true color. For example, an image recorded by a 12 MP camera; since each pixel uses 3 bytes to record true color, the uncompressed image would occupy 36,000,000 bytes of memory, a great amount of digital storage for one image, given that cameras must record and store many images to be practical. Faced with large file sizes, both within the camera and a storage disc, image file formats were developed to store such large images.

1.3 IMAGE FILE FORMATS

Image file formats are standardized means of organizing and storing images. This entry is about digital image formats used to store photographic and other images. Image files are composed of either pixel or vector (geometric) data that are rasterized to pixels when displayed (with few exceptions) in a vector graphic display. Including proprietary types, there are hundreds of image file types. The PNG, JPEG, and GIF formats are most often used to display images on the Internet.

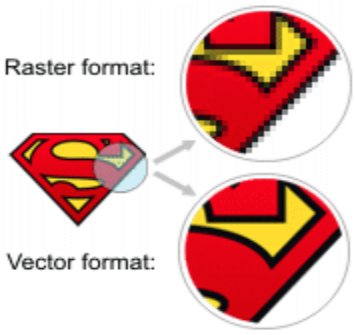


Fig1.3:Image file Formats

In addition to straight image formats, Metafile formats are portable formats which can include both raster and vector information. The metafile format is an intermediate format. Most Windows applications open metafiles and then save them in their own native format.

1.3.1 RASTER FORMATS

These formats store images as bitmaps (also known as pixmaps).

- **JPEG/JFIF**

JPEG (Joint Photographic Experts Group) is a compression method. JPEG compressed images are usually stored in the JFIF (JPEG File Interchange Format) file format. JPEG compression is lossy compression. Nearly every digital camera can save images in the JPEG/JFIF format, which supports 8 bits per color (red, green, blue) for a 24-bit total, producing relatively small files. Photographic images may be better stored in a lossless non-JPEG format if they will be re-edited, or if small "artifacts" are unacceptable. The JPEG/JFIF format also is used as the image compression algorithm in many Adobes PDF files.

- **EXIF**

The EXIF (Exchangeable image file format) format is a file standard similar to the JFIF format with TIFF extensions. It is incorporated in the JPEG writing software used in most cameras. Its purpose is to record and to standardize the exchange of images with image metadata between digital cameras and editing and viewing software. The metadata are recorded for individual images and include such things as camera settings, time and date, shutter speed, exposure, image size, compression, name of camera, color information, etc. When images are viewed or edited by image editing software, all of this image information can be displayed

- **TIFF**

The TIFF (Tagged Image File Format) format is a flexible format that normally saves 8 bits or 16 bits per color (red, green, blue) for 24-bit and 48-bit totals, respectively, usually using either the TIFF or TIF filename extension. TIFFs are lossy and lossless. Some offer relatively good lossless compression for bi-level (black & white) images. Some digital cameras can save in TIFF format, using the LZW compression algorithm for lossless storage. TIFF image format is not widely supported by web browsers. TIFF remains widely accepted as a photograph file standard in the printing business. TIFF can handle device-specific color spaces, such as the CMYK defined by a particular set of printing press inks.

- **PNG**

The PNG (Portable Network Graphics) file format was created as the free, open-source successor to the GIF. The PNG file format supports true color (16 million colors). while the GIF supports only 256 colors. The PNG file excels when the image has large, uniformly colored areas. The lossless PNG format is best suited for editing pictures, and the lossy formats, like JPG, are best for the final distribution of photographic images, because JPG files are smaller than PNG files. PNG, an extensible file format for the lossless, portable, well-compressed storage of raster images. PNG provides a patent-free replacement for GIF and can also replace many common uses of TIFF. Indexed-color, grayscale, and true color images are supported, plus an optional alpha channel. PNG is designed to work well in online viewing applications, such as the World Wide Web. PNG is robust, providing both full file integrity checking and simple detection of common transmission errors.

- **GIF**

GIF (Graphics Interchange Format) is limited to an 8-bit palette, or 256 colors. This makes the GIF format suitable for storing graphics with relatively few colors such as simple diagrams, shapes, logos and cartoon style images. The GIF format supports animation and is still widely used to provide image animation effects. It also uses a lossless compression that is more effective when large areas have a single color, and ineffective for detailed images or dithered images.

- **BMP**

The BMP file format (Windows bitmap) handles graphics files within the Microsoft Windows OS. Typically, BMP files are uncompressed, hence they are large. The advantage is their simplicity and wide acceptance in Windows programs.

1.4 IMAGE PROCESSING

Digital image processing, the manipulation of images by computer, is relatively recent development in terms of man's ancient fascination with visual stimuli. In its short history, it has been applied to practically every type of images with varying degree of success. The inherent

subjective appeal of pictorial displays attracts perhaps a disproportionate amount of attention from the scientists and also from the layman. Digital image processing like other glamour fields, suffers from myths, mis-connect ions, mis-understandings and mis-information. It is vast umbrella under which fall diverse aspect of optics, electronics, mathematics, photography graphics and computer technology. It is truly multidisciplinary endeavor ploughed with imprecise jargon.

Several factors combine to indicate a lively future for digital image processing. A major factor is the declining cost of computer equipment. Several new technological trends promise to further promote digital image processing. These include parallel processing mode practical by low-cost microprocessors, and the use of charge coupled devices (CCDs) for digitizing, storage during processing and display and large low cost of image storage array.

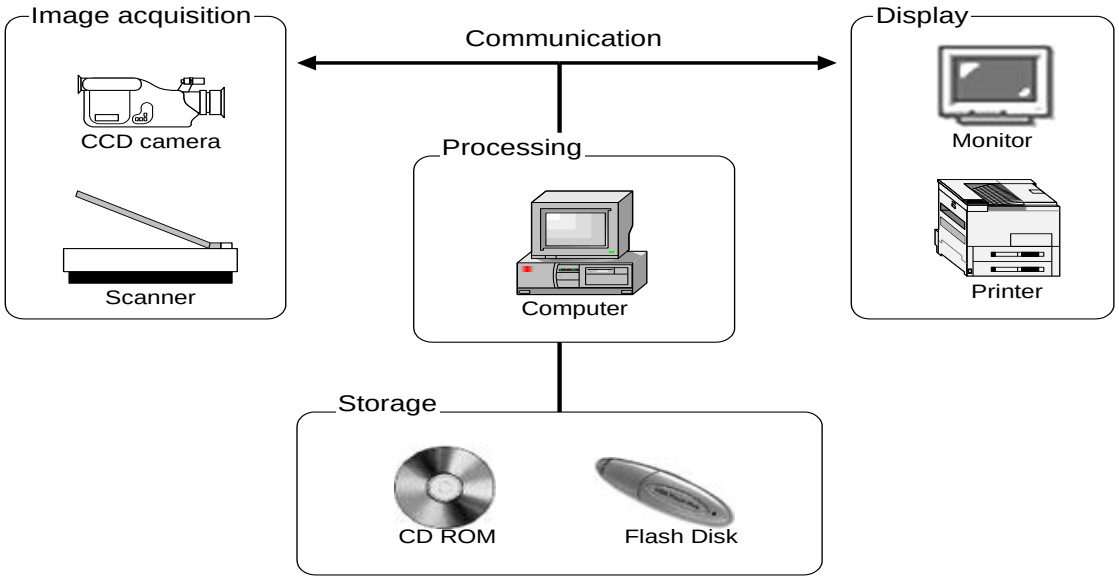


Figure 1.4: The Basic Image Processing System.

1.5 FUNDAMENTAL STEPS IN DIGITAL IMAGE PROCESSING

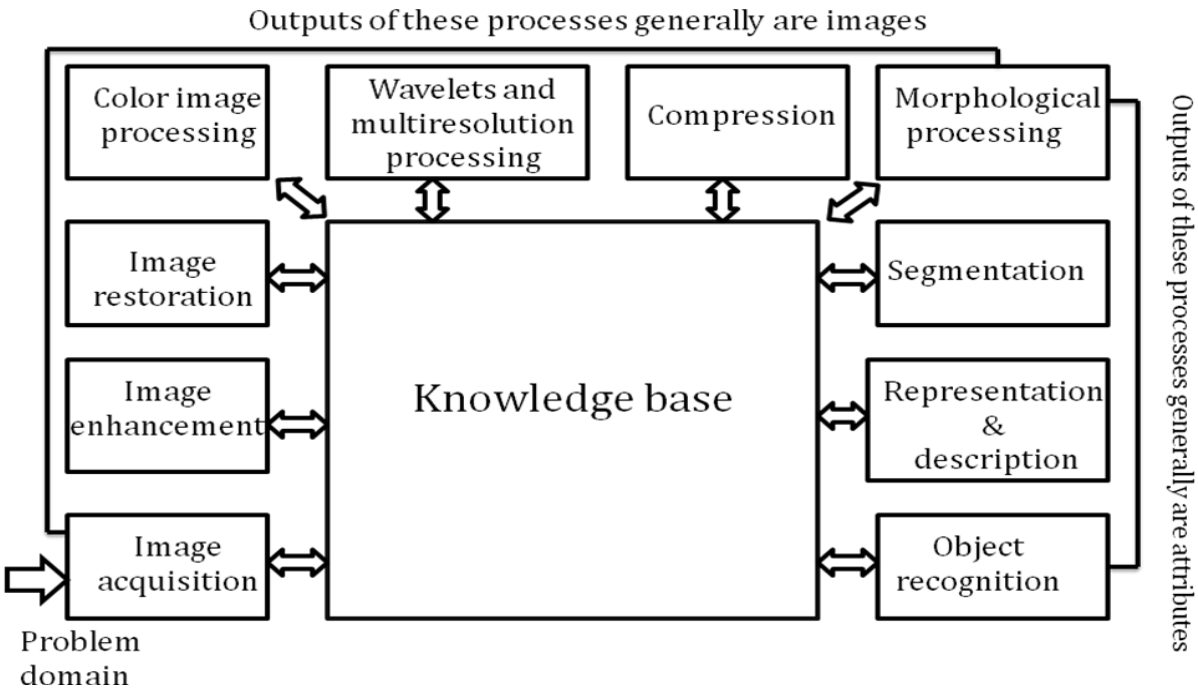


Fig1.5: Fundamental steps of image processing.

1.5.1 Image Acquisition

Image Acquisition is to acquire a digital image. To do so requires an image sensor and the capability to digitize the signal produced by the sensor. The sensor could be monochrome or color TV camera that produces an entire image of the problem domain every 1/30 sec. the image sensor could also be line scan camera that produces a single image line at a time. In this case, the objects motion past the line.

Fig1.6: Image Acquisition

Scanner produces a two-dimensional image. If the output of the camera or other imaging sensor is not in digital form, an analog to digital converter digitizes it. The nature of the sensor and the image it produces are determined by the application.

Fig1.7:Scanner

1.5.2 Image Enhancement

Image enhancement is among the simplest and most appealing areas of digital image processing. Basically, the idea behind enhancement techniques is to bring out detail that is obscured, or simply to highlight certain features of interesting an image. A familiar example of enhancement is when we increase the contrast of an image because "it looks better." It is important to keep in mind that enhancement is a very subjective area of image processing.

Fig1.8:Image Enhancement

1.5.3 Image restoration

Image restoration is an area that also deals with improving the appearance of an image. However, unlike enhancement, which is subjective, image restoration is objective, in the sense that

restoration techniques tend to be based on mathematical or probabilistic models of image degradation.

Fig 1.9: The basic example for image enhancement.

Enhancement, on the other hand, is based on human subjective preferences regarding what constitutes a "good" enhancement result. For example, contrast stretching is considered an enhancement technique because it is based primarily on the pleasing aspects it might present to the viewer, whereas removal of image blur by applying a deblurring function is considered a restoration technique.

1.5.4 Color image processing

The use of color in image processing is motivated by two principal factors. First, color is a powerful descriptor that often simplifies object identification and extraction from a scene. Second, humans can discern thousands of color shades and intensities, compared to about only two dozen shades of gray. This second factor is particularly important in manual image analysis.

Fig 1.10:Color image processing

1.5.5 Wavelets and multi resolution processing

Wavelets are the formation for representing images in various degrees of resolution. Although the Fourier transform has been the mainstay of transform-based image processing since the late1950's, a more recent transformation, called the wavelet transform, and is now making it even easier to compress, transmit, and analyze many images. Unlike the Fourier transform, whose basis functions are sinusoids, wavelet transforms are based on small values, called Wavelets, of varying frequency and limited duration.

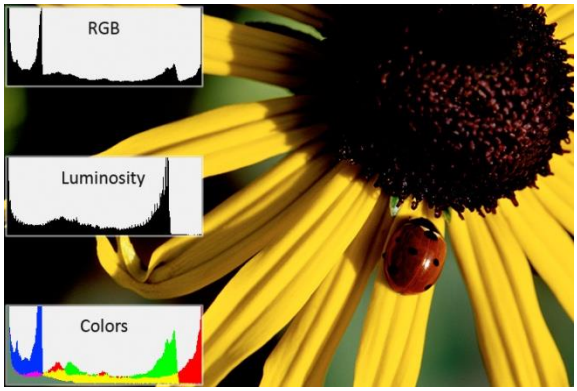


Fig1.11:Wavelets and multi resolution processing

Wavelets were first shown to be the foundation of a powerful new approach to signal processing and analysis called Multi resolution theory. Multi resolution theory incorporates and unifies techniques from a variety of disciplines, including sub band coding from signal processing, quadrature mirror filtering from digital speech recognition, and pyramidal image processing.

1.5.6 Compression

Compression, as the name implies, deals with techniques for reducing the storage required saving an image, or the bandwidth required for transmitting it. Although storage technology has improved significantly over the past decade, the same cannot be said for transmission capacity. This is true particularly in uses of the Internet, which are characterized by significant pictorial content. Image compression is familiar to most users of computers in the form of image file extensions, such as the jpg file extension used in the JPEG (Joint Photographic Experts Group) image compression standard.

1.5.7 Morphological processing

Morphological processing deals with tools for extracting image components that are useful in the representation and description of shape. The language of mathematical morphology is set theory. As such, morphology offers a unified and powerful approach to numerous image processing problems. Sets in mathematical morphology represent objects in an image. For example, the set of all black pixels in a binary image is a complete morphological description of the image.

Fig 1.12: Morphological processing

In binary images, the sets in question are members of the 2-D integer space Z^2, where each element of a set is a 2-D vector whose coordinates are the (x,y) coordinates of a black (or white) pixel in the image. Gray-scale digital images can be represented as sets whose components are in Z^3. In this case, two components of each element of the set refer to the coordinates of a pixel, and the third corresponds to its discrete gray-level value.

1.5.8 Segmentation

Segmentation procedures partition an image into its constituent parts or objects. In general, autonomous segmentation is one of the most difficult tasks in digital image processing. A rugged segmentation procedure brings the process a long way toward successful solution of imaging problems that require objects to be identified individually.

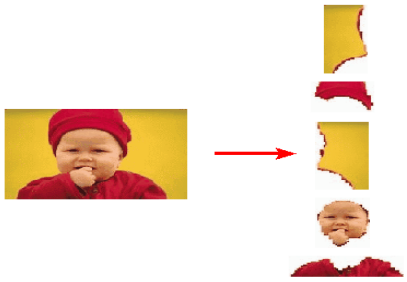


Fig 1.13: Segmentation

On the other hand, weak or erratic segmentation algorithms almost always guarantee eventual failure. In general, the more accurate the segmentation, the more likely recognition is to succeed.

