

**DEVELOPMENT OF ENHANCED ALGORITHM FOR
INFORMATION SECURITY THROUGH
WATERMARKING**

Project Report submitted in partial fulfillment of the requirement
for the degree of Bachelor of Technology.

in

Computer Science Engineering and Information Technology

under the Supervision of

Dr. Hemraj Saini

By

Shivam Aggarwal (091404)

Arjun Sapra (091419)

Ravi Asthana (091426)

Rajat Bajaj (091459)

to



Jaypee University of Information and Technology
Waknaghat, Solan – 173234, Himachal Pradesh

Certificate

This is to certify that work titled “**DEVELOPMENT OF ENHANCED ALGORITHM FOR INFORMATION SECURITY THROUGH WATERMARKING**” submitted by “*Shivam Aggarwal (091404), Arjun Sapra(091419), Ravi Asthana (091426) and Rajat Bajaj (091459)*” in partial fulfillment for the award of degree of Bachelor of Technology in Information Technology of Jaypee University of Information Technology, Wagnaghat has been carried out under my supervision.

This work has not been submitted partially or wholly to any other university or institute for the award of this or any other degree or diploma.

Dr. Hemraj Saini

Assistant Professor,

Department of Computer Science Engineering and Information Technology,

Jaypee University of Information Technology,

Wagnaghat.

Acknowledgement

We express our heartfelt gratitude to all those who have contributed directly or indirectly towards obtaining our baccalaureate degree and at the same time, we cherish the years spent in the department of Computer Science Engineering and Information Technology. We are highly indebted to our esteemed supervisor, Dr.Hemraj Saini, who has guided us through thick and thin. This project would not have been possible without his guidance and active support. His positive attitude towards research and zest for high quality research work has prompted us for its timely completion. We deem it a privilege to be working under Dr. Hemraj Saini who has endeared himself to his students and scholars.

The help rendered by all our teachers, in one way or the other, is thankfully acknowledged. We would also like to thank members of the lab and colleagues from other labs for their constant support. It was a pleasure to work with them.

Shivam Aggarwal (091404)

Arjun Sapra (091419)

Ravi Asthana (091426)

Rajat Bajaj (091459)

Dated:

Table of Contents

1. Chapter 1	1-2
1.1 Abstract.....	1
1.2 Problem	
Statement.....	1
1.3 Motivation.....	2
2. Chapter 2	3-55
2.1 Literature	
survey.....	3
2.2 General framework for	
watermarking.....	11
2.2.1 Watermark	
Characteristics.....	12
2.2.2 Watermark	
Application.....	13
2.2.3 Types of Digital	
Watermarking.....	13
2.2.4 Spatial	
Domain.....	15
2.2.4.1 Least Significant Bit Hidding (Image	
Hidding).....	15
2.2.5 Frequency	
Domain.....	18
2.2.6 Proposed Watermarking	
Algorithm.....	18
2.2.6.1 Discrete Wavelet	
Transform.....	19
2.2.6.2 Watermark Embedding	
Technique.....	19
2.2.6.3 Watermark Extraction	
Technique.....	20
2.3 LSB(least significant bit).....	23
2.3.1 Embedding.....	23

2.3.2	Recovery.....	24
2.4	DWT(DiscreteWaveletTransform)Technique.....	26
2.4.1	Embedding.....	26
2.4.2	Recovery.....	29
2.5	COMPARISONb/w LSB andDWT.....	30
2.6	AdvantagesofDWT.....	31
2.7	Single value decomposition.....	42
2.7.1	Dct Domain Watermarking.....	43
2.7.2	Dwt Domain Watermarking.....	43
2.7.3	Characteristics of DWT.....	44
2.8	Dct-Svd Based Watermarking.....	44
2.9	Dwt-Svd Based Watermarking.....	45
2.10	Dwt-Dct-Svd Based Watermarking.....	45
2.11	SVD.....	46
2.11.1	Digital Image Processing.....	46
2.11.2	Theory of Singular Value Decomposition.....	47
2.11.2.1	Process of singular value decomposition.....	47
2.11.3	Example.....	49
2.11.4	Properties of the SVD.....	51
2.11.5	Methodology of svd applied to image processing.....	52
2.11.5.1	SVD Approach for Image Compression.....	52
2.11.6	Proposed Algorithm using dwt and svd techniques.....	54
2.11.6.1	Embedding Watermark.....	54
2.11.6.2	Watermark Extraction.....	55
2.12	Dwt-Svd Hybrid Code.....	56
3.	Chapter 3.....	63-66
3.1	Hardware and software requirement.....	63
3.2	System Requirements.....	64

3.3 Software	
requirement.....	64
3.4 Hardware	
Requirement.....	65
3.5 Other Requirement	
.....	65
4. Chapter 4.....	67-70
4.1 Architectural	
Design.....	67
4.1.1 Data Flow	
Diagram.....	67
4.1.1.1 Data Flow Diagram Level	
1.....	68
4.1.1.2 Data Flow Diagram Level	
2.....	69
4.1.2 Activity	
diagram.....	70
5. Chapter 5.....	71-74
5.1 Conclusion.....	71
5.2 References.....	72

LIST OF FIGURES

TITLE	PAGE NO
FIGURE 2.1:	
A: Original Image	3
B: RONI Watermarked Image	3
C: RONI and ROI Watermarked Image	3
FIGURE 2.2: Watermark distribution for whole image	4
FIGURE 2.3: Watermarked image	6
FIGURE 2.4: Degradation in visual quality with embedded information	7
FIGURE 2.5:	
A: host image	8
B: watermarked image	8
C: RONI image	8
D: ROI image	8
FIGURE 2.6: ROI as a binary image which is used as a watermark	8
FIGURE 2.7: Block diagram to embed and extract watermark	10
FIGURE 2.8: Areas used for embedding watermark	11
FIGURE 2.9: Watermark embedding steps	11
FIGURE 2.10: Block diagram of digital watermarking	13
FIGURE 2.11: Watermarking Flowchart	16
FIGURE 2.12: Sample Image Matrix	17
FIGURE 2.13: Steganography Techniques Computer Security	20
FIGURE 2.14: Watermarking Embedding Technique	25
FIGURE 2.15: Watermarking Extraction Technique	26
FIGURE 2.16: Original Image	27
FIGURE 2.17: Image to be Embedded	27
FIGURE 2.18: Embedding of Image Using LSB	29

FIGURE 2.19:Image Recovery Using LSB Algorithm	31
FIGURE 2.20:Embedding Using DWT Algorithm	34
FIGURE 2.21:Image Recovery Using DWT Algorithm	36
FIGURE 2.22: Cover Image and Payload Image	37
FIGURE 2.23:LSB Embedding	38
FIGURE 2.24:LSB Recovery	38
FIGURE 2.25: DWT Embedding	39
FIGURE 2.26: DWT Recovery	39
FIGURE 2.27 Cover and Payload Image	40
FIGURE 2.28LSB Embedding	40
FIGURE 2.29 LSBRecovery	41
FIGURE 2.30: DWT Embedding	41
FIGURE 2.31: DWT Recovery	42
FIGURE 2.32: SVD(Original Image)	60
FIGURE 2.33 : SVD(Watermark Image)	60
FIGURE 2.34 :SVD(Watermarked Image)	61
FIGURE 2.35:SVD(Gaussian Noise)	61
FIGURE 2.36 :SVD(Poisson Noise)	62
FIGURE 2.37: SVD(Recovery Image)	62
FIGURE 4.1 :Data Flow Diagrams	67
FIGURE 4.2 : Data Flow Diagram Level 1	68
FIGURE 4.3 : Data Flow Diagram 2	69
FIGURE 4.4 : Activity Diagram	70

CHAPTER 1

1.1 ABSTRACT

Digital watermarking is a technique for inserting information (watermark) into an image, which can be later extracted or detected for variety of purposes including identification and authentication purpose. With this technique, we can recognize the source, owner, distributor or creator of a document or an image. Digital watermarks are potentially useful in many applications including : ownership assertion, fingerprinting, copy prevention or control. Digital cinema can be considered as a practical application, where information can be embedded as a watermark in every frame. Now, there are few important issues that arise in the study of digital watermarking techniques and they are : capacity, robustness, transparency and security. Until now, there are only few of the techniques through which watermarking can be done. The easiest way to watermark an image/video, is to change directly the values of the pixels, in the spatial domain. But there is a drawback of this technique that the inserted information may be easily detected using computer analysis. A more advanced way to do it, is to insert the watermark in the frequency domain, using one of the well known transforms : Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) . Other techniques are possible as well, like using Fractals.