1.5.9 Representation and description

Representation and description almost always follow the output of a segmentation stage, which usually is raw pixel data, constituting either the boundary of a region (i.e., the set of pixels separating one image region from another) or all the points in the region itself. In either case, converting the data to a form suitable for computer processing is necessary. The first decision that must be made is whether the data should be represented as a boundary or as a complete region. Boundary representation is appropriate when the focus is on external shape characteristics, such as corners and inflections.

Regional representation is appropriate when the focus is on internal properties, such as texture or skeletal shape. In some applications, these representations complement each other. Choosing a representation is only part of the solution for transforming raw data into a form suitable for subsequent computer processing. A method must also be specified for describing the data so that features of interest are highlighted. Description, also called feature selection, deals with

extracting attributes that result in some quantitative information of interest or are basic for differentiating one class of objects from another.

1.5.10 Object recognition

The last stage involves recognition and interpretation. Recognition is the process that assigns a label to an object based on the information provided by its descriptors. Interpretation involves assigning meaning to an ensemble of recognized objects.

1.5.11 Knowledgebase

Knowledge about a problem domain is coded into image processing system in the form of a knowledge database. This knowledge may be as simple as detailing regions of an image when the information of interests is known to be located, thus limiting the search that has to be conducted in seeking that information. The knowledge base also can be quite complex, such as an intern related to list of all major possible defects in a materials inspection problem or an image data base containing high resolution satellite images of a region in connection with change deletion application. In addition to guiding the operation of each processing module, the knowledge base also controls the interaction between modules. The system must be endowed with the knowledge to recognize the significance of the location of the string with respect to other components of an address field. This knowledge glides not only the operation of each module, but it also aids in feedback operations between modules through the knowledge base. We implemented preprocessing techniques using MATLAB.

Digital Image Analysis System

- A 2D image is nothing but a mapping from a region to a matrix
- A Digital Image Processing System consists of

1. Acquisition – scanners, digital camera, ultrasound,

   X-ray, MRI, PMT

2. Storage – HD (120GB), CD (700MB), DVD (4.7GB),

   Flash memory (512MB~4GB), 3.5” floppy diskettes,

i-pod, …

3. Processing Unit – PC, Workstation, PC-cluster

4. Communication – telephone lines, cable, wireless, …

5. Display – LCD monitor, laser printer, laser-jet printer.

1.6 COMPONENTS OF AN IMAGE PROCESSING

As recently as the mid-1980s, numerous models of image processing systems being sold throughout the world were rather substantial peripheral devices that attached to equally substantial host computers. Late in the 1980s and early in the 1990s, the market shifted to image processing hardware in the form of single boards designed to be compatible with industry standard buses and to fit into engineering workstation cabinets and personal computers. In addition to lowering costs, this market shift also served as a catalyst for a significant number of new companies whose specialty is the development of software written specifically for image processing.

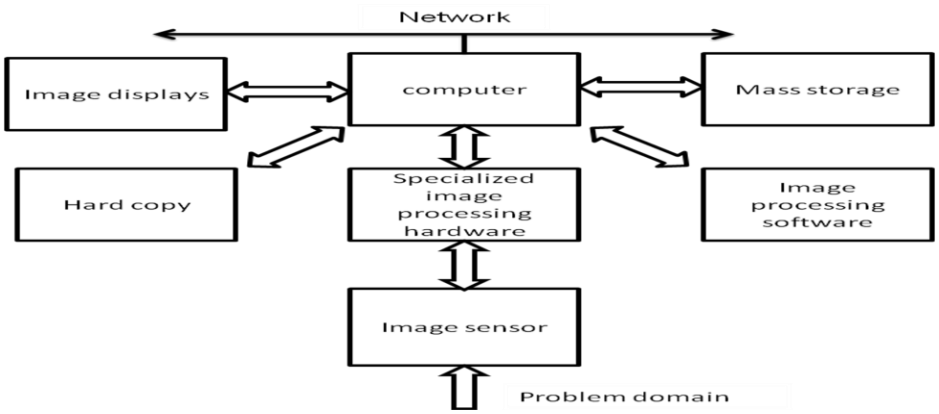


Fig 1.14: Components of image processing system

Although large-scale image processing systems still are being sold for massive imaging applications, such as processing of satellite images, the trend continues toward miniaturizing and blending of general-purpose small computers with specialized image processing hardware. Figure 1.2 shows the basic components comprising a typical general-purpose system used for digital image processing. The function of each component is discussed in the following paragraphs, starting with image sensing.

- **Image sensors**

With reference to sensing, two elements are required to acquire digital images. The first is a physical device that is sensitive to the energy radiated by the object we wish to image. The second, called a digitizer, is a device for converting the output of the physical sensing device into digital form. For instance, in a digital video camera, the sensors produce an electrical output proportional to light intensity. The digitizer converts these outputs to digital data.

- **Specialized image processing hardware**

Specialized image processing hardware usually consists of the digitizer just mentioned, plus hardware that performs other primitive operations, such as an arithmetic logic unit (ALU), which performs arithmetic and logical operations in parallel on entire images. One example of how an ALU is used is in averaging images as quickly as they are digitized, for the purpose of noise reduction. This type of hardware sometimes is called a front-end subsystem, and its most distinguishing characteristic is speed. In other words, this unit performs functions that require fast data throughputs (e.g., digitizing and averaging video images at 30 frames) that the typical main computer cannot handle.

- **Computer**

The computer in an image processing system is a general-purpose computer and can range from a PC to a supercomputer. In dedicated applications, sometimes specially designed computers are used to achieve a required level of performance, but our interest here is on general-purpose image processing systems. In these systems, almost any well-equipped PC-type machine is suitable for offline image processing tasks.

- **Image processing software**

Software for image processing consists of specialized modules that perform specific tasks. A well-designed package also includes the capability for the user to write code that, as a minimum, utilizes the specialized modules. More sophisticated software packages allow the integration of those modules and general-purpose software commands from at least one computer language.

- **Mass storage**

Mass storage capability is a must in image processing applications. An image of size 1024*1024 pixels, in which the intensity of each pixel is an 8-bit quantity, requires one megabyte of storage space if the image is not compressed. When dealing with thousands, or even millions, of images, providing adequate storage in an image processing system can be a challenge. Digital storage for image processing applications falls into three principal categories: (1) short-term storage for use during processing, (2) on-line storage for relatively fast recall, and (3) archival storage, characterized by infrequent access. Storage is measured in bytes (eight bits), Kbytes (one thousand bytes), Mbytes (one million bytes), Bytes (meaning giga, or one billion, bytes), and Bytes (meaning tera, or one trillion, bytes).

One method of providing short-term storage is computer memory. Another is by specialized boards, called frame buffers that store one or more images and can be accessed rapidly, usually at video rates. The latter method allows virtually instantaneous image zoom, as well as scroll (vertical shifts) and pan (horizontal shifts). Frame buffers usually are housed in the specialized image processing hardware unit shown in Fig. 1.24. Online storage generally takes the form of magnetic disks or optical-media storage. The key factor characterizing on-line storage is frequent access to the stored data. Finally, archival storage is characterized by massive storage requirements but infrequent need for access. Magnetic tapes and optical disks housed in "jukeboxes" are the usual media for archival applications.

- **Image displays**

Image displays in use today are mainly color (preferably flat screen) TV monitors. Monitors are driven by the outputs of image and graphics display cards that are an integral part of the computer system. Seldom are their requirements for image display applications that cannot be met by display cards available commercially as part of the computer system. In some cases, it is necessary to have stereo displays, and these are implemented in the form of headgear containing two small displays embedded in goggles worn by the user.

- **Hardcopy**

Hardcopy devices for recording images include laser printers, film cameras, heat-sensitive devices, inkjet units, and digital units, such as optical and CD-ROM disks. Film provides the

highest possible resolution, but paper is the obvious medium of choice for written material. For presentations, images are displayed on film transparencies or in a digital medium if image projection equipment is used. The latter approach is gaining acceptance as the standard for image presentations.

Network

Networking is almost a default function in any computer system in use today. Because of the large amount of data inherent in image processing applications, the key consideration in image transmission is bandwidth. In dedicated networks, this typically is not a problem, but communications with remote sites via the Internet are not always as efficient. Fortunately, this situation is improving quickly as a result of optical fiber and other broadband techniques.

CHAPTER-2

DATA HIDING

DATA HIDING

2.1 INTRODUCTION

"Data hiding is the technique in which the data is transfers through the image i.e. the data is not visible to us ". With the increasing popularity of digital media and network, tremendous information is transmitted over the Internet. For many cases, the delivered information may contain secret messages, such as confidential personal information, full credit card records or military satellite images, etc. If there is no security mechanism to protect these secret messages while delivering, it is easier to be accessed or grabbed illegally by someone who is interesting in those data. Encryption is a common technique for preventing data from being grabbed. The encrypted data can only be accessed when the correct key is loaded. For an encrypted digital media, though the original contents cannot be accessed, the scattered information already revealed the media are encrypted and may contain some valuable information. If the encrypted information is embedded into the digital media, the embedded media attract little attention from unexpected users, and subsequently prevent the embedded messages from being analyzed.

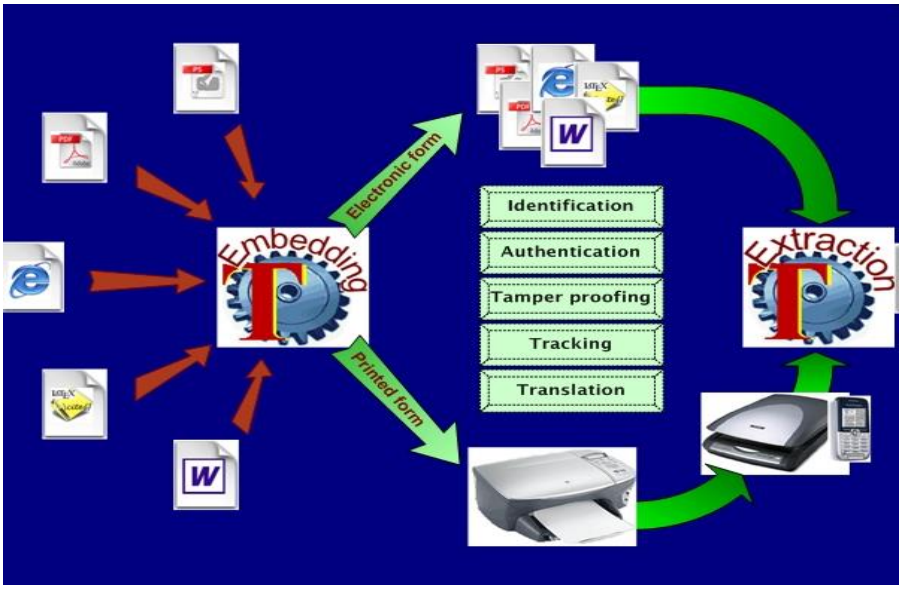


Figure 2.1: An Overview of Data hiding in image.

Since several years, the protection of multimedia data is becoming very important. The protection of this multimedia data can be done with encryption or data hiding algorithms. To decrease the

transmission time, the data compression is necessary. Since few years, a new problem is trying to combine in a single step, compression, encryption and data hiding. So far, few solutions have been proposed to combine image encryption and compression for example. Nowadays, a new challenge consists to embed data in encrypted images. Since the entropy of encrypted image is maximal, the embedding step, considered like noise, is not possible by using standard data hiding algorithms. A new idea is to apply reversible data hiding algorithms on encrypted images by wishing to remove the embedded data before the image decryption. Recent reversible data hiding methods have been proposed with high capacity, but these methods are not applicable on encrypted images. In this paper we propose an analysis of the local standard deviation of the marked encrypted images in order to remove the embedded data during the decryption step. We have applied our method on various images, and we show and analyze the obtained results.

Data hiding is an art of data concealment in which the presence of embedded messages cannot be detected. Digital images are often used for carrying data in many data hiding techniques because they are often delivered over the Internet. If a digital image is served as a message carrier, the image for carrying data is called a cover image, and the image that carried data is called a stego image. During data embedding, distortion of images occurs since the pixel values in the cover image will be inevitably changed. If the embedding algorithm has no capability to recover the distorted pixels back to their original ones, then this type of embedding is termed lossy embedding. On the other hand, if the stego image can be recovered to its original state after extracting the secret data, the corresponding embedding technique is termed lossless or reversible data hiding. Reversible data hiding techniques can be performed both in spatial domain and in compressed domain. (For spatial domain embedding, pixel values in the cover image are modified so that data can be embedded into pixels. Reversible data hiding of this domain often achieves larger payload because images in spatial domain provides rich redundancies, which are suitable for data embedding. For compressed domain embedding, data are embedded by modifying the compressed codes. For example, the index table of VQ-compressed codes can be modified for carrying data. Embedding data in compressed domain sometimes is preferred because compressed codes are beneficial for saving the storage space. However, these methods often suffer from lower payload and higher computational cost because they are performed in compressed domain, and redundancies in this domain are often smaller than those in the spatial domain.

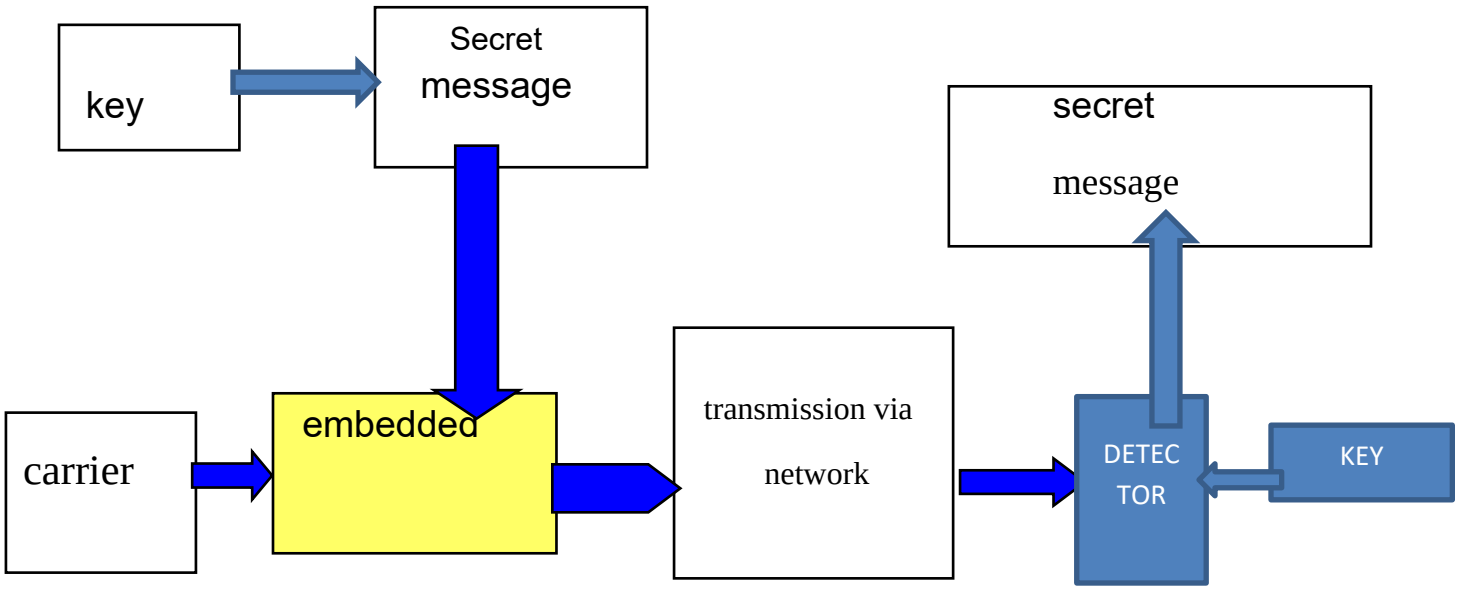


Figure 2.2: The Basic Block Diagram for Data Hiding Process.

- Relationship carrier - message
- Who extracts the message? (Source versus destination coding)
- How many recipients are there?
- Is the key a public knowledge or a shared secret?
- Do we embed different messages into one carrier?
- Embedding / detection bundled with a key in a tamper-proof hardware?
- Is the speed of embedding / detection important?

2.2 History & Various Techniques for Data Hiding

- First techniques included invisible ink, secret writing using chemicals, templates laid over text messages, microdots, changing letter/word/line/paragraph spacing, changing fonts.
- Images, video, and audio files provide sufficient redundancy for effective data hiding.
- Postscript files, PDF files, and HTML can also be used for non-robust data hiding to a limited extent.
- Executable files, provide very little space for data hiding.
- Fonts.

The earliest reversible data hiding technique reported in the literature is a pattern worked by Barton in 1997 (Barton, 1997). Barton compresses some overlaying bits and embeds them together with secret messages into a cover image. In the extraction phase, the overlaying data are decompressed and are used to recover the modified pixels. In 2002 and 2003, Fredrich et al. (2002) and Tian (2003) proposed remarkable reversible data hiding methods respectively, and have better payload with lower distortion than that of Barton's work. Alattar (2004) extended Tian's work by embedding n−1 bits into n pixels, so that the payload is increased from 1/2 bpp in Tian's method to (n−1)/n bpp. Kamstra and Heiman's (2005) also proposed an alternative of Tian's method using wavelet techniques and sorting, and have a better embedding efficiency than Tian's method. In 2006, Ni et al. (2006) proposed a reversible data hiding scheme based on the histogram-shifting technique. Their method achieves a high stego image quality; however, the embedding capacity is low and highly depends on the distribution of image histogram. In general, the higher the image histogram, the larger the embedding capacity could be achieved. Hodi and Rodriguez (2007) combining the difference-expansion and histogram-shifting technique, proposed an alternative method to improve the distortion performance at low embedding rate of Tian's method and has significant improvement in image quality and payload. In 2008, Lin et al. (2008) proposed another high-capacity reversible data hiding technique. They shifted the histogram of prediction errors and achieve a high embedding capacity. However, a considerable amount of side information has to be kept, thus the overall performance is degraded. In 2009, Kim et al. (2009) proposed a high-quality reversible data hiding scheme by exploiting spatial correlation between sub-sampled images. Data bits are embedded by modifying the difference histogram. In the same year, Hu et al. (2009) designed an embedding method based on expansion technique which allows

theirmethodto construct a location map with a good compressibility. Their method has higher image quality under the same embedding capacity compared to other expansion-based methods. Sachnev et al. (2009) also proposed a novel reversible data hiding method using sorting and prediction without using location map in most cases. Their method employs rhombus pattern prediction technique to obtain prediction errors. A sorting technique is then applied to these prediction errors based on the magnitude of the corresponding variance. Data are embedded by using the error-expansion and histogram-shifting techniques. Because the location map is not required in most cases, the payload of their method is significantly increased. Another reversible data hiding scheme based on modification of prediction errors was proposed by Tsai et al. in 2009 (Tsai et al., 2009). They selected a set of basic pixels as the predicted value of their neighbors and embed data bits into the histogram of prediction errors. In Tsai et al.'s method, pixel values are modified one grayscale at most to produce a high quality stego image; therefore, their method is suitable for applications requiring very low distortion such as medical imaging. However, Tsai et al.'s method does not fully exploit the correlation of neighboring pixels, leading to a less accuracy prediction results and subsequently reducing the amount of payload. Besides, their method does not consider the pixel activities in image blocks. Both smooth and complex blocks are processed using the same algorithm in the embedding phase, resulting in a considerable amount of image degradation. Although a high quality stego image can also be obtained in Hodi and Rodríguez (2007), Hu et al. (2009), Sachnevh et al. (2009) by limiting the changes of pixel values at most by one, their embedding algorithms are designed for general purpose and might not be optimized for applications requiring high quality image

.

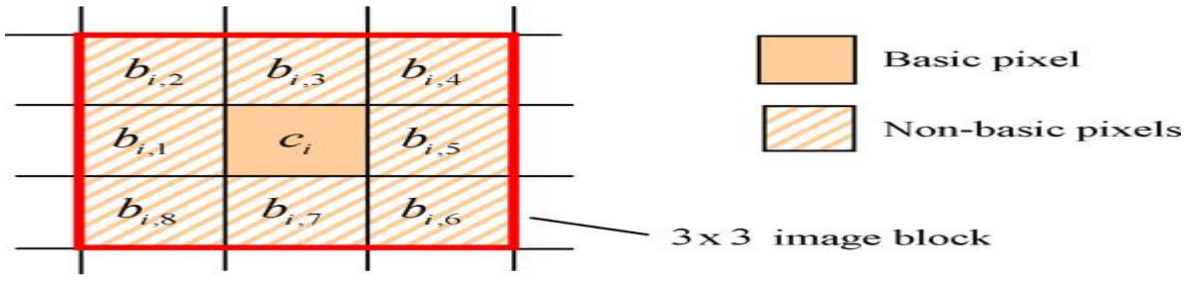


Fig2.3: A 3×3 image block in Tsai et al.'s method.

2.3 Need for Data Hiding

- Covert communication using images (secret message is hidden in a carrier image)
- Ownership of digital images, authentication, copyright
- Data integrity, fraud detection, self-correcting images
- Traitor-tracing (fingerprinting video-tapes)
- Adding captions to images, additional information, such as subtitles, to video, embedding subtitles or audio tracks to video (video-in-video)
- Intelligent browsers, automatic copyright information, viewing a movie in a given rated version
- Copy control (secondary protection for DVD).

2.4 Properties of Hiding Schemes

- **Robustness**

The ability to extract hidden information after common image processing operations: linear and nonlinear filters, lossy compression, contrast adjustment, recoloring, resampling, scaling, rotation, noise adding, cropping, printing / copying / scanning, D/A and A/D conversion, pixel permutation in small neighborhood, color quantization (as in palette images), skipping rows / columns, adding rows / columns, frame swapping, frame averaging (temporal averaging), etc.

- **Undetectability**

Impossibility to prove the presence of a hidden message. This concept is inherently tied to the statistical model of the carrier image. The ability to detect the presence does not automatically imply the ability to read the hidden message. Undetectability should not be mistaken for invisibility – a concept related to human perception.

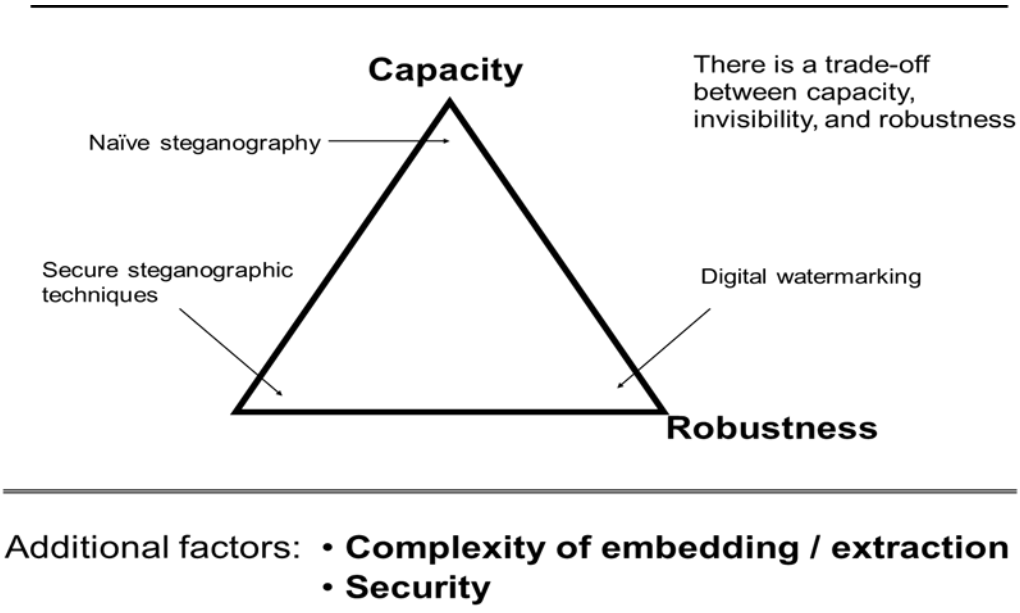
- **Invisibility**

Perceptual transparency. This concept is based on the properties of the human visual system or the human audio system.

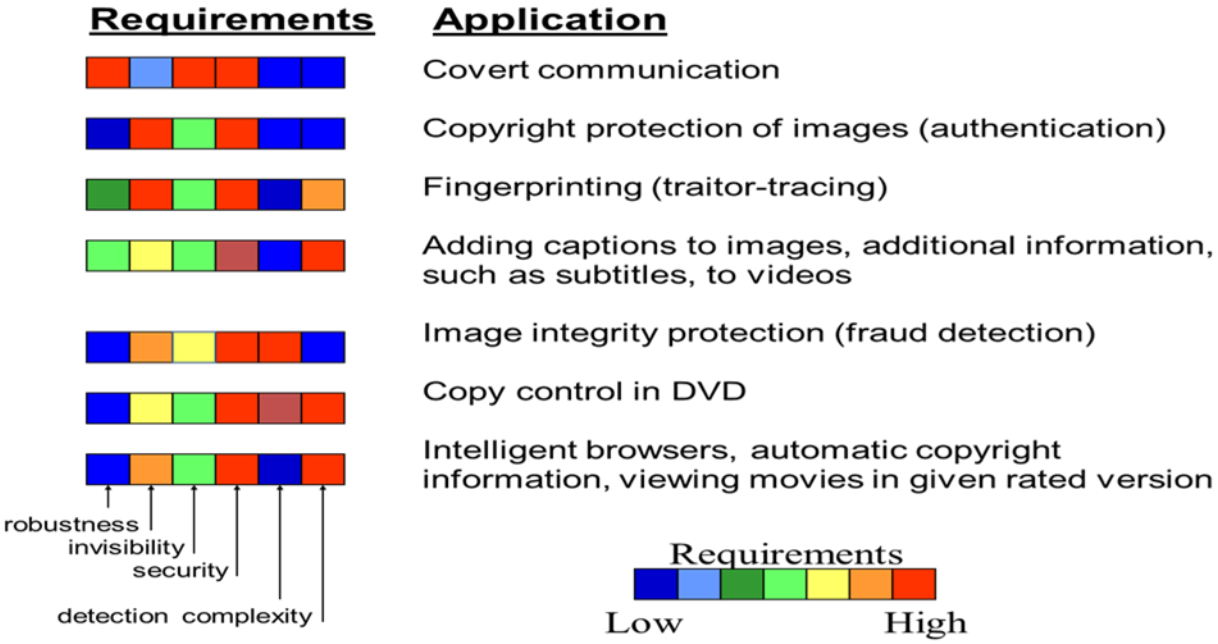
- **Security**

The embedded information cannot be removed beyond reliable detection by targeted attacks based on a full knowledge of the embedding algorithm and the detector (except a secret key), and the knowledge of at least one carrier with hidden message.

2.5 The "Magic" Triangle for Data hiding Techniques



2.6 A simple Color Code for Data Hiding with respect to Application



CHAPTER-3

METHODS FOR DATA HIDING

METHODS FOR DATA HIDING

3.1 INTRODUCTION

There are several methods are there for the purpose of to hide the data in an image. Basically, there are several popular methods are available to protect the Data such as

1.Cryptography.

2.Steganography.

3.Digital Water marking.

3.2 Cryptography

The earliest forms of information hiding can actually be considered to be highly crude forms of private-key cryptography; the "key" in this case being the knowledge of the method being employed (security through obscurity). Steganography books are filled with examples of such methods used throughout history. Greek messengers had messages tattooed into their shave head, concealing the message when their hair finally grew back. Wax tables were scraped down to bare wood where a message was scratched. Once the tablets were re-waxed, the hidden message was secure Over time these primitive cryptographic techniques improved, increasing both speed, capacity and security of the transmitted message.

Today, crypto-graphical techniques have reached a level of sophistication such that properly encrypted communications can be assumed secure well beyond the useful life of the information transmitted. In fact, it's projected that the most powerful algorithms using multi kilobit key lengths could not be comprised through brute force, even if all the computing power worldwide for the next 20 years was focused on the attack. Of course, the possibility exists that vulnerabilities could be found, or computing power breakthroughs could occur, but for most users in most applications, current cryptographic techniques are generally sufficient.

Why then pursue the field of information hiding? Several good reasons exist, the first being that "security through obscurity" isn't necessarily a bad thing, provided that it isn't the only security mechanism employed. Steganography for instance allows us to hide encrypted messages in mediums less likely to attract attention. A garble of random characters being transmitted between two users may tip off a watchful 3rd party that sensitive information is being transmitted; whereas baby pictures with some additional noise present may not. The underlying information in

the pictures is still encrypted, but attracts far less attention being distributed in the picture then it would otherwise.

This becomes particularly important as the technological disparity between individuals and organizations grows. Governments and businesses typically have access to more powerful systems and better encryption algorithms then individuals. Hence, the chance of individual's messages being broken increases which each passing year. Reducing the number of messages intercepted by the organizations as suspect will certainly help to improve privacy.

Another advantage hinted at by A. is that information hiding can fundamentally change the way that we think about information security. Cryptographic techniques generally rely on the metaphor of a piece of information being placed in a secure "box" and locked with a "key". The information itself is not disturbed and anyone with the proper key can gain access. Once the box is open, all of the information security is lost. Compare this to information hiding techniques where the key is embedded into, he information itself.

Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern ending, patience, determination, and luck. Cryptanalysts are also called attackers. Cryptology embraces both cryptography and cryptanalysis.

First, we start with a few definitions. Cryptography can be defined as the processing of information into an unintelligible (encrypted) form for the purposes of secure transmission. Through the use of a "key" the receiver can decode the encrypted message (decrypting) to retrieve the original message. Stenography improves on this by hiding the fact that a communication even occurred. The message m is imbedded into a harmless message c which is defined as the cover-object. The message m is then embedded into c, generally with use of a key k that is defined as the stego-key. The resulting message is then embedded into the cover-object c, which results in stego-objects.

3.2.1 Steganography

'Steganography is the art of hiding information in ways that prevent the detection of hidden messages,". Steganography means to hide secret information into innocent data. Digital images are ideal for hiding secret information. An image containing a secret message is called a cover image. First, the difference of the cover image and the stego image should be visually unnoticeable. The embedding itself should draw no extra attention to the stego image so that no hackers would try to extract the hidden message illegally. Second, the message hiding method should be reliable. It is impossible for someone to extract the hidden message if she/he does not have a special extracting method and a proper secret key. Third, the maximum length of the secret message that can be hidden should be as long as possible.