1.2 PROBLEM STATEMENT

As presented, LSB Embedding has the advantage that it is simple to implement. It also allows for a relatively high payload, carrying one bit of the secret message per byte of pixel data. In addition, it is also seemingly undetectable by the average human if done right.

In addition to being vulnerable to detection techniques, LSB is extremely vulnerable to corruption. That is, the integrity of the hidden message can easily be destroyed. All the

attacker must do is to randomize the LSBs of the image. The attacker may not even know that it is a stego-image, but such actions would destroy the secret message. Due to these possible attacks, LSB Embedding is relatively insecure, at least in its primitive form. However, due to its advantages, it is useful for applications where security is desired, but not necessary. It is also a good foundation to build more secure steganographic techniques. Therefore we are trying to implement a hybrid of SVD and DWT to overcome these drawbacks.

1.3 MOTIVATION

This project aims at integrating digital security, securing the transmission of images taking place which gives individuals the freedom to embrace the digital lifestyle – to confidently engage in everyday interactions across all digital devices. Image security affects all aspects of the digital lifestyle, which, among others, comprises computers and the internet, telecommunications, financial transactions, transportation, healthcare, and secure access. The FBI, CIA, and Pentagon, are all leaders in utilizing secure controlled access technology for any of their image transmissions. However, the use of this form of technology is spreading into the entrepreneurial world. More and more companies are taking advantage of the development of digitally secure controlled access technology.

The Internet is a great way to send your photographs to anyone around the world. Sending images through web is child's play compared to hanging a gallery show or publishing a book. But what is to stop an unscrupulous web hacker from stealing your confidential images?

Therefore implementing a hybrid of lsb and dwt gives a very secure method for transmission of images securely.

CHAPTER 2

2.1 LITERATURE SURVEY

JASNI M ZAIN 2006

The purpose of this paper was to see whether digitally watermarked images changed clinical diagnoses when assessed by radiologists. We embedded 256 bits watermark to various medical images in the region of non-interest (RONI) and 480K bits in both region of interest (ROI) and RONI. Our results showed that watermarking medical images did not alter clinical diagnoses. In addition, there was no difference in image quality when visually assessed by the medical radiologists. We therefore concluded that digital watermarking medical images were safe in terms of preserving image quality for clinical purposes.



Fig. 2.1

(a)Original Image (b)RONI Watermarked Image (c)RONI and ROI Watermarked Image

It was also evident that the area where watermarking was embedded was immaterial as both sites;ROI and RONI gave similar results when they were clinically assessed.

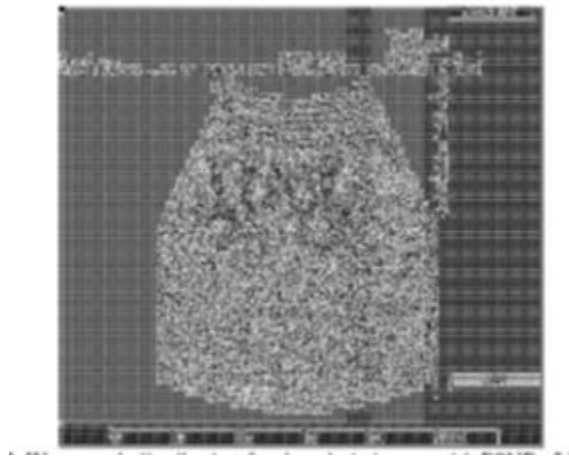


Fig. 2.2

Watermark distribution for whole image with PSNR=54.15 db

The three assessors evaluated 225 images. Each received 25 nWM and 50 WM (ROI and RONI) images.

K. A NAVAS 2007

Most of the works are on the tamper detection of the images and embedding of the Electronics Patient Record (EPR) data in the medical images. Watermarked medical images can be used for transmission, storage or tele-diagnosis. Tamper detection

watermarks are useful to locate the regions in the image where some manipulations have been made. EPR data hiding in images improves the confidentiality of the patient data, saves memory storage space and reduce the bandwidth requirement for transmission of images. There are so many medical image watermarking (MIW) applications like- Integration and storage of medical data with images, Tele-diagnosis through www and e-mail, Web based teleconferencing etc.

There are so many advantages of MIW like-Memory saving, Bandwidth saving, Avoiding detachment, Confidentiality, Security, Non-repudiation. The works on watermarking medical images are classified into two.

1. tamper detection and authentication
2. EPR data hiding.

Based on these, there are so many algorithms like-

- **HYUNG ET AL ALGORITHM:-** To avoid illegal forgery, ROI information is embedded in the no-ROI region. This technique is implemented in wavelet transform for high robustness.
- **HIRAL ET AL ALGORITHM:-** This method provides exact authentication to medical image through reversible or erasable watermark. The merits of this method are very good perceptual transparency for watermarked image, recovery of the original cover image, and high value of PSNR.
- **EPR DATA HIDING ALGORITHMS:-** The priority order of requirements of EPR data hiding is imperceptibility, capacity and robustness.
- **ACHARYA ET AL ALGORITHM:-** LSB technique of data hiding in frequency domain is proposed in. The image is transformed to frequency domain using DCT. The coefficients are run length encoded.

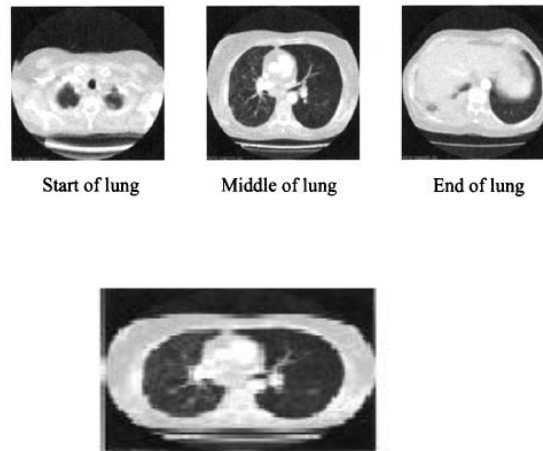
NISAR AHMED MANON 2008

Author suggest that ROI is the region that contains the important information from diagnosis point of view so it must be stored without any distortion. We have proposed a digital watermarking technique which avoids the distortion of image in ROI by embedding the watermark information in NROI. The higher the PSNR, the better the quality of watermarked image. The PSNR is given by:

$$PSNR= 10 \log_{10} \frac{R^2}{MSE}$$
$$MSE = \frac{\sum_{M,N} [(I_1(m,n) - I_2(m,n))]^2}{M \times N}$$

Source:-<http://www.mathworks.in/help/vision/ref/psnr.html>

Where MSE is mean square error and R is is the maximum fluctuation in the input image data. PSNR decreases with increase in the strength of watermark.



source:nisar ahmed manon, “Fast and robust watermarking of JPEG files,” Proc. IEEE 5th Southwest Symp. Image Analysis and Interpretation, 2008, pp. 158-162.

Fig. 2.3:Watermarked image(PSNR=55.60 db)

Where M and N are number of rows and number of columns in both the cover and watermarked image. The degradation in terms of PSNR and MSE in the cover image.

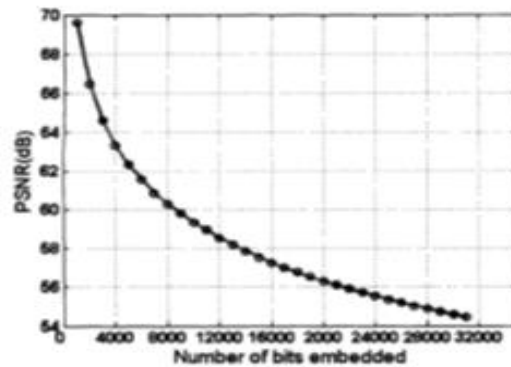


Fig. 2.4

Degradation in visual quality with embedded information

While embedding the data region of interest (ROI) of medical image has been avoided to ensure the integrity of ROI. The scheme allows the simultaneous storage and transmission of electronic patient record which can be extracted at the receiving end without the original image.

EHAB F. BADRAN 2009

It has the potential of being a value-added tool for medical confidentiality protection, patient-related information hiding, and information retrieval. Medical image watermarking requires extreme care when embedding additional data within the medical images because the additional information must not affect the image quality as this may cause misdiagnosis. In this paper we present a scheme that depends on the extraction of the ROI (region of interest) and its use as a watermark to be embedded twice; first as a robust watermark in the RONI (region of non interest) in the wavelet domain and again as a fragile watermark in the ROI in the spatial domain.

Author's algorithm is divided into 3 steps which are; watermark generation, watermark embedding and finally watermark extraction. The watermark generation step is as follows; first the ROI which is in our case the brain tumor after its extraction from the image is decomposed into three wavelet decomposition levels.

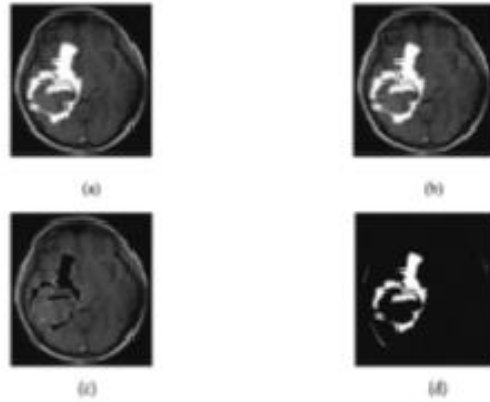


Fig. 2.5

(a)host image (b)watermarked image (c)RONI image (d)ROI image

Source:ehab f. badran, “Digital watermarking extension to JPEG coded domain,” Proc. IEEE Int. Conf. Information Technology: Coding and Computing, 2009, pp. 133-138



Fig. 2.6

ROI as a binary image which is used as a watermark

$$PSNR = 10 * \log_{10} \frac{255^2}{MSE}$$

$$MSE = \frac{1}{MN} \sum_{m=1}^M \sum_{n=1}^N e(m, n)$$

The PSNR of the watermarked image is calculated for different Q (jpeg compression attack) and written below tables 2.1.




JPEG Compressed watermarked Image(Q-factor)	PSNR (dB)	NHD Tumor Hidden
10	22.3750	0.0420 
20	24.7278	0.0391 
50	28.8586	0.0352 

Table 2.1

NHD and PSNR under JPEG compression attack($\alpha=1$)(new scheme)
 PSNR=31.5236 db

Medical image protection and authentication are becoming increasingly important in an e-Health environment.

SHIKHA TRIPATHI 2010

In this paper we propose a DWT based dual watermarking technique wherein both blind and non-blind algorithms are used for the copyright protection of the cover/host image and the watermark respectively. We use the concept of embedding two watermarks into the cover image by actually embedding only one, to authenticate the source image and protect the watermark simultaneously. A new approach for embedding is proposed, wherein, the watermark pixels are chosen pseudo-randomly, besides pseudo-randomly selecting the locations for embedding the watermark in the mid-frequency region of the source image. This increases the security two-fold. To further increase the security a pseudo random number generator (PRNG) is used at various instances in the algorithm. This reduces the chances of watermark extraction by prediction.

- **NON BLIND EMBEDDING ALGORITHM:-** Firstly the original logo is divided into various sub-blocks and pxq sub-blocks are chosen pseudo-randomly for embedding each bit of the sign. Each sub-block is decomposed into single level of DWT.

- BLIND EMBEDDING ALGORITHM:**-This algorithm makes use of the concept of thresholding. The watermark is a $m \times n$ image and the cover image is of size $k \times k$. The proposed algorithm uses the standard deviation of the sub-blocks to determine the threshold levels.

WATERMARK EXTRACTION:-we discuss the extraction procedure of the signed logo. The original logo and the extracted logo are divided into sub blocks and transformation is taken as explained in the embedding procedure.

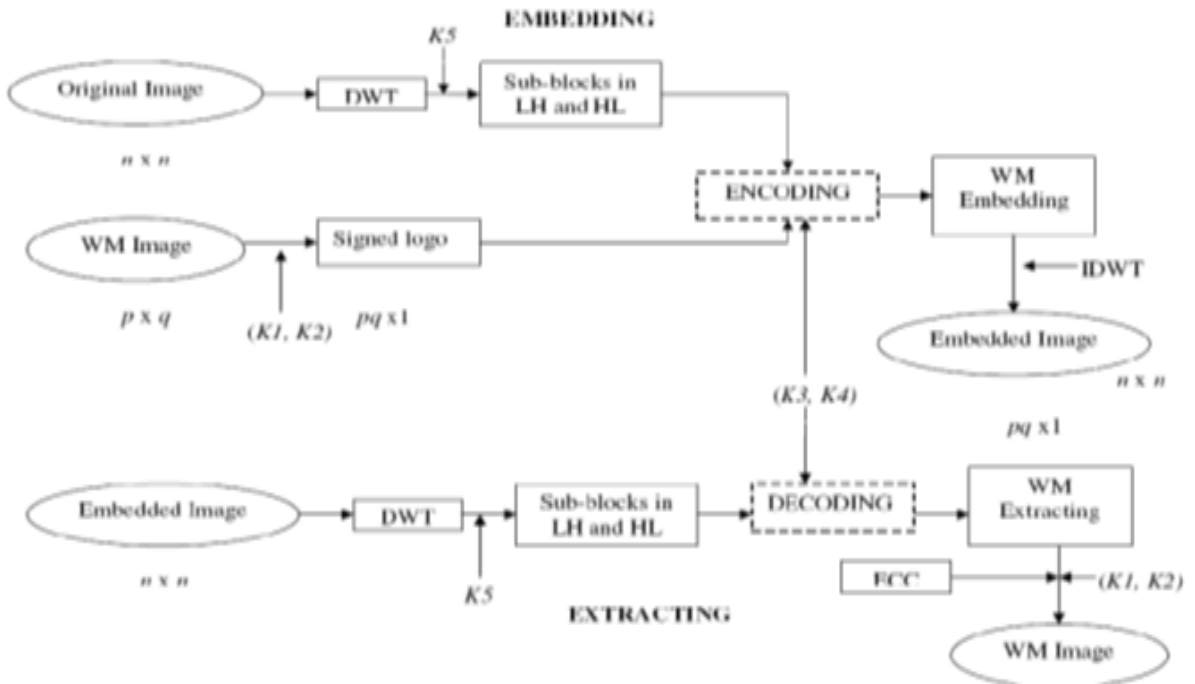


Fig. 2.7

Block diagram to embed and extract watermark

source: shikhatipathi "A novel watermark embedding and detection scheme for images,"
 iee trans. circuits syst. video technol., 2010, vol. 13, pp. 813-830.