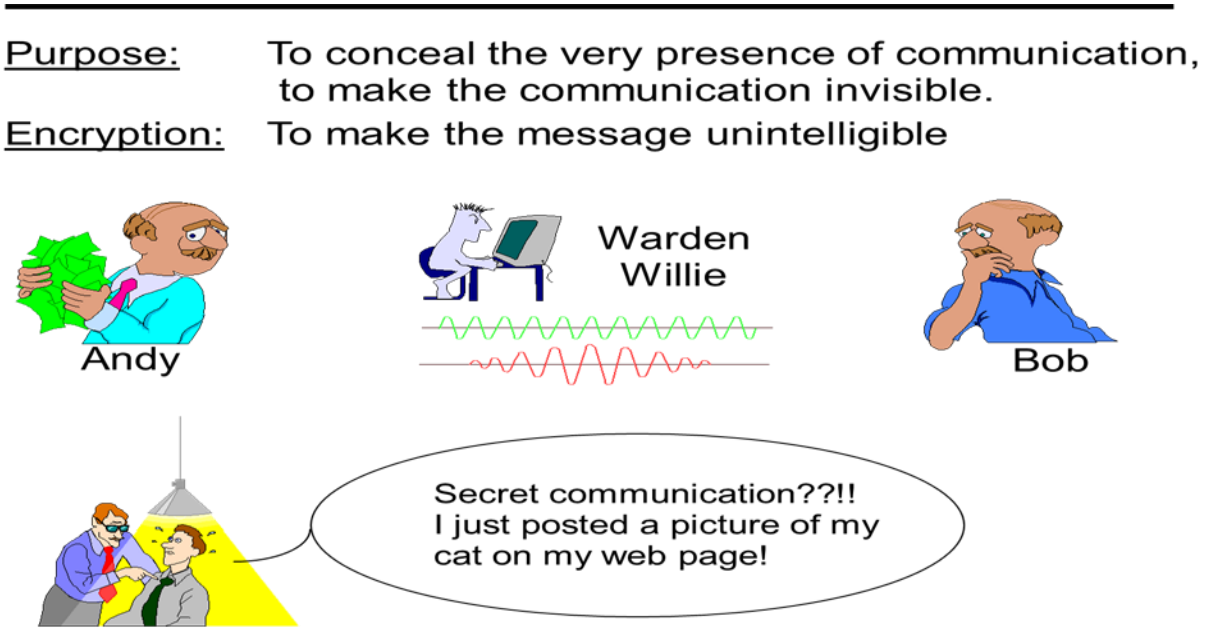


Figure3.1: Covert Communication

3.2.2 Steganography in History

Steganography comes from Greek and means "covered writing." The ancient Greeks wrote text on wax-covered tablets. To pass a hidden message, a person would scrape off the wax and write the message on the underlying wood. He/she would then once again cover the wood with wax so it appeared unused. Many developments in steganography occurred during World War II. This included the development of invisible inks, microdots, and encoded messages. One known message sent by a German spy was, apparently neutral's protest is thoroughly discounted and ignored. Is man hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suits and vegetables oils. Extracting second letter in each word reveals: Pershing sails from NY *June 1.*

3.2.3 Steganography in the Digital Age

Steganography is the art of secret communication. Its purpose is to hide the very presence of communication as opposed to cryptography whose goal is to make communication unintelligible to those who do not possess the right keys. Digital images, videos, sound files, and other computer files that contain perceptually irrelevant or redundant information can be used as "covers" or carriers to hide secret messages. After embedding a secret message into the cover-image, a so-called stego-image is obtained. It is important that the stego-image does not contain any easily detectable artifacts due to message embedding. A third party could use such artifacts as an indication that a secret message is present. Once this message detection can be reliably achieved, the steganography tool becomes useless.

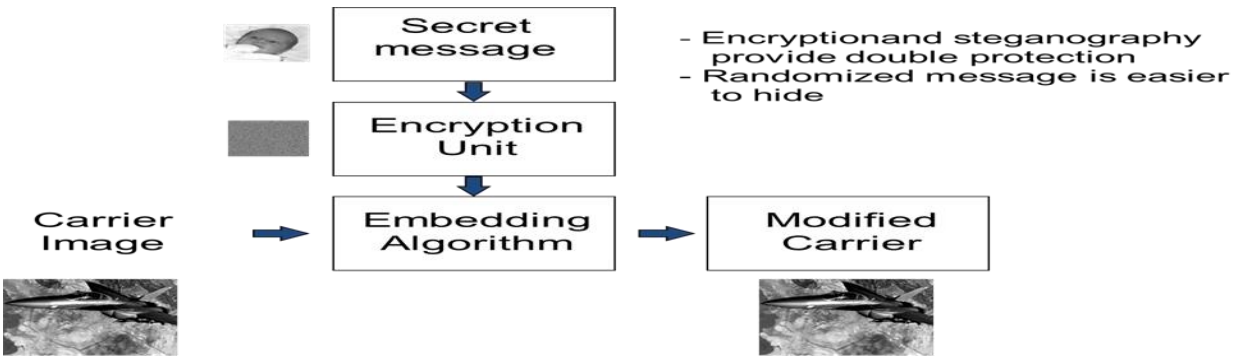


Figure3.2: Block Diagram for Covert Communication.

Obviously, the less information is embedded into the cover-image, the smaller the probability of introducing detectable artifacts by the embedding process. Another important factor is the choice of the cover-image. The selection is at the discretion of the person who sends the message. The sender should avoid using cover-images that would be easy to analyze for presence of secret messages. For example, one should not use computer art, charts, images with large areas of uniform color, images with only a few colors, and images with a unique semantic content, such as fonts. Although computer-generated fractal images may seem as good covers[6] because of their complexity and irregularity, they are generated by strict deterministic rules that may be easily violated by message embedding.

3.2.4 Basic Steganography Techniques

- Substitution techniques substitute redundant part of the cover-object with a secret message.
- Transform domain techniques embed secret message in a transform space of the signal (e.g., in the frequency domain).
- Spread spectrum techniques embed secret messages adopting ideas from spread spectrum communications.
- Statistical techniques embed messages by changing some statistical properties of the cover-objects and use hypothesis-testing methods in the extraction process.
- Distortion techniques store secret messages by signal distortion and measure the deviation from the original cover in the extraction step.
- Cover generation techniques do not embed messages in randomly chosen cover-objects, but create covers that fit a message that need to be hidden.

3.2.5 Steganography for RGB Images

This is Absolutely secure steganographic technique

Method: Embed a small message (8 bits), by repeated scanning of a cover image till a certain password-dependent message-digest function returns the required 8-tuple of bits.

Comments:

- Absolute secrecy tantamount to one time pad used in cryptography

- Guarantees correct noise distribution and undetectability.
- Time consuming, very limited capacity, not applicable to image carriers for which we only have one copy.

3.2.5.1 LSB Encoding Method

Method:

- Replace the LSB of each pixel with the secret message
- Pixels may be chosen randomly according to a secret key
- Pixels may be chosen adaptively according to neighborhood
- Message should always be encrypted

Comments:

- The simplest and most common steganographic technique
- Premise = changes to the least significant bit will be masked by noise commonly present in digital images.
- Color images provide more room for hiding messages
- If more than one LSB is used, statistically detectable changes may result
- A provably secure method should introduce changes *consistent*

with the noise model.

3.2.5.2 Steganography for palette images

LSB encoding cannot be directly applied to palette-based images because new colors, that are not present in the palette, would be created.

Two sources of palette images

1. Color truncation + dithering of photographs

2. Computer generated images (fractals, cartoons, animations).

Note: A secure steganographic method will produce modified carriers compatible with the source.

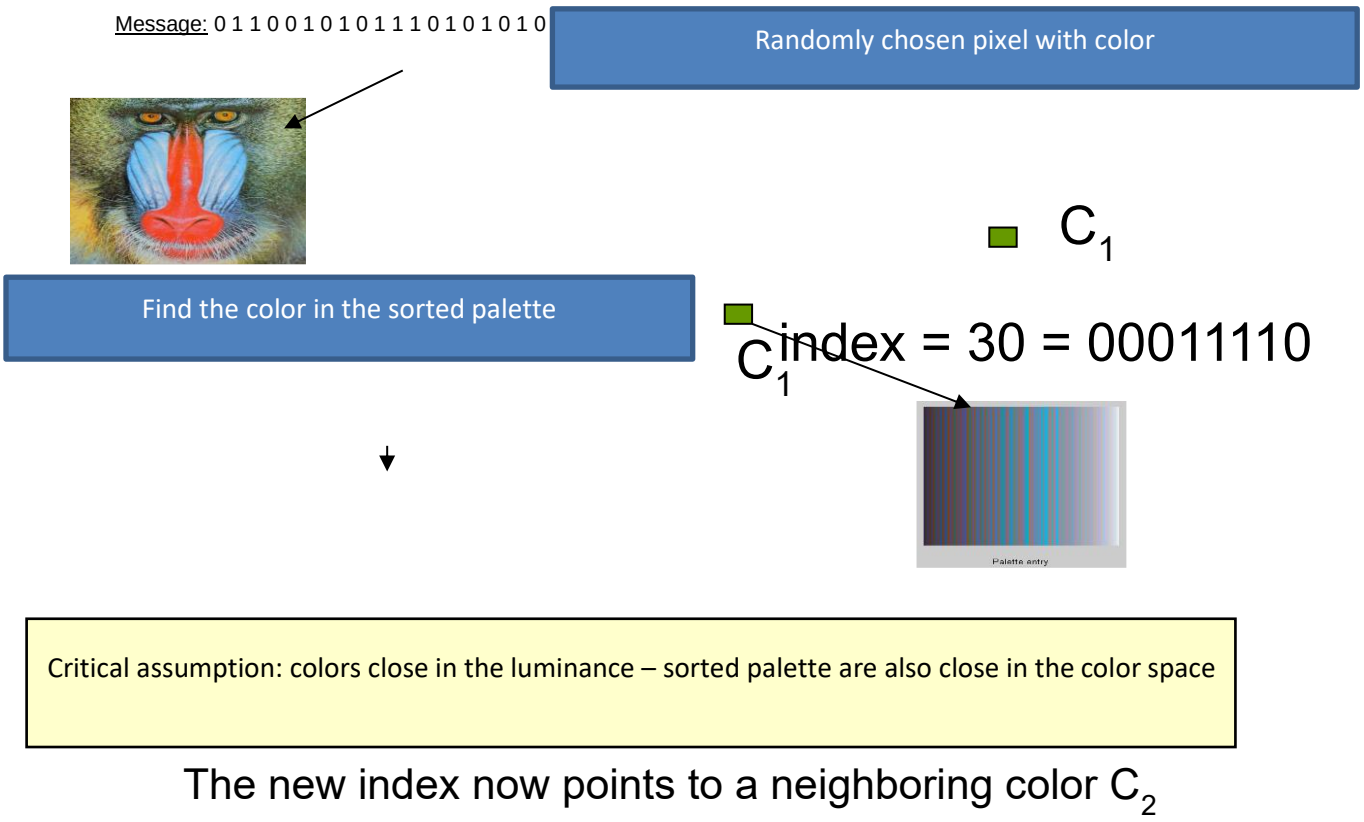


Fig 3.3 message hiding in the image data

3.2.6 Cryptography vs Steganography

Cryptography is the science of encrypting data in such a way that nobody can understand the encrypted message, whereas in steganography the existence of data is conceived means its presence cannot be noticed. The information to be hidden is embedded into the cover object which can be text, image, audio or video so that the appearance of cover object doesn't vary even after

the information is hidden. Information to be **hidden + cover object = stego object.** To add more security the data to be hidden is encrypted with a key before embedding. To extract the hidden information, one should have the key. A stego object is one, which looks exactly same as cover object with a hidden information. Here is a graphical version of the stegosystem:

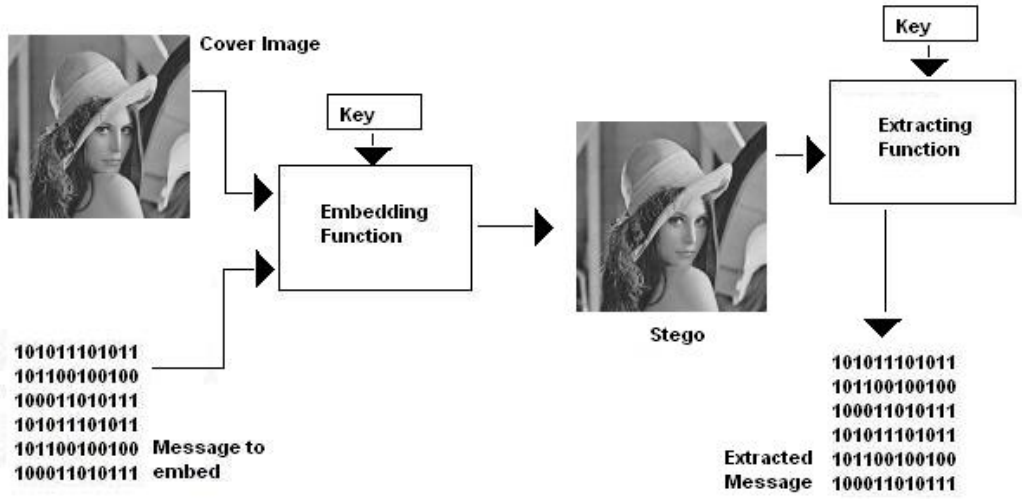


Fig3.4: stego system

Steganography refers to the science of "invisible" communication. Unlike cryptography, where the goal is to secure communications from an eavesdropper, steganographic techniques strive to hide the very presence of the message itself from an observer. Although steganography is an ancient subject, the modern formulation of it is often given in terms of the prisoner's problem where Alice and Bob are two inmates.

Who wish to communicate in order to hatch an escape plan? However, all communication between them is examined by the warden, Wendy, who will put them in solitary confinement at the slightest suspicion of covert communication. Specifically, in the general model for steganography, we have Alice wishing to send a secret message to Bob. In order to do so, she" embeds" into a cover-object, to obtain the stego-object.

The stego-object is then sent through the public channel. The warden, Wendy, who is free to examine all messages exchanged between Alice and Bob, can be *passive* or *active*. A passive warden simply examines the message and tries to determine if it potentially contains a hidden message. If it appears that it does, she then takes appropriate action, else, shelets the message through without any action. An active warden, on the other hand, can alter messages deliberately, even though she may not see any trace of a hidden message, in order to foil any secret communication that can nevertheless be occurring between Alice and Bob. The amount of change the warden is allowed to make depends on the model being used and the cover objects being employed. For example, with images, it would make sense that the warden is allowed to make changes as long as she does not alter significantly the subjective visual quality of a suspected stego-image.

It should be noted that the main goal of steganography is to communicate securely in a completely undetectable manner. That is, Wendy should not be able to distinguish in any sense between cover-objects (objects not containing any secret message) and stego-objects (objects containing a secret message). In this context, "*steganalysis*" refers to the body of techniques that are designed to distinguish between cover-objects and stego-objects. It should be noted that nothing might be gleaned about the contents of the secret message. When the existence of hidden message is known, revealing its content is not always necessary. Just disabling and rendering it useless will defeat the very purpose of steganography. In this paper, we present a stegoanalysis technique for detecting *stego-images*, i.e., still images containing hidden messages, using image quality metrics. Although we focus on images, the general techniques we discuss would also be applicable to audio and video media. Given the proliferation of digital images, and given the high degree of redundancy present in a digital representation of an image (despite compression), there has been an increased interest in using digital images as cover-objects for the purpose of steganography. The simplest of such techniques essentially embeds the message in a subset of the LSB (least significant bit) plane of the image, possibly after encryption. It is well known that an image is generally not visually affected when its least significant bit plane is changed. Popular steganographic tools based on LSB like embedding vary in their approach for hiding information. For example, Steganos and Stools use LSB embedding in the spatial domain, while Jsteg embeds in the frequency domain. Other more sophisticated techniques include the use of quantization and dithering. For a good survey of steganography techniques, the reader is referred to. What is

common to these techniques is that they assume a passive warden framework. That is they assume the warden Wendy will not alter the image. We collectively refer to these techniques as passive warden steganography techniques.

Conventional passive warden steganography techniques like LSB embedding are not useful in the presence of an active warden as the warden can simply randomize the LSB plane to thwart communication. In order to deal with an active warden Alice must embed her message in a robust manner. That is, Bob should be able to accurately recover the secret message despite operations like LSB randomizing, compression, filtering, and rotation by small degrees, etc. performed by the active warden Wendy. Indeed, the problem of embedding messages in a robust manner has been the subject of intense research in the image processing community, albeit for applications other than steganography, under the name of robust digital watermarking A robust digital watermark is an imperceptible signal added to digital content that can be later detected or extracted in order to make some assertion about the content. For example, the presence of her watermark can be used by Alice to assert ownership of the content. Recent years have seen an increasing interest in digital watermarking with many different applications ranging from copyright protection and digital rights management, to secret communication. Essentially robust digital watermarks provide a means of image-based steganography in the presence of an active warden since modifications made by the warden will not affect the embedded watermark as long as the visual appearance of the image is not significantly degraded. However, despite this obvious and commonly observed connection to steganography, there has been very little effort aimed at analyzing or evaluating the effectiveness of common robust watermarking techniques for steganographic applications. Instead, most work has focused on analyzing or evaluating the watermarking algorithms for their robustness against various kinds of attacks that try to remove or destroy them. However, if robust digital watermarks are to be used in active warden steganography applications, detection of their presence by an unauthorized agent defeats their very purpose. Even in applications that do not require hidden communication, but only robustness, we note that it would be desirable to first detect the possible presence of a watermark before trying to remove or manipulate it. This means that a given signal would have to be first analyzed for the presence of a watermark. In this project, we develop steganalysis techniques both for conventional LSB-like embedding used in the context of a passive warden model and for watermarking which can be used to embed secret messages in the context of an active warden. In order to distinguish between these two models, we will be using

the terms watermark and message when the embedded signal is in the context of an active warden and a passive warden, respectively. Furthermore, we simply use the terms marking or embedding when the context of discussion is general to include both active and passive warden steganography. The techniques we present are novel and to the best of our knowledge, the first attempt at designing general purpose tools for steganalysis. General detection techniques as applied to steganography have not been devised and methods beyond visual inspection and specific statistical tests for individual techniques like LSB embedding are not present in the literature. Since too many images have to be inspected visually to sense hidden messages, the development of a technique to automate the detection process will be very valuable to the steganalyst. Our approach is based on the fact that hiding information in digital media requires alterations of the signal properties that introduce some form of degradation, no matter how small. These degradations can act as signatures that could be used to reveal the existence of a hidden message. For example, in the context of digital watermarking, the general underlying idea is to create a watermarked signal that is perceptually identical but statistically different from the host signal. A decoder uses this statistical difference in order to detect the watermark. However, the very same statistical difference that is created could potentially be exploited to determine if a given image is watermarked or not.

3.3 Image Watermarking

The main goal of watermarking is to hide a message m in some audio or video (cover) data d, to obtain new data d', practically indistinguishable from d, by people, in such a way that an eavesdropper cannot remove or replace m in d'.

Figure3.5: Digital water marking images.

3.3.1 History of Water Marking Systems

Paper watermarks appeared in the art of handmade paper marking 700 hundred years ago. Watermarks were mainly used to identify the mill producing the paper and paper format, quality and strength. Paper watermarks was a perfect technique to eliminate confusion from which mill paper is and what are its parameters. Legal power of watermarks has been demonstrated in 1887 in France when watermarks of two letters, presented as a piece of evidence in a trial, proved that the letters had been predated, what resulted in the downfall of a cabinet and, finally, the resignation of the president Grévy. Paper watermarks in bank notes or stamps inspired the first use of the term *water mark* in the context of digital data. The first publications that really focused on watermarking of digital images were from 1990 and then in 1993.

3.3.2 Water marking Methods

- Visible Water marking
- Invisible Water marking

3.3.3 Visible Water Marking

- Content producer does not like to degrade the image
- Customers don’t appreciate them either
- Visible watermarks are easier to remove
- Easy to detect for people
- But more difficult to detect automatically.

3.3.4 Invisible Watermark

- There is no perceptible difference between the original and watermarked image.
- But the difference image looks interesting.
- The watermark is present everywhere.

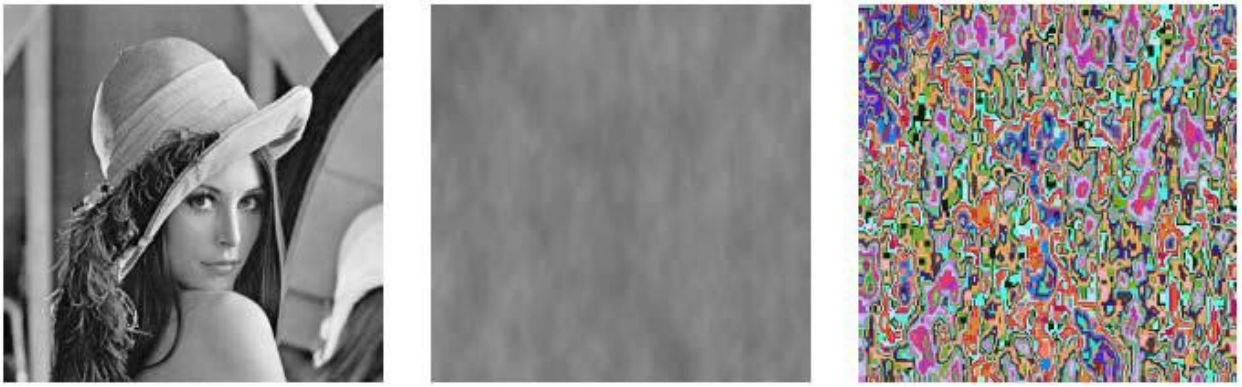


Fig 3.6: Invisible Watermark

3.3.5 Image Watermarking

- Non-removable Difficult or even impossible to be removed by a hacker, at least without obviously degrading the original signal
- Robustness Survive under lossy compression and other signal processing's
- Unambiguous Retrieval of watermark should unambiguously identify the owner, and the accuracy of identification should only degrade gracefully in the face of attack.
- Imperceptible or Transparency Not affect the viewing experience of the image.

3.3.6 Multimedia Watermarking

Video:

- Correlation Based Techniques
- Video Watermarking by Parity Bit Modification
- VLC based
- Future Watermarking working

Audio:

- Using acoustic model and masking effect to embed the signal into the imperceptible part.
- Commercial detection.

3.3.7 Embedding and recovery systems in water marking systems

The below Figure shows the basic scheme of the watermarks embedding systems.

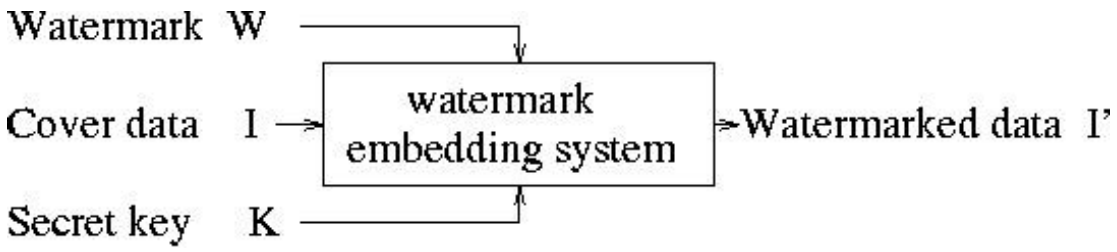


Figure 3.7: Watermark embedding scheme.

Inputs to the scheme are the watermark, the cover data and an optional public or secret key. The output are watermarked data. The key is used to enforce security. The below Figure shows the basic scheme for watermark recovery schemes.

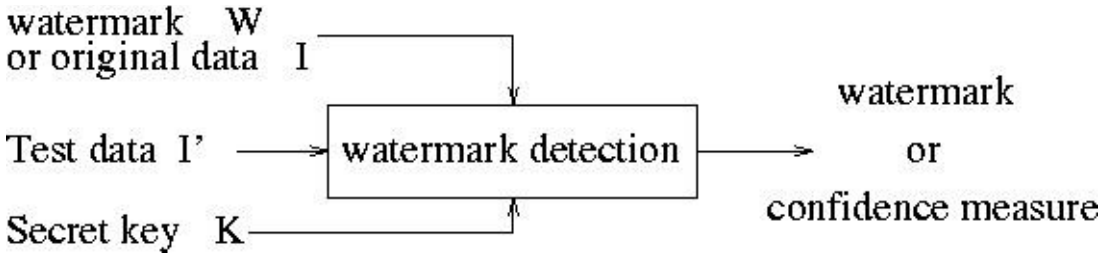


Figure3.8 : Watermark recovery scheme

Inputs to the scheme are the watermarked data, the secret or public key and, depending on the method, the original data and/or the original watermark. The output is the recovered watermarked *W* or some kind of confidence measure indicating how likely it is for the given watermark at the input to be present in the data under inspection.

3.4 TYPES OF WATERMARKING SCHEMES

Private (non-blind) watermarking systems require for extraction/detection the original cover-data.

· Type I systems use the original cover-data to extract the watermark from stego-data and use original cover-data to determine where the watermark is.

· Type II systems require a copy of the embedded watermark for extraction and just yield a yes/no answer to the question whether stego-data contains a watermark..

Semi-private (semi-blind) watermarking does not use the original cover-data for detection, but tries to answer the same question. (Potential application of blind and semi-blind watermarking is for evidence in court ownership,)

Public (blind) watermarking - neither cover-data nor embedded watermarks are required for extraction - this is the most challenging problem.

3.5 INVISIBLE COMMUNICATIONS

We describe some important cases of information hiding.

Subliminal channels. We have seen how to use a digital signature scheme to establish a subliminal cannel for communication.

Covert channels in operating systems. Covert channels can arise when one part of the system, operating at a specific security level, is able to supply a service to another system part with a possibly different security level.

Video communicating systems. Steganography can be used to embed secret messages into a video stream recorded by videoconferencing systems.

Data hiding in executable files. Executable files contain a lot of redundancies in the way independent instructions are scheduled or an instruction subset is chosen to solve a specific problem. This can be utilized to hide messages.

3.6 SECRET SHARING by SECRET HIDING

A simple technique has been developed, by Naor and Shamir, that allows for a given n and $t < n$ to hide any secret (image) message m in images on transparencies in such a way that each of n parties receives one transparency and

- not -1 parties are able to obtain the message m from the transparencies they have.

- any *t* of the parties can easily get (read or see) the message *m* just by stacking their transparencies together and aligning them carefully.

TO REMEMBER !!!

There is no use in trying, she said: one cannot believe impossible things.

I dare to say that you have not had much practice, said the queen,

When I was your age, I always did it for half-an-hour a day and sometimes I have believed as many as six impossible things before breakfast.

Lewis Carroll: Through the Looking-glass, 1872.

CHAPTER-4

IMAGE TRANSFORM TECHNIQUES

IMAGE TRANSFORM TECHNIQUES

4.1 INTRODUCTION

The choice of a particular transform in a given application depends on the amount of reconstruction error that can be tolerated and the computational resources available. Compression is achieved during the quantization of the transformed coefficients not during the transformation step. Image modeling or transformation is aimed at the exploitation of statistical characteristics of the image (i.e., high correlation, redundancy).

4.2 Some transform techniques

- Fourier Transform (FFT, DFT, WFT)
- Discrete Cosine Transform (DCT)
- Walsh-Hadamard Transform (WHT)
- Wavelet Transform (CWT, DWT, FWT)

For Fourier Transform and DCT basis images are fixed i.e. they are input independent and sinusoidal (cosines and sines) in nature. Provides frequency view i.e. provide frequency information and temporal information is lost in transformation process. WHT is non-sinusoidal in nature and easy to implement. (Frequency domain) Wavelet Transforms provides time-frequency view i.e., provides both frequency as well as temporal (localization) information. Wavelets give time-scale viewpoint and exhibits multiresolution characteristics. Fourier is good for periodic or stationary signals but Wavelet is good for transients i.e., for non-stationary data. Localization property allows wavelets to give efficient representation of transients. 2. Fourier Transform Since the Fourier Transform is widely used in analyzing and interpreting signals and images, I will first have a survey on it prior to going further to the Wavelet Transform. The tool which converts a spatial (real space) description of an image into one in terms of its frequency components is called the Fourier transform. Through Fourier Transform, it is possible to compose a signal by superposing a series of sine and cosine functions. These sine and cosine functions are known as basis functions (Figure 2.2.1) and are mutually orthogonal. The transform decomposes the signal into the basis functions, which means that it determines the contribution of each basis function in the structure of the original signal. These individual contributions are called the Fourier

coefficients. Reconstruction of the original signal from its Fourier coefficients is accomplished by multiplying each basis function with its corresponding coefficient and adding them up together, i.e., a linear superposition of the basic functions. Fourier Analysis and Orthogonality Fourier analysis is one of the most widely used tools in spectral analysis. The basis for this analysis is the Fourier Integral, which computes the amplitude spectral density F(ω) of a time-domain signal f(t).

$$F(\omega) = \int_{-\infty}^{\infty} f(t) \exp(-j\omega t)\, dt$$

F(ω) is actually complex, so one obtains the amplitude spectral density A(f) and phase spectral density φ(f) as a function of frequency. Another way of looking at the Fourier transform is that it answers the question: what continuous distribution of sine waves. A (f) cos(jωt+ φ(f)) when added together on a continuous basis best represents the original time signal? We call these distributions the amplitude and phase spectral densities (or spectra). Complex exponentials are popular basis functions because in many engineering and science problems, the relevant signals are sinusoidal in nature. It is noticed that when signals are not sinusoidal in nature, a wide spectrum of the basis function is needed in order to represent the time signal accurately. An important property of any family of basis functions ψ(t) is that it is orthogonal.

The basic functions in the Fourier Transform are **$\psi(t) = \exp(+j\omega t)$**, so the Fourier Transform could be more generally written as

$$F(\omega) = \int_{-\infty}^{\infty} f(t) \psi^{*}(t)\, dt$$

where * denotes complex conjugate. The test for orthogonality is done as follows

$$\int_{-\infty}^{\infty} \psi_m(t) \psi_n^{*}(t)\, dt = \begin{cases} k & m = n \\ 0 & m \neq n \end{cases}$$

For complex exponentials, because they are infinite in duration, one end up with k=∞, when m=n so it is necessary to define the orthogonality test in a different way:

$$\lim_{T \to \infty} \frac{1}{T} \int_{-T/2}^{T/2} \psi_m(t) \psi_n^{*}(t)\, dt = \begin{cases} k & m = n \\ 0 & m \neq n \end{cases}$$

For **complex exponential**, this becomes:

$$\lim_{T \to \infty} \frac{1}{T} \int_{-T/2}^{T/2} \exp(j\omega_m t) \exp(-j\omega_n t)\, dt = \lim_{T \to \infty} \frac{\sin(T[\omega_m - \omega_n]/2)}{T[\omega_m - \omega_n]/2} = \begin{cases} 1 & m = n \\ 0 & m \neq n \end{cases}$$

When the constant k=1, the function is said to be orthonormal.

Various types of signals can be analyzed with the Fourier Transform. If f(t) is periodic, then the amplitude spectral density clusters at discrete frequencies that are harmonics (integer multiples) of the fundamental frequency. One need to invoke Dirac Delta functions if the Fourier Transform is used– otherwise Fourier series coefficients can be computed and same result can be obtained. If f (t) is deterministic and discrete, the discrete time Fourier Transform (DTFT) may be used to generate a periodic frequency response. If f(t) is assumed to be both periodic and discrete, then the discrete Fourier Transform (DFT), or its fast numeric equivalent the FFT may be applied to compute the spectrum. If f(t) is random, then in general one will have a difficult time of computing the Fourier Integral of the random 'data'. Hence treat the input as data and use an FFT, but the result of doing so is a random spectrum. This single random spectrum can give an idea of the frequency response, but in many instances it can be misleading. A better approach is to take the average of the random spectra. This leads to the formulation of power spectral density, which is an average over the FFT magnitude spectrum squared.