A LAVANYA 2011

Digital watermarking is proposed as a method to enhance medical data security. Medical image watermarking requires extreme care when embedding additional information within medical images, because the additional information should not degrade medical image quality. In our scheme a well-known technique least significant bit substitution (LSB) is adapted to fulfill the requirements of datahiding and authentication in medical images. The DWT (Discrete Wavelet Transform) of ROI-MSB (most significant bit) embedded into the LSB middle of the image. The scheme divide Digital Imaging and Communications in Medicine (DICOM) image into two parts ROI and non-ROI (non-region of interest).

Enhancing security of DICOM images in distributed environment

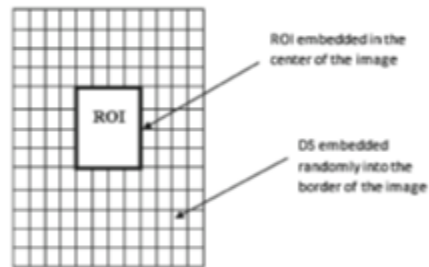


Fig. 2.8

Areas used for embedding watermark

Followings are the embedding procedures which contains steps:- Image preprocessing, Digital signature, DWT, Embedding.

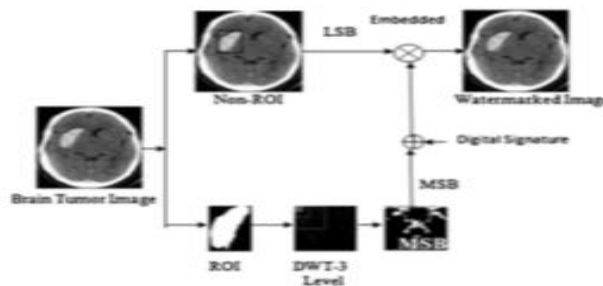


Fig. 2.9

Watermark embedding steps

source: a lavanya, "watermarking embedding techniques," proc. fourth international symposium on watermarking, 2011, pp. 182-187.

Extraction:- The original image stored in database server is required to extract the watermark. If the watermark in the attacked image is failed to extract, the image is re-transmitted to the user. This procedure is reversed as the embedding procedure and it uses the subtraction of watermarked image and the original image.

KOUSHIK PAL 2012

A novel scheme for biomedical image watermarking by hiding multiple copies of the same data in the cover image using bit replacement in horizontal (HL) and vertical (LH) resolution approximation image components of wavelet domain. The proposed scheme use an approach for recovering the hidden information from the damaged copies due to unauthorized alteration of data under attack by applying an algorithm to find the closest twin of the embedded information by bit majority algorithm. Data hiding, Integrity control, Authenticity, Imperceptible/Reversible Watermarking are Four main objectives in the medical. The embedding and recovery of information logo is analyzed in detail. To measure the amount of visual quality degradation between original and watermarked images different types of image quality metrics are used. In present work we have used peak signal-to-noise ratio (PSNR) and structural similarity index measure (SSIM).

Peak signal-to-noise ratio is ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. PSNR is usually expressed in terms of dB for wide range signals.

- **STRUCTURAL SIMILARITY INDEX MEASURE:-** It is a method for measuring the similarity between two images. The SSIM index is a full reference metric, in other words, the measuring of image quality based on an initial distortion-free image as reference. SSIM is designed to improve on traditional methods like PSNR and MSE, which have proved to be inconsistent with human eye perception. The resultant SSIM index is a decimal value between -1 and 1, and value 1 is only reachable in the case of two identical sets of data.

Access to or sharing of an isolated medical document requires that the document can be identified. It can be easily understandable that, as a compliment to all other modern security tools, watermarking can raise up the security level by detecting unauthorized manipulations and malicious actions.

2.2 GENERAL FRAMEWORK FOR WATERMARKING

The general functioning of a typical watermark can be easily understood by means of the Fig. Presented below The original content (image, audio or video) is mixed with the modified version of the watermark to produce a suitable watermarked digital content at the sender's end. At the receiving end, a normal human being perceives the image and is unable to appreciate the presence of watermark. However, a watermark detector at the receiving end extracts the coded watermark from the content and decodes it to obtain the original watermark.

In the given Fig. following notations have been followed. W : Watermark, SO' : perceived information at the receiving end, SW : Watermarked image,

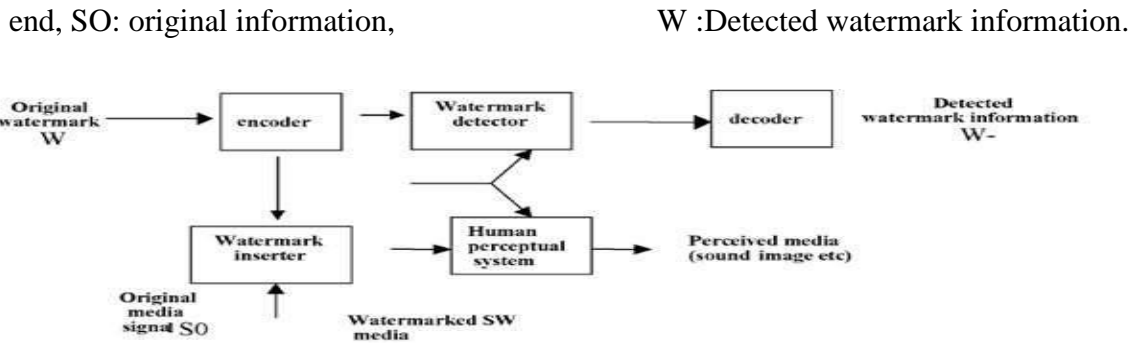


Fig. 2.10

Block diagram of digital watermarking

Source: G. C. Langelaar and R. Lagendijk, "Digital image watermarking of images,"
IEEE Trans. Image Processing, 2001, vol. 10, pp. 148-158.

Thus the first step is to encode watermark bit sin to a form that will easily combine with the media data. For example in digital images, watermarks may between dimension spatial patterns. This encoded information is then mixed with the original media content by means of watermark inserter. After insertion of the watermark also the resultant media looks similar to the original on eusing the peculiarities of the human visual system.

Some techniques use the principle that in eight bit gray images, changes to the least significant bit can not be perceived by the human eye Turner. The human visual system looks at only the others even bits thus ignoring the watermark in for mati on so the fidelity of the image is maintained. Other techniques convert the digital image into corresponding frequency domain and mix the watermark information in the high frequency part of the image. Human eye can perceive only low frequency components significantly thus ignoring the higher frequency components which are used by the watermark.

This is similar to the principle used in lossy compression as proposed by R.Schyndel. Methods using as ingle key are being employed but with different level of access and are termed 'restricted key' and 'unrestricted key' methods. No method using two different keys at send er and receiver is yet known in the area of watermarking.

2.2.1 WATERMARKING CHARACTERISTICS

1. Fragility
2. Tamper resistance
3. Key restrictions
4. Fidelity
5. Robustness

6. False positive rate
7. Data payload

2.2.2 WATERMARK APPLICATIONS

1. Copy control
2. Digital signatures
3. Fingerprinting
4. Authentication
5. Broadcast monitoring
6. Secret communication

2.2.3 TYPES OF DIGITAL WATERMARK

Watermarks and watermarking techniques can be divided into various categories in various ways. The watermarks can be applied in **spatial domain**. An alternative to spatial domain watermarking is **frequency domain** watermarking. It has been pointed out that the frequency domain method is more robust than the spatial domain techniques. Different types of watermark are shown in the figure below.