In certain signals, both random and deterministic, we are interested in the spectrum as a function of time in the signal. This suggests finding the spectrum over a limited time bin, moving the bin (sometimes with overlap, sometimes without), re-computing the spectrum, and so on. This method is known as the short-time Fourier Transform (STFT), or the Gabor Transform.

Discrete Fourier Transform (DFT) is an estimation of the Fourier Transform, which uses a finite number of sample points of the original signal to estimate the Fourier Transform of it. The order of computation cost for the DFT is in order of O (n^2), where n is the length of the signal.

Fast Fourier Transform (FFT) is an efficient implementation of the Discrete Fourier Transform, which can be applied to the signal if the samples are uniformly spaced. FFT reduces the computation complexity to the order of O(nlogn) by taking advantage of self similarity properties of the DFT.**If the input is a non-periodic signal**, the superposition of the periodic basis functions does not accurately represent the signal. One way to overcome this problem is to extend the signal at both ends to make it periodic.

Another solution is to use **Windowed Fourier Transform (WFT)**. In this method the signal is multiplied with a window function (in below Figure) prior to applying the Fourier transform. The window function localizes the signal in time by putting the emphasis in the middle of the window and attenuating the signal to zero towards both ends.

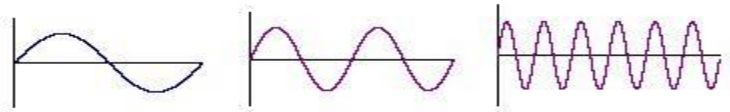
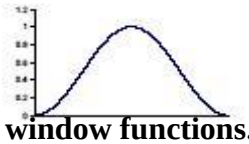
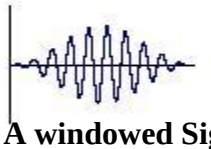


Figure4.1: A Set of Fourier basis functions.



A window functions.



A windowed Signal.

4.3 Discrete Cosine Transform (DCT)

The discrete cosine transform (DCT) helps separate the image into parts (or spectral sub-bands) of differing importance (with respect to the image's visual quality). The DCT is similar to the discrete Fourier transform: it transforms a signal or image from the spatial domain to the frequency domain.

With an input image, A, the coefficients for the output "image," B, are:

$$B(k_1, k_2) = \sum_{i=0}^{N_1-1} \sum_{J=0}^{N_2-1} 4.A(i,j).\cos\left[\frac{\pi.k_1}{2.N_1}.(2.i+1)\right].\cos\left[\frac{\pi.k_2}{2.N_2}.(2.j+1)\right]$$

The input image is N_2 pixels wide by N_1 pixels high; A (i, j) is the intensity of the pixel in row i and column j; B (k_1, k_2) is the DCT coefficient in row k1 and column k2 of the DCT matrix. All DCT multiplications are real. This lowers the number of required multiplications, as compared to the discrete Fourier transform. The DCT input is an 8 by 8 array of integers. This array contains each pixel's gray scale level; 8-bit pixels have levels from 0 to 255. The output array of DCT coefficients contains integers; these can range from -1024 to 1023. For most images, much of the signal energy lies at low frequencies; these appear in the upper left corner of the DCT. The lower

right values represent higher frequencies, and are often small - small enough to be neglected with little visible distortion. It is computationally easier to implement and more efficient to regard the DCT as a set of **basis functions** which given a known input array size (8 x 8) can be pre-computed and stored. This involves simply computing values for a convolution mask (8 x8 window) that get applied (sum values x pixel the window overlaps with image apply window across all rows/columns of image). The values as simply calculated from the DCT formula. The 64 (8 x 8) DCT basis functions are there. Most software implementations use fixed point arithmetic. Some fast implementations approximate coefficients so all multiplies are shifts and adds.

4.4 DCT Vs Fourier:

- DCT is similar to the Fast Fourier Transform (FFT), but can approximate lines well with fewer coefficients.
- DCT (Discrete Cosine Transform) is actually a cut-down version of the FFT i.e., it is only the real part of FFT.
- DCT Computationally simpler than FFT and much effective for Multimedia Compression.
- DCT is associated with very less MSE value in comparison to others.
- DCT has best information packing ability.

- DCT minimizes the block like appearance (blocking articrafts), that results when the boundaries between the sub-images become visible. But DFT gives rise to boundary discontinuities.

4.5 Wavelet Transform:

Wavelet means ‘small wave’. So, wavelet analysis is about analyzing signal with short duration finite energy functions. They transform the signal under investigation in to another representation which presents the signal in more useful form. This transformation of the signal is called Wavelet Transform [1,7,10] i.e., Wavelet Transforms are based on small waves, called wavelets, of varying frequency and limited duration. Unlike the Fourier transform, we have a variety of wavelets that are used for signal analysis. Choice of a particular wavelet depends on the type of application in hand. Wavelet Transforms provides time-frequency view i.e., provides both frequency as well as temporal (localization) information and exhibits multiresolution characteristics. Fourier is good for periodic or stationary signals and Wavelet is good for transients. Localization property allows

wavelets to give efficient representation of transients. In Wavelet transforms a signal can be converted and manipulated while keeping resolution across the entire signal and still based in time i.e., Wavelets have special ability to examine signals simultaneously in both time and frequency. Wavelets are mathematical functions that satisfy certain criteria, like a zero mean, and are used for analyzing and representing signals or other functions. A set of dilations and Translations of a chosen mother wavelet is used for the spatial/frequency analysis of an input signal. The Wavelet Transform uses overlapping functions of variable size for analysis. The overlapping nature of the transform alleviates the blocking artifacts, as each input sample contributes to several samples of the output. The variable size of the basic functions, in addition, leads to superior energy compaction and good perceptual quality of the decompressed image. Wavelets Transform is based on the concept of sub-band coding.

The current applications of wavelet include statistical signal processing, Image processing, climate analysis, financial time series analysis, heart monitoring, seismic signal de- noising, de-noising of astronomical images, audio and video compression, compression of medical image stacks, finger print analysis, fast solution of partial differential equations, computer graphics and so on.

4.6 Wavelets Vs Fourier and DCT:

- Fourier and DCT transforms converts a signal from time Vs amplitude to frequency Vs amplitude i.e., provides only frequency information and temporal information is lost during transformation process. But Wavelet transforms provides both frequency as well as temporal (localization) information.

- In Fourier and DCT basis functions are sinusoids (sine and cosine) and cosines respectively but in Wavelet Transform basis functions are various wavelets.
- Since Wavelet Transforms are both computationally efficient and inherently local (i.e.). there basis functions are limited in duration), subdivision of original image before applying transformation is not required as required in DCT and others.

- The removal of subdivision step in Wavelet Transform eliminates the blocking anticraft but FFT suffers from it. This property also characterizes DCT-based approximation, at higher compression ratios.
- Wavelets provide unconditional basis for large signal class. Wavelet coefficients drops sharply hence good for compression, de-noising, detection and recognition.
- Fourier is good for periodic or stationary signals. Wavelet is good for transients. Localization property allows wavelets to give efficient representation of transients.
- Wavelets have local description and separation of signal characteristics. Fourier puts localization information in the phase in a complicated way. STFT cannot give localization and orthogonality.
- Wavelets can be adjusted or adapted to application.
- Computation of wavelet coefficients is well suited to computer. No derivatives of integrals needed as required in Fourier and DCT and hence turn out to be a digital filter bank.

CHAPTER-5

DISCRETE WAVELET TRANSFROM

DISCRETE WAVELET TRANSFORM

5.1 INTRODUCTION TO DISCRETE WAVELET TRANSFORM

Wavelet is a „small wave". It is a special kind of function which exhibits oscillatory behavior for a short period of time and then dies out. In signal processing using Fourier transform, the signal is decomposed into a series of sines or cosines. It is impossible to know simultaneously the exact frequency and the exact time of occurrence of that particular frequency in a signal. In order to know the frequency, the signal must be spread in time, or vice versa. A solution is to split the signal up into components that are not sine or cosine waves. A single function and its dilations and translations may be used to generate a set of orthonormal basis functions to represent a signal. This would help to condense the information in both the time and frequency domains. This idea led to the introduction of wavelets. Figure 6.1 shows the example of a wavelet.

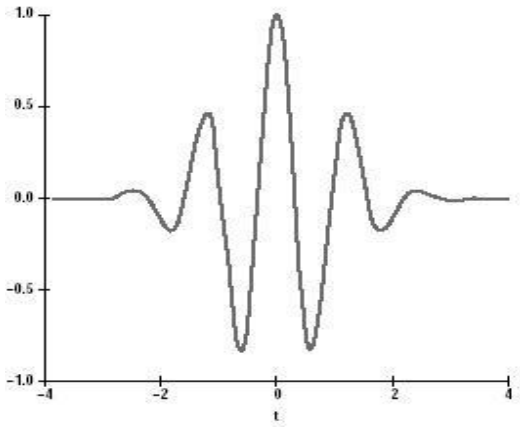


Figure 5.1. Morlet Wavelet

Wavelets (Soman, Ramachandran, & Rasmi, 2010) can be manipulated in two ways – by translation and by scaling. In translation, the central position of the wavelet is changed along the time axis. In scaling, its frequency is changed.

Figures 5.2 and 5.3 show the translated and scaled versions of a wavelet.

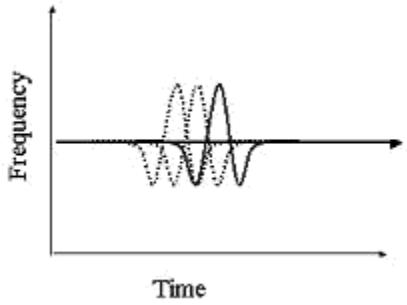


Figure 5.2. Translation of a Wavelet

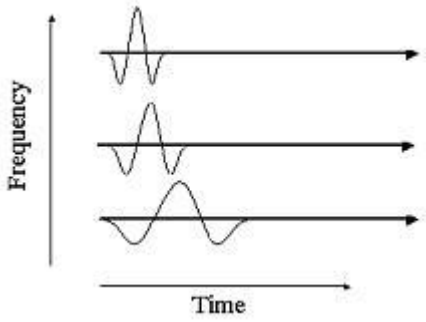


Figure 5.3: Scaling of a Wavelet

CHAPTER-6

PROPOSED METHOD

PROPOSED METHOD

6.1 INTRODUCTION

DATA hiding technique aims to embed some secret information into a carrier signal by altering the insignificant components for copyright protection or covert communication. In general cases, the data-hiding operation will result in distortion in the host signal. However, such distortion, no matter how small it is, is unacceptable to some applications, e.g., military or medical images. In this case it is imperative to embed the additional secret message with a reversible manner so that the original contents can be perfectly restored after extraction of the hidden data. A number of reversible data hiding techniques have been proposed, and they can be roughly classified into three types: lossless compression-based methods, difference expansion (DE) methods, and histogram modification (HM) methods. The lossless compression-based methods make use of statistical redundancy of the host media by performing lossless compression in order to create a spare space to accommodate additional secret data.

In this project we propose a robust blind private watermarking algorithm for image Copyright protection. The algorithm is based on Wavelet Packets. Our basic idea is to decompose the original image into a series of details at different scales by using Wavelet Packets; a binary image used as a watermark is then embedded into the different levels of details.

The embedding process includes: usage of a unique (secret) binary identification key to select the Wavelet decomposition scheme, Wavelet Packet decomposition, selection of the Wavelet coefficient groups to be used for hiding the watermark, insertion of the watermark in the corresponding group of coefficients by modifying the mean value of the group and Inverse Wavelet Transform. Experiments showed that our algorithm does only minimal degradation to the original image and can improve the robustness of watermarking against different attacks.

Digital watermarking is the act of hiding a message related to a digital signal (i.e., an image, song, video) within the signal itself. It is a concept closely related to steganography, in that they both hide a message inside a digital signal. However, what separates them is their goal. Watermarking tries to hide a message related to the actual content of the digital signal, while in steganography the digital signal has no relation to the message, and it is merely used as a cover to hide its existence. Watermarking has been around for several centuries, in the form of watermarks found initially in plain paper and subsequently in paper bills. However, the field of digital watermarking was only developed during the last 15 years and it is now being used for many

different applications. In the following sections I will present some of the most important applications of digital watermarking, explain some key properties that are desirable in a watermarking system, and give an overview of the most common models of watermarking as presented in the book by Ingemar Cox, Matthew Miller, Jeffrey Bloom, Jessica Friedrich and Ton Kalker. These basic models will be further illustrated by the use of example watermarking systems that were developed in MATLAB.

6.2 Watermarking properties

Every watermarking system has some very important desirable properties. Some of these properties are often conflicting and we are often forced to accept some tradeoffs between these properties depending on the application of the watermarking system. The first and perhaps most important property is effectiveness. This is the probability that the message in a watermarked image will be correctly detected. We ideally need this probability to be 1. Another important property is the image fidelity. Watermarking is a process that alters an original image to add a message to it, therefore it inevitably affects the image's quality. We want to keep this degradation of the image's quality to a minimum, so no obvious difference in the image's fidelity can be noticed. The third property is the payload size. Every watermarked work is used to carry a message. The size of this message is often important as many systems require a relatively big payload to be embedded in a cover work. There are of course applications that only need a single bit to be embedded. The false positive rate is also very important to watermarking systems. This is the number of digital works that are identified to have a watermark embedded when in fact they have no watermark embedded. This should be kept very low for watermarking systems. Lastly, robustness is crucial for most watermarking systems. There are many cases in which a watermarked work is altered during its lifetime, either by transmission over a lossy channel or several malicious attacks that try to remove the watermark or make it undetectable. A robust watermark should be able to withstand additive Gaussian noise, compression, printing and scanning, rotation, scaling, cropping and many other operations.

A watermark is a recognizable image or pattern in paper that appears as various shades of lightness/darkness when viewed by transmitted light (or when viewed by reflected light, a dark background), caused by thickness or density variations in the paper. There are two main ways of producing watermarks in paper; the dandy roll process and complex cylinder mold process. Watermarks are often used as security features of bank notes, passports, postage stamps and other

documents to prevent counterfeiting. Watermark is very useful in the examination paper because it can be used for dating, identifying sizes, mill trademarks and locations, and the quality of a paper. We are living in the era of information where billions of bits of data is created in every fraction of a second and with the advent of internet, creation and delivery of digital data (images, video and audio files, digital repositories and libraries, web publishing) has grown many fold. Since copying a digital data is very easy and fast too so, issues like, protection of rights of the content and proving ownership, arises. Digital watermarking came as a technique and a tool to overcome shortcomings of current copyright laws for digital data. The specialty of watermark is that it remains intact to the cover work even if it is copied. So, to prove ownership or copyrights of data watermark is extracted and tested. It is very difficult for counterfeiters to remove or alter watermark.

As such the real owner can always have his data safe and secure. Our aim is to study different watermarking techniques and all types of attack. Counterfeiters try to degrade the quality of watermarked image by attacking an image (generally attacks are scaling, compression and rotation of watermarked image). By attacking watermarked image, it becomes very difficult to recover watermark back from the watermarked image and even if it extracted one may no longer use it to prove the ownership and copyrights. So, our main idea is to find such regions, also known as patches, in an image which are very stable and resistant to attacks. The term watermark may have been derived from the German term, seamark. The term is actually a misnomer, in that water is not especially important in the creation of the mark. It was probably given because the marks resemble the effects of water on paper.

At the beginning of 1990 the idea of digital watermarking has emerged, it embedding imperceptible information into audio visual data. The first watermarking methods were proposed for digital images by Caronni in 1993. Digital watermarks have mainly three application fields: data monitoring, copyright protection and data authentication. The art of watermarking was invented in China over one thousand years earlier. The marks were made by adding thin wire patterns to the paper moulds. The paper would be slightly thinner where the wire was thicker and hence more transparent. The meaning and purpose of the earliest watermarks are uncertain. They may have been used for practical functions such as identifying the moulds on which sheets of papers were made, or as trademarks to identify the paper maker.

6.2.1 DISCRETE WAVELET TRANSFORM

In numerical analysis and functional analysis, a discrete wavelet transform (DWT) is any wavelet transform for which the wavelets are discretely sampled. As with other wavelet transforms, a key advantage it has over Fourier transforms is temporal resolution: it captures both frequency and location information (location in time). The discrete wavelet transform has a huge number of applications in science, engineering, mathematics and computer science. Most notably, it is used for signal coding, to represent a discrete signal in a more redundant form, often as a preconditioning for data compression. Practical applications can also be found in signal processing of accelerations for gait analysis, in digital communications and many others. It is shown that discrete wavelet transform (discrete in scale and shift, and continuous in time) is successfully implemented as analog filter bank in biomedical signal processing for design of low-power pacemakers and also in ultra-wideband (UWB) wireless communications.

6.2.2 DISCRETE COSINE TRANSFORM

DCT breaks the image into two different frequency components: low frequency and high frequency. Low frequency component contains high energy and can be considered as luminance part of image whereas reflectance is constituted by high frequency component as it contains the low energy. A discrete cosine transform (DCT) expresses a finite sequence of data points in terms of a sum of cosine functions oscillating at different frequencies. DCTs are important to numerous applications in science and engineering, from lossy compression of audio (e.g. MP3) and images (e.g. JPEG) (where small high-frequency components can be discarded), to spectral methods for the numerical solution of partial differential equations. The use of cosine rather than sine functions is critical for compression, since it turns out (as described below) that fewer cosine functions are needed to approximate a typical signal), whereas for differential equations the cosines express a particular choice of boundary conditions. In particular, a DCT is a Fourier-related transform similar to the discrete Fourier transform (DFT), but using only real numbers.

DCTs are equivalent to DFTs of roughly twice the length, operating on real data with even symmetry (since the Fourier transform of a real and even function is real and even), where in some variants the input and/or output data are shifted by half a sample. There are eight standard DCT variants, of which four are common. The most common variant of discrete cosine transform is the

type-II DCT, which is often called simply "the DCT", its inverse, the typeIII DCT, is correspondingly often called simply "the inverse DCT" or "the IDCT". The discrete cosine transform (DCT) helps separate the image into parts (or spectral sub-bands) of differing importance (with respect to the image's visual quality). The DCT is similar to the discrete Fourier transform: it transforms a signal or image from the spatial domain to the frequency domain.

6.3 BACTERIAL FORAGING OPTIMIZATION

Bacteria Foraging Optimization Algorithm (BFOA), is a new comer to the family of nature-inspired optimization algorithms. For over the last five decades, optimization algorithms like Genetic Algorithms (GAs), Evolutionary Programming (EP), Evolutionary Strategies (ES), which draw their inspiration from evolution and natural genetics, have been dominating the realm of optimization algorithms. Recently natural swarm inspired algorithms like Particle Swarm Optimization (PSO), Ant Colony Optimization (ACO) have found their way into this domain and proved their effectiveness. Application of group foraging strategy of a swarm of E. coli bacteria in multi-optimal function optimization is the key idea of the new algorithm. Bacteria search for nutrients in a manner to maximize energy obtained per unit time. Individual bacterium also communicates with others by sending signals. A bacterium takes foraging decisions after considering two previous factors. The process, in which a bacterium moves by taking small steps while searching for nutrients, is called chemotaxis and key idea of BFOA is mimicking chemotactic movement of virtual bacteria in the problem search space. Since its inception, BFOA has drawn the attention of researchers from diverse fields of knowledge especially due to its biological motivation and graceful structure. Researchers are trying to hybridize BFOA with different other algorithms in order to explore its local and global search properties separately. It has already been applied to many real-world problems and proved its effectiveness over many variants of GA and PSO. During foraging of the real bacteria, locomotion is achieved by a set of tensile flagella. Flagella help an E. coli bacterium to tumble or swim, which are two basic operations performed by a bacterium at the time of foraging. When they rotate the flagella in the clockwise direction, each flagellum pulls on the cell. That results in the moving of flagella independently and finally the bacterium tumbles with lesser number of tumbling whereas in a harmful place it tumbles frequently to find a nutrient gradient. Moving the flagella in the counter clockwise direction helps the bacterium to swim at a very fast rate. In the above-mentioned

algorithm the bacteria undergo chemotaxis, where they like to move towards a nutrient gradient and avoid noxious environment.

6.4 PROJECT IMPLEMENTATION

In our work we have developed a graphical user interface (GUI) in MATLAB which provides the freedom to select any type of image and message to be hidden in to image. To prove the efficiency of proposed work we have compared the results with DWT, DWT-DCT and DWT-DT-BFO algorithm. As discussed above parameters for comparison considered here are; PSNR and NCC. We have used multiple images to check the algorithms efficiency. The images are categorized on the basis of their threshold bins distribution as shown in table 1 below. On the basis of these images, it has been checked whether watermarking algorithm is more robust for which type of image. To make this process easier we have made a graphical user interface using
MATLAB. Results on the basis of PSNR, NCC and IF are tabulated for each type of image in table (a), (b), (c) for low key image, medium key and high key image. Bacterial foraging optimization (BFO) and PSO. The performance criteria for image watermarking are PSNR (Peak signal to noise ratio) value, NCC (normalized cross correlation) and IF (image fidelity). The value of PSNR and NCC must be high for good embedding of message. The embedding of message by any selected method comes with a constraint that the message should be recovered at the receiver end clearly and in that case, validation can be done by the NCC as normalized cross correlation between the original message and recovered message must be high. So, a gain factor in the proposed embedding process is introduced, discussed in next section, which decides the depth of message hiding and retrieval also. But it is also required that embedding should be invisible and robust also to any type of attack or noise introduced during transmission of image. High PSNR value guarantees robustness of watermarked image. So gain factor value must be selected so that a balance between the PSNR and NCC can be managed. To set the optimum value of gain factor bacterial foraging optimization is used in our work. The PBFO as discussed in previous chapter minimize the objective function value to get the best location of E. coli bacteria. So, the task is to formulate the objective function to achieve the best gain value. For this purpose, inverse of normalized cross correlation has been considered the parameter which is to be minimized. Initially random gain value is selected and that is passed to the embedding and retrieval process of message using DWT and DCT watermarking process. At the watermarked image by this process various noises like

Gaussian noise, salt & pepper noise, speckle noise and Poisson noise have been added and message is recovered from these noisy images. NCC between
the original message and recovered from these noisy watermarked images have been found out. Then the inverse of sum of all these NCCs is considered as the objective function of PBFO.

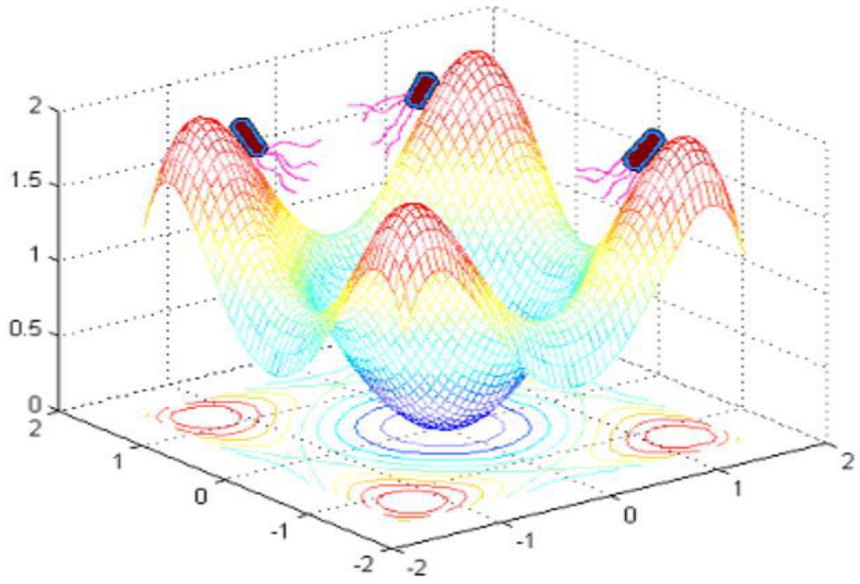


Figure6.1: A bacterial swarm on a multi-modal objective function surface.

6.5 PARTICLE SWARM OPTIMIZATION

Particle swarm optimization (PSO) is a population based stochastic optimization technique developed by Dr. Eberhart and Dr. Kennedy in 1995, inspired by social behavior of bird flocking or fish schooling. PSO shares many similarities with evolutionary computation techniques such as Genetic Algorithms (GA). The system is initialized with a population of random solutions and searches for optima by updating generations. However, unlike GA, PSO has no evolution operators such as crossover and mutation. In PSO, the potential solutions, called particles, fly through the problem space by following the current optimum particles. Compared to GA, the advantages of PSO are that PSO is easy to implement and there are few parameters to adjust.

Suppose the following scenario: a group of birds are randomly searching food in an area. There is only one piece of food in the area being searched. All the birds do not know where the food is. But

they know how far the food is in each iteration. So what's the best strategy to find the food? The effective one is to follow the bird which is nearest to the food. PSO learned from the scenario and used it to solve the optimization problems. In PSO, each single solution is a "bird" in the search space. We call it "particle". All of particles have fitness values which are evaluated by the fitness function to be optimized, and have velocities which direct the flying of the particles. The particles fly through the problem space by following the current optimum particles. PSO is initialized with a group of random particles (solutions) and then searches for optima by updating generations. In every iteration, each particle is updated by following two "best" values. The first one is the best solution (fitness) it has achieved so far. (The fitness value is also stored.) This value is called pbest. Another "best" value that is tracked by the particle swarm optimizer is the best value, obtained so far by any particle in the population. This best value is a global best and called best. When a particle takes part of the population as its topological neighbors, the best value is a local best and is called blest.

After finding the two best values, the particle updates its velocity and positions with following equation (a) and (b).

v [] = v [] + c1 * rand () * (pbest [] - present []) + c2 * rand () * (gbest [] - present []) (a) present [] = present [] + v [] (b)

v [] is the particle velocity, present [] is the current particle (solution). pbest [] and gbest [] are defined as stated before. rand () is a random number between (0,1). c1, c2 are learning factors. usually, c1 = c2 = 2. bacterial foraging optimization (BFO) and PSO. The performance criteria for image watermarking are PSNR (Peak signal to noise ratio) value, NCC (normalized cross correlation) and IF (image fidelity). The value of PSNR and NCC must be high for good embedding of message. The embedding of message by any selected method comes with a constraint that the message should be recovered at the receiver end clearly and in that case, validation can be done by the NCC as normalized cross correlation between the original message and recovered message must be high. So, a gain factor in the proposed embedding process is introduced, discussed in next section, which decides the depth of message hiding and retrieval also. But it is also required that embedding should be invisible and robust also to any type of attack or noise introduced during transmission of image. High PSNR value guarantees robustness of watermarked image. So, gain factor value must be selected so that a balance between the PSNR and NCC can be managed. To set the optimum value of gain factor bacterial foraging optimization

is used in our work. The PBFO as discussed in previous chapter minimize the objective function value to get the best location of E. coli bacteria. So, the task is to formulate the objective function to achieve the best gain value. For this purpose, inverse of normalized cross correlation has been considered the parameter which is to be minimized. Initially random gain value is selected and that is passed to the embedding and retrieval process of message using DWT and DCT watermarking process. At the watermarked image by this process various noises like Gaussian noise, salt & pepper noise, speckle noise and Poisson noise have been added and message is recovered from these noisy images. NCC between the original message and recovered from these noisy watermarked images have been found out. Then the inverse of sum of all these NCCs is considered as the objective function of PBFO.

CHAPTER-7

RESULTS & DISCUSSION

RESULTS & DISCUSSION

In our work we have developed a graphical user interface (GUI) in MATLAB which provides the freedom to select any type of image and message to be hidden in to image. To prove the efficiency of proposed work we have compared the results with DWT, DWT-DCT and DWT-DT-BFO algorithm. As discussed above parameters for comparison considered here are; PSNR and NCC. We have used multiple images to check the algorithms efficiency. The images are categorized on the basis of their threshold bins distribution as shown in table 1 below. On the basis of these images ,it has been checked whether watermarking algorithm is more robust for which type of image. To make this process easier we have made a graphical user interface using MATLAB. Results on the basis of PSNR, NCC and IF are tabulated for each type of image in table (a),(b), (c) for low key image, medium key and high key image.