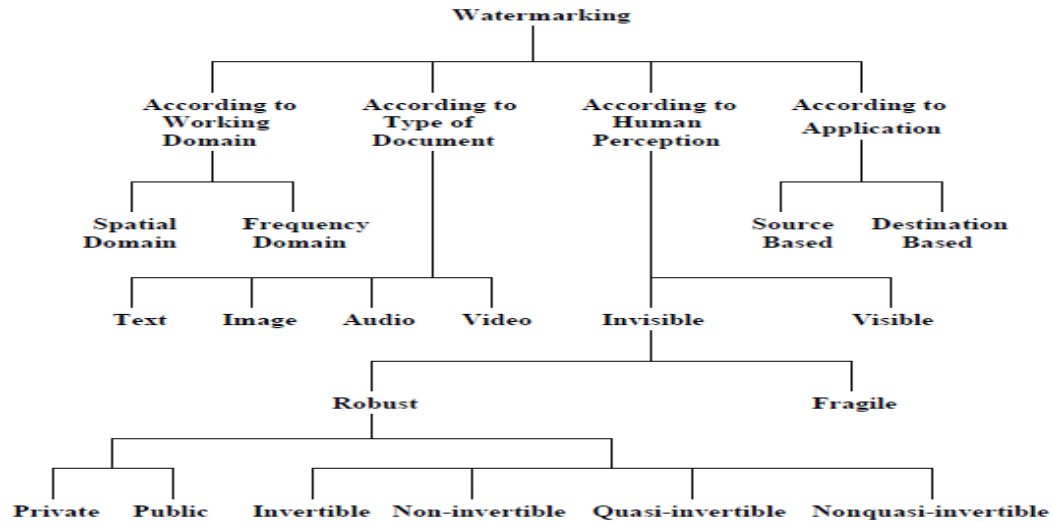


Fig. 2.11

Watermarking Flowchart

Source:http://www.ee.uta.edu/Dip/Courses/EE5359/Abrar%20Ahmed%20Syed_Digital%20Watermarking.pdf

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

1. Image Watermarking
2. Video Watermarking
3. Audio Watermarking

IMAGEWATERMARKING

The basic idea is to embed the information with in an image. An image is an array, or a matrix, of square pixels (picture elements) arranged in columns and rows.

Or we can say an image is a 2-D signal:

1. Spatial signal
2. Intensity value as $I(X,Y)$

Digital image is digitized 2-D signal:

1. Use rectangular shape as called pixels
2. Digital representation: 8 bit, 16 bit, 24 bit....

While image processing digital image are represented using matrices

Example

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \dots & a_{3n} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & a_{m3} & \dots & a_{mn} \end{bmatrix} \quad \leftarrow \text{second row}$$

↑
third column

Fig. 2.12

Sample Image Matrix

Source: <http://cnx.org/content/m21457/latest/?collection=col10685/latest>

There are plenty of image watermarking techniques algorithms available in. We will discuss a few of them. Image watermarking depends on the domain in which the watermarking is done: the spatial and frequency domains.

2.2.4 SPATIAL DOMAIN

Several different methods enable watermarking in the spatial domain. The simplest (too simple for many applications) is just to flip the lowest-order bit of chosen pixels. This works well only if the image is not subject to any modification. A more robust watermark can be embedded by superimposing a symbol over an area of the picture. The resulting mark may be visible or not, depending upon the intensity value. Picture cropping, e.g., (a common operation of image editors), can be used to eliminate the watermark.

Spatial watermarking can also be applied using color separation. In this way, the watermark appears in only one of the color bands. This renders the watermark visibly subtle such that it is difficult to detect under regular viewing. However, the mark appears immediately when the colors are separated for printing. This renders the document useless for the print or unless the watermark can be removed from the color band. This approach is used commercially for journalists to inspect digital pictures from a photo-stock house before buying unmarked versions.

A simple Spatial watermarking algorithm— **The LSB technique**

2.2.4.1 LSB – Least Significant Bit Hiding (Image Hiding)

This method is probably the easiest way of hiding information in an image and yet it is surprisingly effective. It works by using the least significant bits of each pixel in one image to hide the most significant bits of another. So in a JPEG image for example, the following steps would need to be taken.

1. First load up both the host image and the image you need to hide.
2. Next chose the number of bits you wish to hide the secret image in. The more bits used in the host image, the more it deteriorates. Increasing the number of bits used though obviously has a beneficial reaction on the secret image increasing its clarity.
3. Now you have to create a new image by combining the pixels from both images. If you decide for example, to use 4 bits to hide the secret image, there will be four bits left for the host image. (PGM - one byte per pixel, JPEG - one byte each for red, green, blue and one byte for alpha channel in some image types)

Host Pixel: 10110001

Secret Pixel: 00111111

New Image Pixel: 10110011

4. To get the original image back you just need to know how many bits were used to store the secret image. You then scan through the host image, pick out the least significant bits according the number used and then use them to create a new image with one change - the bits extracted now become the most significant bits.

Host Pixel: 10110011

Bits used: 4

New Image: 00110000

Figure Least significant bit hiding.

ORIGINAL IMAGES



Bits Used: 1



Bits Used: 4 Bits Used: 7

Fig 2.13:Steganography Techniques Computer Security

To show how this technique affects images, Figure 6 shows examples using different bit values. Dr. Ryan's image on the left is the host image while Mr. Sexton's on the right is the secret one we wish to hide.

This method works well when both the host and secret images are given equal priority. When one has significantly more room than another, quality is sacrificed. Also while in this example an image has been hidden, the least significant bits could be used to store text or even a small amount of sound. All you need to do is change how the least significant bits are filled in the host image. However this technique makes it very easy to find and remove the hidden data

The LSB technique is the simplest technique of watermark insertion. If we specifically consider till images, each pixel of the color image has three components—red, green and blue. Let us assume we allocate 3 bytes for each pixel. Then, each colour has 1 byte, or 8 bits, in which the intensity of that colour can be specified on a scale of 0 to 255.

So a pixel that is bright purple in colour would have full intensity for red and blue, but no green. Thus that pixel can be shown as

$$X_0 = \{R=255, G=0, B=255\}$$

Now let's have a look at another pixel:

$$X_1 = \{R=255, G=0, B=254\}$$

We've changed all the value of B here. But how much of a difference does it make to the human eye? For the eye, detecting a difference of 1 on a scale of 256 is almost impossible.

Now since each color is stored in a separate byte, the last bit in each byte stores this difference of one. That is, the difference between values 255 and 254, or 127 and 126 is stored in the last bit, called the Least Significant Bit (LSB). Since this difference does not matter much, when we replace the color intensity information in the LSB with watermarking information, the image will still look the same to the naked eye.

Thus a simple algorithm for this technique would be: Let W be watermarking information for every pixel in the image, X_i

Do Loop:

Store the next bit from W in the LSB position of X_i [red] byte
Store the next bit from W in the LSB position of X_i [green] byte
Store the next bit from W in the LSB position of X_i [blue] byte
End Loop

To extract watermark information, we would simply need to take all the data in the LSBs of the color bytes and combine them.

A modification of this method would be to use a secret key to choose a random set of bits, and

Replace them with the watermark. This technique of watermarking is invisible, as changes are made to the LSB only, but is not robust. Image manipulations, such as resampling, rotation, format conversions and cropping, will in most cases result in the watermarking formation being lost

2.2.5 FREQUENCY DOMAIN

In watermarking in the transform domain, the original host data is transformed, and the transformed coefficients are perturbed by a small amount in one of several possible ways in order to represent the watermark. Coefficient selection is based on perceptual significance or energy significance. When the watermarked image is compressed or modified by any image processing operations, noise is added to the already perturbed coefficients. The private retrieval operation subtracts the received coefficients from the original ones to obtain the noise perturbation. The watermark is then estimated from the noisy data as best as possible. The most difficult problem associated with blind watermark detection in the frequency domain is to identify the coefficients used for watermarking. Embedding can be done by adding a pseudo-random noise, quantization (threshold) or image (logo) fusion. Most algorithms consider HVS to minimize perceptibility. The aim is to place more information bits where they are most robust to attack and are least noticeable. Most schemes operate directly on the components of some

transform of the cover like Discrete Cosine Transform(DCT), Discrete Wavelet Transforms(DWT), and Discrete Fourier Transforms (DFT). In this section we will introduce each domain, illustrates its main features and introduce some techniques that used this domain in watermarking.

2.2.6 PROPOSED WATERMARKING SCHEME

The wavelet decomposition decomposes the image into three spatial directions i.e. horizontal, vertical and diagonal. Hence wavelets reflect the an isotropic properties of HVS more precisely. The human visual system (HVS) is related to the perceptual quality ,measured according to the sensitivity/ sharpness of a humane yet to see details in an image. Research into human perception in dicates that the retina of the eye splits an image into several frequency channels each spanningab and width of approximately one octave. The signal sin these channels are processed in dependently. Similarly, inmultire solution decomposition, the image is separate d into bands of approximately equal bandwidth on a logarithmic scale. It is therefore expected that use of the discrete wavelet transform will allow the independent processing of the resulting components without significant perceptible interaction between them, and hence makes the process of imperceptible watermarking

More effective. The multi resolution successive approximation not only enhances the resolution of an image, but also enhances the resolution of watermark simultaneously. This advantage of the DWT allows using higher energy watermark sinre gions where the HVS is known to beless sensitive so that embedding watermarks in the seregions provides to increase the robustness of the watermarking techniques. The watermark detection is a blind method i.e .is with out the use of original image. We embed a watermark into an image by modifying coefficient so fmid frequency bands i.e. LH and HL sub-bands, and extract the watermark by analyzing perturbation of coefficients from a suspected image.

2.2.6.1 DISCRETE WAVELET TRANSFORM(DWT)

The Fourier transform, which provides a representation of the transformed signal in the frequency domain, is widely used in signal processing. However, the loss of time information in a signal by Fourier transform will lead to the difficulty in processing. The wavelet transform is an excellent time-frequency analysis method, which can be well adapted for extracting the information content of the image. A brief introduction to wavelet is as follows.

MULTIPLE-LEVEL DECOMPOSITION

Applying a 1-D wavelet transform to all the rows of the image and then repeating on all of the columns can compute the 2-D wavelet transform. When one-level 2-D DWT is applied to an image, four transform coefficient sets are created. The four sets are LL, HL, LH, and HH, where the first letter corresponds to applying either low pass frequency operation or high pass frequency operation to the rows, and the second letter refers to the filter applied to the columns.

Wavelet analysis of an original image can be divided into an approximate image LL and three detail images LH, HL and HH. The approximate image holds most of the information of the original image, while the others contain some details such as the edge and textures will be represented by large coefficients in the high frequency sub-bands. The reconstruction of the image is achieved by the inverse discrete wavelet transform (IDWT).

2.2.6.2 WATERMARK EMBEDDING TECHNIQUE

The pseudo random sequences generated with the key as the initial seed are added to the horizontal and vertical DWT coefficients (HL, LH) of the original image according to the equation:

$$I_w(x, y) = I(x, y) + k \times W(x, y) \quad (1)$$

In which $I(x, y)$ representing the DWT coefficients of the original image, $I_w(x, y)$ is the watermarked image, K denotes the gain factor that is usually used to adjust the invisibility of the watermark. The robustness of the watermarked image increases as the gain K increases. But, with increase in the gain K the quality of the final watermarked image reduces. If the pixel in the watermark vector is zero then the PN sequence with appropriate gain is added to the selected Sub-band coefficients, the watermark embedding process is shown in Fig.

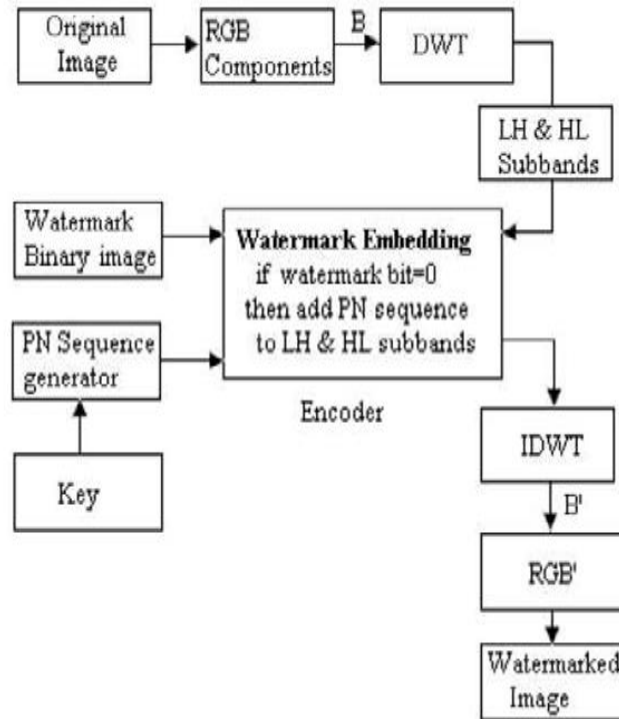


Fig. 2.14

WATERMARKING EMBEDDING TECHNIQUE

Source:

http://www.ee.uta.edu/Dip/Courses/EE5359/Abrar%20Ahmed%20Syed_Digital%20Watermarking.pdf

2.2.6.3 WATERMARK EXTRACTION TECHNIQUE

Proposed watermarking scheme deals with the extraction of the watermark information in the absence of the original image, i.e., blind watermarking. Hence correlation measure, is used to detect the watermark. The correlation is calculated between the generated PN sequence matrix and modified sub-band coefficients for each of the pixel in the watermark string and if it exceeds a particular threshold then the watermark is said to be detected. The threshold for the decision is set as the mean of the correlation value for all the pixels. During computation in the first level resolution the watermark is called detected, if the correlation between the extract edbit sand the original bits is above a threshold. If the reiso watermarked detected then, the decode radds the second resolution level. Once again, if the correlation between the extracted bits and the original bits is above a threshold then the watermark i detected, the watermark extraction process is shown.

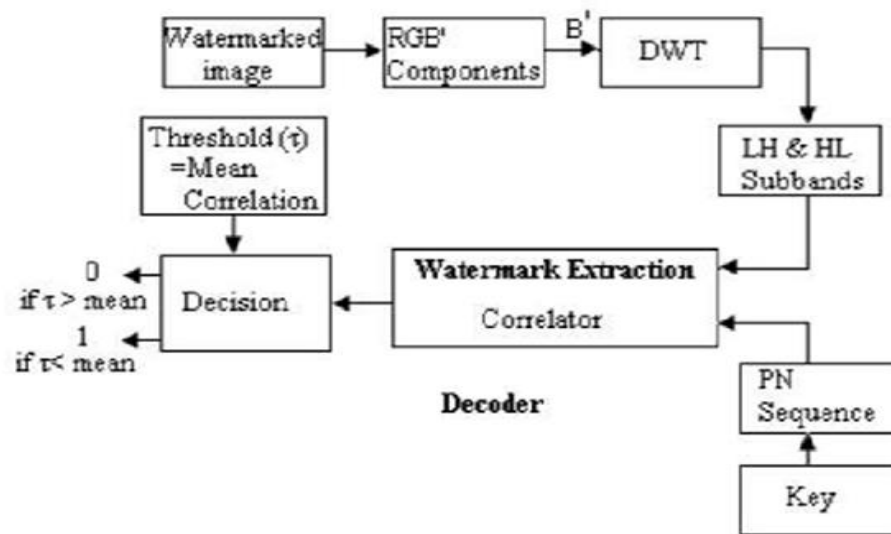


Fig. 2.15

Watermarking Extraction Technique

Source:http://www.ee.uta.edu/Dip/Courses/EE5359/Abrar%20Ahmed%20Syed_Digital%20Watermarking.pdf