7.1 RESULT:

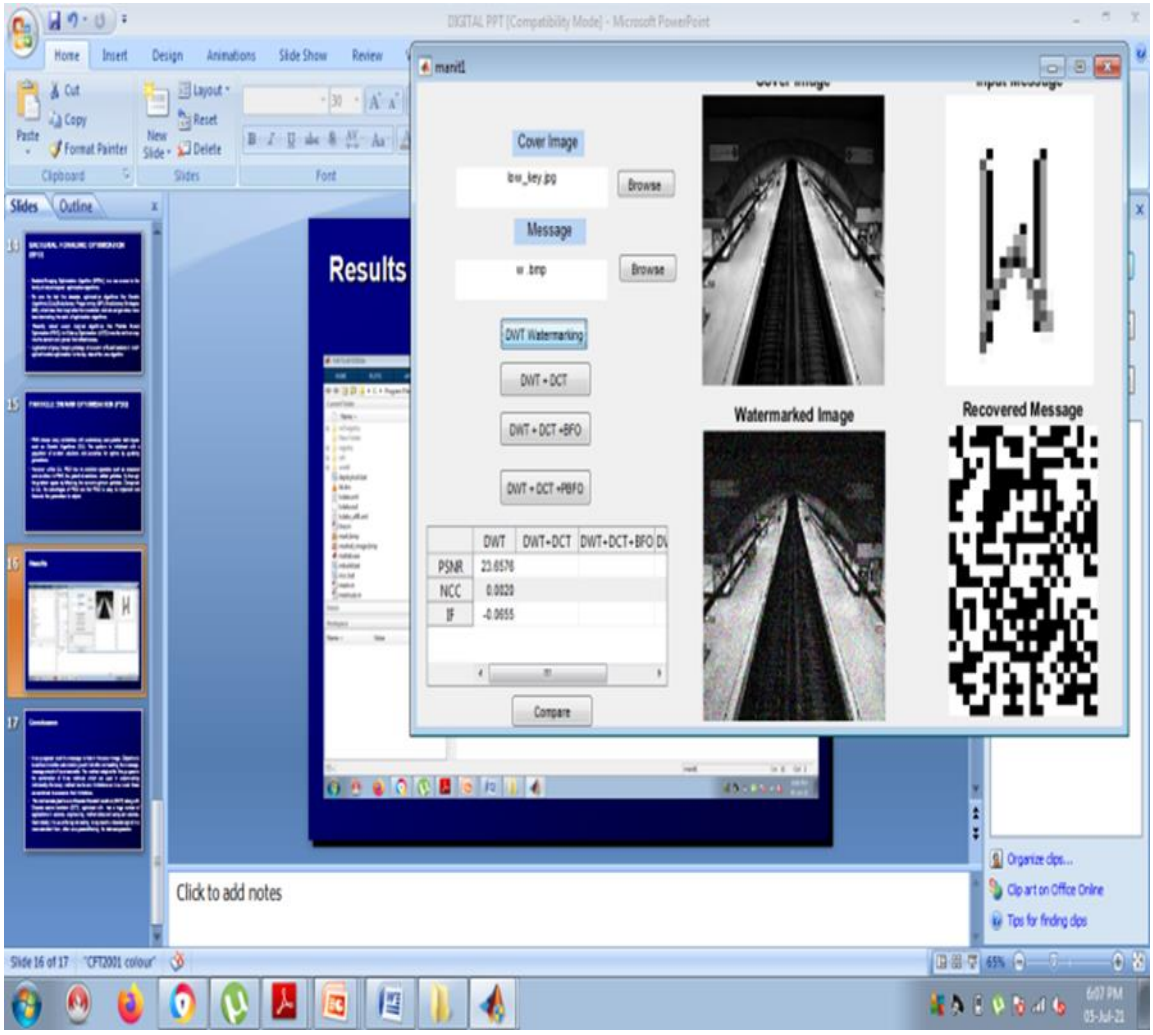


Fig7.1:Input image and Secrete Water Mark image

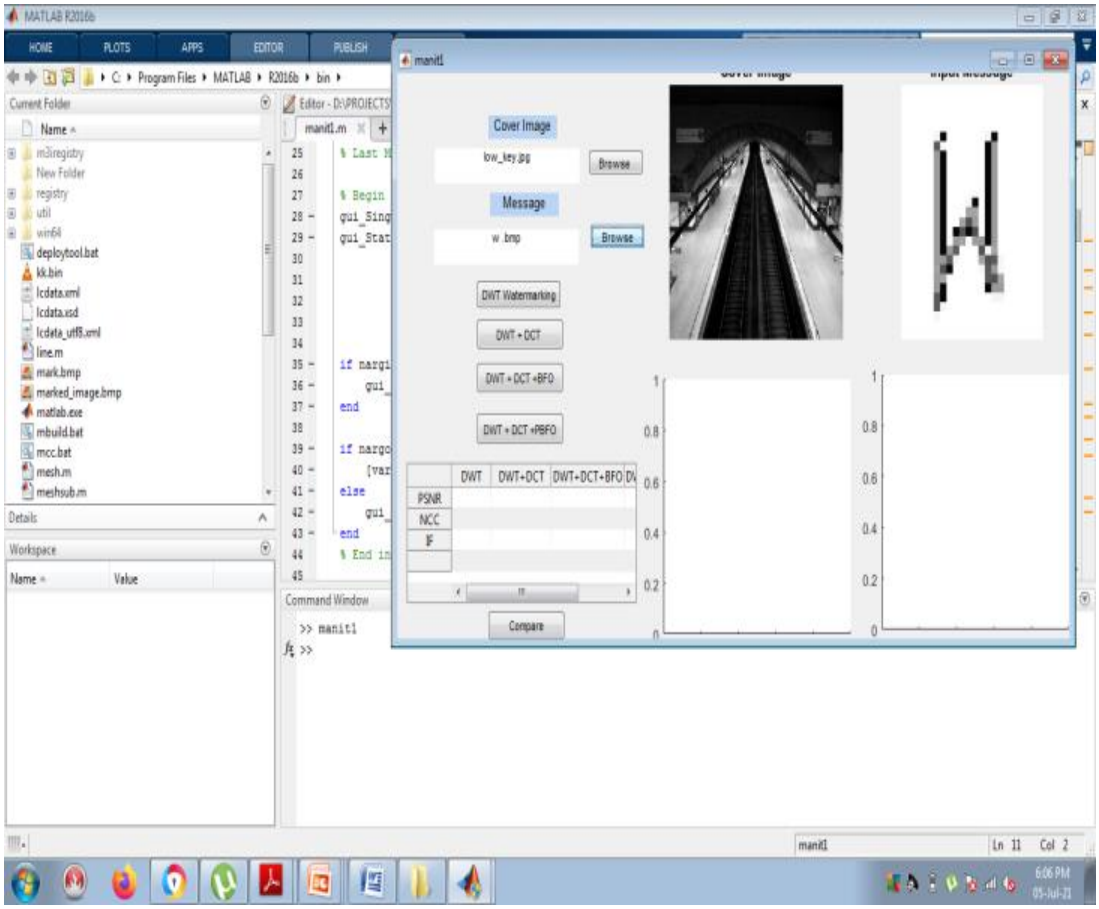


Fig7.2:Output water Marked image

7.2 ADVANTAGE

- A receiver can successfully extract the embedded secret data and recover the original content in the subsets with an order.
- The optimal transfer mechanism implemented in every subset except the last one is used to achieve a good payload-distortion performance.
- The proposed invisible watermarking system is secure as the data is stored in different segments of the images randomly. There is no static area to store data in image. In this work area will be selected dynamically by the proposed system itself.

- The proposed system is efficient as message is hidden in the image that makes it more robust as proved with increase in PSNR values.
- The proposed system is easy to understand with basic knowledge of the matrix system.
- Typically proposed technique is computationally pricey, and unpredictable. This remains one of the major problems in the development of robust digital watermarking for digital images Even if the algorithm is known it is not easy to retrieve the data.

7.3 APPLICATIONS

The increasing amount of research on watermarking over the past decade has been largely driven by its important applications in digital copyrights management and protection. One of the first applications for watermarking was broadcast monitoring. It is often crucially important that we are able to track when a specific video is being broadcast by a TV station. This is important to advertising agencies that want to ensure that their commercials are getting the air time they paid for. Watermarking can be used for this purpose. Information used to identify individual videos could be embedded in the videos themselves using watermarking, making broadcast monitoring easier. Another very important application is owner identification. Being able to identify the owner of a specific digital work of art, such as a video or image can be quite difficult. Nevertheless, it is a very important task, especially in cases related to copyright infringement. So, instead of including copyright notices with every image or song, we could use watermarking to embed the copyright in the image or the song itself. Transaction tracking is another interesting application of watermarking. In this case the watermark embedded in a digital work can be used to record one or more transactions taking place in the history of a copy of this work. For example, watermarking could be used to record the recipient of every legal copy of a movie by embedding a different watermark in each copy. If the movie is then leaked to the Internet, the movie producers could identify which recipient of the movie was the source of the leak. Finally, copy control is a very promising application for watermarking. In this application, watermarking can be used to prevent the illegal copying of songs, images of movies, by embedding a watermark in them that would

instruct a watermarking compatible DVD or CD writer to not write the song or movie because it is an illegal copy.

CODING

CODING

```
gui_Singleton = 1;
gui_State = struct('gui_Name',       mfilename, ...
                   'gui_Singleton',  gui_Singleton, ...
                   'gui_OpeningFcn', @manit1_OpeningFcn, ...
                   'gui_OutputFcn',  @manit1_OutputFcn, ...
                   'gui_LayoutFcn',  [] , ...
                   'gui_Callback',   []);
if nargin && ischar(varargin{1})
   gui_State.gui_Callback = str2func(varargin{1});
end

if nargout
   [varargout{1:nargout}] = gui_mainfcn(gui_State, varargin{:});
else
   gui_mainfcn(gui_State, varargin{:});
end

handles.output = object;
guidata(object, handles);
varargout{1} = handles.output;
S = imread([pathname,filename]);
S=imresize(S,[512,512]);
```

```
axes(handles.axes1)
imshow(S)
title('Cover Image')
set(handles.text3,'string',filename)
handles.S=S;

msg = imread([pathname,filename]);
axes(handles.axes2)
imshow(msg)
title('Input Message')
set(handles.text4,'string',filename)
handles.msg=msg;
guidata(hObject,handles)

message=handles.msg;
cover_object=handles.S;
k=10;
[watermrkd_img,PSNR,IF,NCC,recmessage]=dwt(cover_object,message,k);
axes(handles.axes3)
imshow(watermrkd_img)
title('Watermarked Image')
axes(handles.axes4)
imshow(recmessage)
```

```
title('Recovered Message')
a=[PSNR,NCC,IF]';
t=handles.uitable1;
set(t,'Data',a)
handles. A=a;
guidata(hObject,handles)


a=handles. A;
message=handles.msg;
cover_object=handles.S;
k=10;
[watermrkd_img,recmessage,PSNR,IF,NCC1] =
detect(cover_object,message,k);
axes(handles.axes3)
imshow(watermrkd_img)
title('DWT+DCT Watermarked Image')
axes(handles.axes4)
imshow(recmessage)
title('DWT+DCT Recovered Message')
b=[PSNR,NCC1,IF]';
t=handles.uitable1;
set(t,'Data',[a b])
handles.b=b;
```

```
guidata(hObject,handles)


a=handles.a;

b=handles.b;

message=handles.msg;

cover_object=handles.S;

[watermrkd_img,recmessage,PSNR,IF,NCC,pbest] =
BG(cover_object,message);

axes(handles.axes3)

imshow(watermrkd_img)

title('DWT+DCT+BFO Watermarked Image')

axes(handles.axes4)

imshow(recmessage)

title('DWT+DCT+BFO Recovered Message')

c=[PSNR,NCC,IF]';

t=handles.uitable1;

set(t,'Data',[a b c])

handles.c=c;

guidata(hObject,handles)


a=handles.a;

b=handles.b;

c=handles.c;
```

```
d=handles.d;
PSNR=[a(1),b(1),c(1),d(1) ];
NCC=[a(2),b(2),c(2),d(2)];
IF=[a(3),b(3),c(3),d(3)];
figure
bar(PSNR)
set(gca, ‘XTickLabel',' ');
ylabel('PSNR')
text(1,0,'DWT','Rotation',260,'Fontsize',8);
text(2,0,'DWT+DCT','Rotation',260,'Fontsize',8);
text(3,0,'DWT+DCT+BFO','Rotation',260,'Fontsize',8);
text(4,0,'DWT+DCT+PBFO','Rotation',260,'Fontsize',8);
[t]=get(gca, ‘position');
set(gca, ‘position',[t(1) 0.31 t(3) 0.65])
title('Bar Graph Comparison of PSNR')

figure
bar(NCC)
set(gca, ‘XTickLabel',' ');
ylabel('NCC')
text(1,0,'DWT','Rotation',260,'Fontsize',8);
text(2,0,'DWT+DCT','Rotation',260,'Fontsize',8);
text(3,0,'DWT+DCT+BFO','Rotation',260,'Fontsize',8);
```

```
text(4,0,'DWT+DCT+PBFO','Rotation',260,'Fontsize',8);

[t]=get(gca, ‘position');

set(gca, ‘position',[t(1) 0.31 t(3) 0.65])

title('Bar Graph Comparison of NCC')


a=handles.a;

b=handles.b;

c=handles.c;

message=handles.msg;

cover_object=handles.S;

[watermrkd_img,recmessage,PSNR,IF,NCC,pbest]
=BG_PSO(cover_object,message);

axes(handles.axes3)

imshow(watermrkd_img)

title('DWT+DCT+PBFO Watermarked Image')

axes(handles.axes4)

imshow(recmessage)

title('DWT+DCT+PBFO Recovered Message')

d=[PSNR,NCC,IF]';

t=handles.uitable1;

set(t,'Data',[a b c d])

handles.d=d;

guidata(hObject,handles)
```

CONCLUSION AND FUTURE SCOPE

CONCLUSION AND FUTURE SCOPE

.

➢ CONCLUSION

The effectiveness of the whole scheme is proven through simulation results like 1) PSNR quality assessment objectives are achieved 2) watermarked image have very good visual quality 3) no auxiliary data is required for quality estimation (only embedded watermarks and test images are needed). In this work, a still image watermarking scheme with high robustness in the frequency domain is applied. The proposed scheme tests only image rather than audio or video. This algorithm can be used for data hiding in many applications such as authentication and copyright protection. In this dissertation, a general coding-type framework which provides useful and constructive tools in the analysis and design of watermarking system is used. That particularly demonstrates the effectiveness of watermarking approach in achieving design objectives such as robustness, capacity, security, and implementation efficiency.

➢ FUTURE SCOPE

- From this project the secrete image can be watermarked into an original image.
- Finally to project the original image, that means to preserve the image quality as the original image.
- In future it will use in company way because the important documents ,file watermark in a path.

REFERENCES

REFERENCES

[1]. Abdelaziz I. Hammouri, Bassem Alrifai and Heba Al-Hairy," An Intelligent Watermarking Approach Based Particle Swarm Optimization in Discrete Wavelet Domain" IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 2, No 1, March 2013

[2]. Ray-Shine Run, Shi-Jinn Horn, Jiu-Lin Lai, Tzeng-Wang Kao, Rong-Jian Chen," An improved SVD-based watermarking technique for copyright protection" Expert Systems with Applications 39 (2012)

[3]. Sunil Sood, Ajay Goyal," Watermarking Relational Databases using Genetic Algorithm & Bacterial Foraging Algorithm" International Journal of Information & Computation Technology, Volume 4, Number 17 (2014)

[4]. Hsiang-Che Huang, Yueh-Hong Chen, Ajith Abraham," Optimized Watermarking Using Swarm-Based Bacterial Foraging" Journal of Information Hiding and Multimedia Signal Processing, Volume 1, Number 1, January 2010.

[5]. Sunil Sood," Digital Watermarking Using Hybridization of Optimization Techniques: A Review" International Journal of Computer Science and Information Technologies, Vol. 5 (4) , 2014.

[6]. P. Surekha and S. Sumathi," Implementation of Genetic Algorithm For A Dwt Based Image Watermarking Scheme" Intact Journal On Soft Computing: Special Issue On Fuzzy In Industrial And Process Automation, July 2011, Volume: 02, Issue: 01.

[7]. Hucheng Wei, Hao Li, Lufeng Dai, Sashing Wang," Image Watermarking Based on Genetic Algorithm" IEEE 2006

[8]. Mahmoud El Najjar, A.A Zaiden, B.B Zaiden, Mohamed Elhaida Musharraf and amdan.O.Alanazi," Optimization Digital Image Watermarking Technique for Patent Protection" Journal Of Computing, Volume 2, Issue 2, February 2010.

[9]. Khaled Luharuka," Optimal Image Watermarking Algorithm Based on LWT-SVD via Multi-objective Ant Colony Optimization" Journal of Information Hiding and Multimedia Signal Processing, Volume 2, Number 4, October 2011.

[10]. Mona M. Soliman, Abou Ella Sassanian, Neven I. Ghalib and Hooda M. Onis," An adaptive Watermarking Approach for Medical Imaging Using Swarm Intelligent" International Journal of Smart Home Vol. 6, No. 1, January, 2012.

[11]. V. Aslant as," Optimal SVD based Robust Watermarking using Differential Evolution Algorithm" Proceedings of the World Congress on Engineering 2008 Vol I.

[12]. Verminy, Rakesh," An Optimization Technique for Image Watermarking Scheme" International Journal of Computer Trends and Technology (IJCTT) – volume 5 number 3 –Nov 2013.

[13]. Krait Vyas, B.L. Pal," Proposed Method In Image Steganography To Improve Image Quality With Lbs. Technique" International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 1, January 2014.

[14]. Parisa Gurami, Subarian Ibrahim, Murtaza Bashardost," Least Significant Bit Image Steganography using Particle Swarm Optimization and Optical Pixel Adjustment" International Journal of Computer Applications (0975 – 8887) Volume 55– No.2, October 2012.

[15]. Navdeep Kaur," Steganography Using Particle Swarm Optimization-A Review" International Journal Of Engineering Sciences & Research Technology, November, 2013.

[16]. Aisha Fernandes, Wilson Ebberson," A Simple Steganographic Technique with a Good Embedding Capacity" International Journal of Darshan Institute on Engineering Research and Emerging Technology Vol. 2, No. 2, 2013, pp. 56-61