CODES:



Fig 2.16: ORIGINAL IMAGE (COVER IMAGE)



Fig 2.17: IMAGE TO BE EMBEDDED

2.3 LSB(Least Significant Bit)Technique

2.3.1 EMBEDDING

```
clearall;
%cover object used for embedding
file_name='CT22.bmp';
cover_object=imread(file_name);
c_double=uint8(double(cover_object));
%message image that needs to be hide in the cover image
file_name='sign2.bmp';
message=imread(file_name);
%conversionsneededtospreadtheimagevaluesona256gray- scale
message=double(message);
message=round(message./256);
message=uint8(message);
%determine the size of cover image used for
embeddingMc=size(cover_object,1);    %Height
Nc=size(cover_object,2);%Width
%determine the size of message object to embed
Mm=size(message,1);                %Height
Nm=size(message,2);                %Width
%titlethemessageobjectouttocoverobjectsizetogenerate watermark
forii = 1:Mc
forjj = 1:Nc
watermark(ii,jj)=message(mod(ii,Mm)+1,mod(jj,Nm)+1);
end;
end;
```

OUTPUT:



Fig2.18: EMBEDDEDING OF IMAGE USING LSB

2.3.2 RECOVERY

```
clearall;
%read in watermarked image
file_name='lsb_watermarked.bmp';
watermarked_image=imread(file_name);
%determine size of
watermarked image Mw=size(watermarked_image,1);
%Height
%use lsb of watermarked image to recover watermark
forii = 1:Mw
forjj = 1:Nw
watermark(ii,jj)=bitget(watermarked_image(ii,jj),1);
end
end
%scale the recovered watermark
watermark=256*double(watermark);
%scale and display recovered watermark
figure(1)
imshow(watermark,[])
imwrite(watermark,'lsb_recover_watermark.bmp');
title('RecoveredWatermark')
```


OUTPUT:

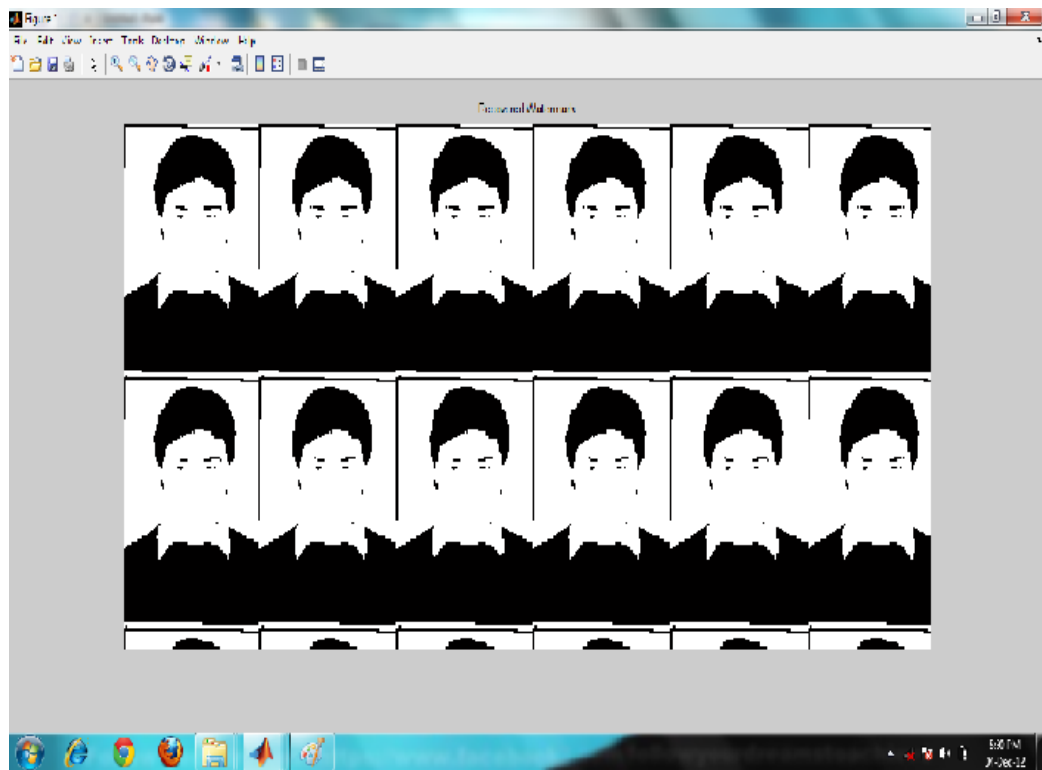


Fig 2.19:IMAGE RECOVERY USING LSB ALGORITHM

2.4 DWT(DISCRETEWAVELETTRANSFORM)TECHNIQUE

2.4.1 EMBEDDING

```
clc;
clf;
clearall;
%readcover image file_name='lena.bmp';
X=imread(file_name);
%decompositionof cover image
[cA1,cH1,cV1,cD1]= dwt2(X,'db1');
%readpayload image file_name='ITBHU3200.bmp';
J=imread(file_name);

imshow(X);
title('Cover image');
subplot(1,2,2);
imshow(J);
title('Payload img');

title('LL plane');
subplot(2,2,2);
imshow(cH1);
title('HL plane');

subplot(2,2,3);
imshow(cV1);
title('LH plane');
subplot(2,2,4);
imshow(cD1);
title('HH plane');
%determining size
cod=(cA1);
I=double(cod);
[m,n]=size(I);
```

```

%forming a new image matrix w from J of scale factors as m and n
w=imresize(J,[m,n]);

%setting the gain factor for embedding
k=input('Gain factor k=');

%creating another new matrix w1 with gain factor multiplied
w1=w*k;
J1=double(w1);
% Adding the new matrix values to the approximation coefficient matrix
for i=1:m
    for j=1:n
        A(i,j)=I(i,j)+J1(i,j);
    end
end

%plotting the LL plane images figure;
subplot(1,2,1);
cod1=double(cod);
imshow(uint8(cod1));
title('LLplane without watermarked image');

subplot(1,2,2);
imshow(uint8(A));
title('LLplane with watermarked image');

%plotting the final watermarked image figure;
watermarked_image= idwt2(A,cH1,cV1,cD1,'db1');
watermarked_convertedimage=uint8(watermarked_image);
imshow(watermarked_convertedimage);
title('stegoimage');
imwrite(watermarked_convertedimage,'dwtwatermarkedimage1.bmp','bmp');

```

OUTPUT:

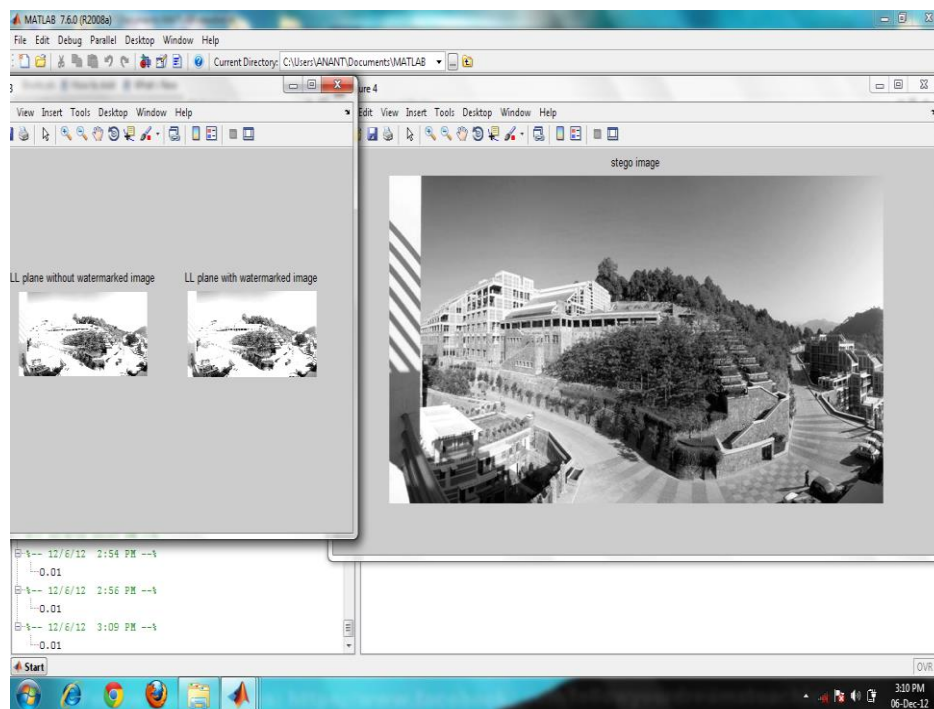
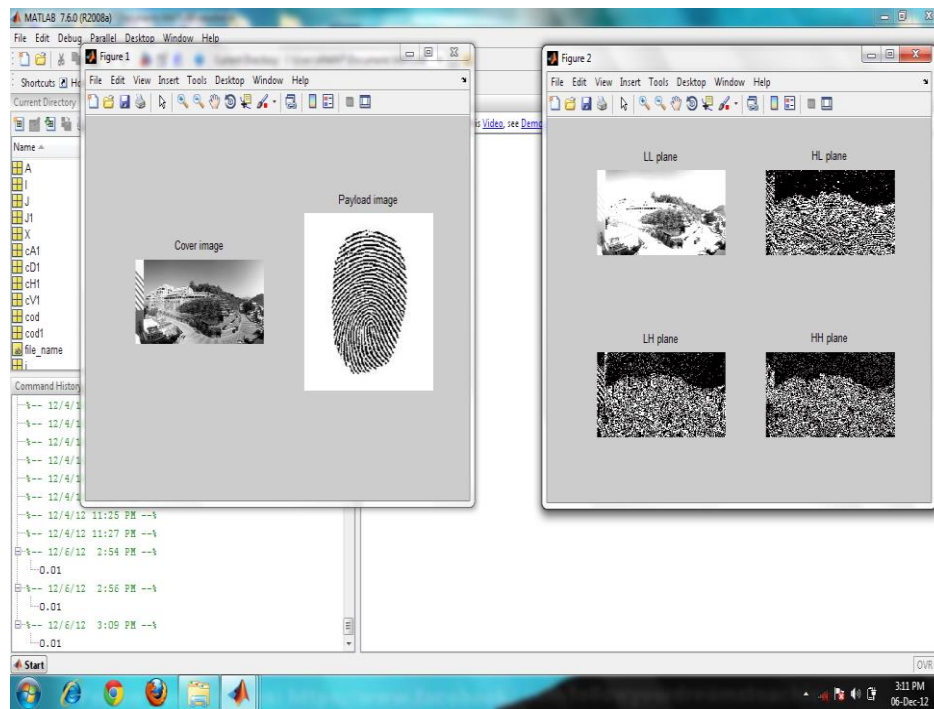


Fig 2.20: EMBEDDING USING DWT ALGORITHM

2.4.2 RECOVERY

```
Clc
clearall;
%readcover image file_name='lena.bmp'; X=imread(file_name);
%decomposingthe cover image [cA1,cH1,cV1,cD1] = dwt2(X,'db1');
J8=cA1;
%settingthe gain factor for embedding
k=input('scaling factor k=');
%readin the watermarked image
file_name='dwtwatermarkedimage1.bmp';
A0=imread(file_name);
%decomposing the watermarked image
[cA1,cH1,cV1,cD1]= dwt2(A0,'db1');
%determiningsize of one of the decomposed coefficients ie
cA [x,y]=size(cA1)
cA1=double(cA1);
%subtracting the original values of coefficient
from the coefficient of% watermarkedimage
and dividing by scale factor for i=1:x

forj=1:y
s(i,j)=cA1(i,j)-J8(i,j);
s(i,j)=s(i,j)/k;
end
%resizingthe resulted image matrix s1=imresize(s,[256 256]);
s1=double(s1);

%plottingthe images figure(1)
imshow(A0);
title('Watermarkedimage');
figure(2);
message=uint8(s1);
imshow(message);
title('extracted image');
imwrite(message,'dwtrecoveredwatermark1.bmp','bmp');
```

OUTPUT:

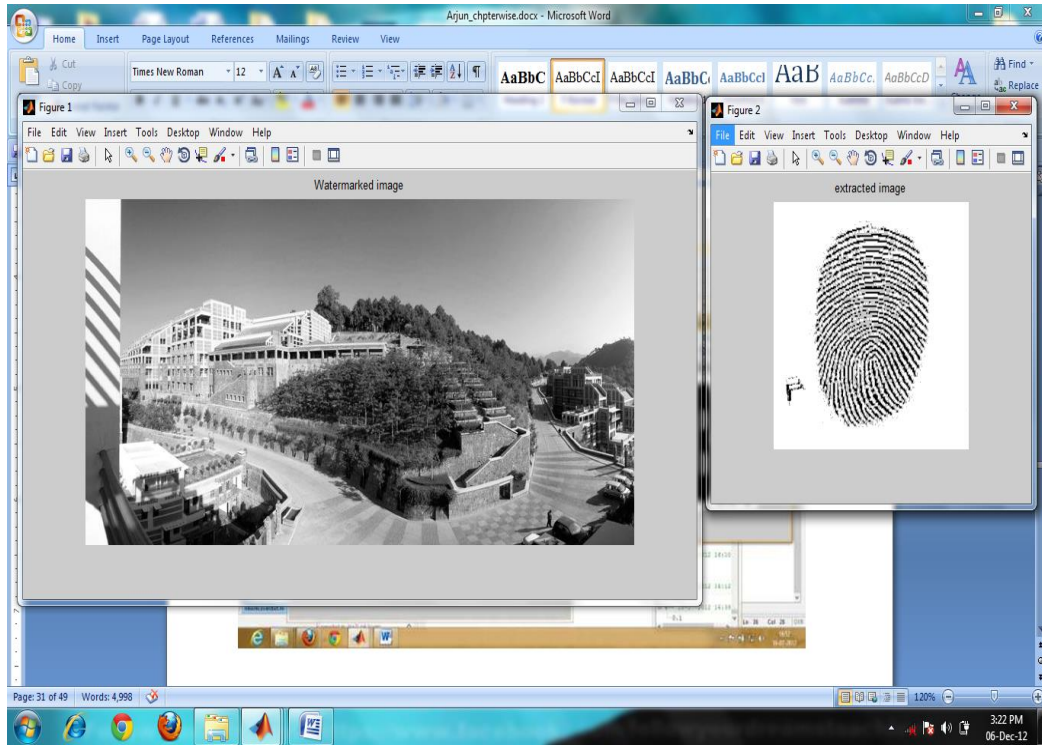


Fig 2.21: IMAGE RECOVERY USING DWT ALGORITHM

2.5 COMPARISON b/w LSB and DWT

Limitations of Spatial Domain Watermarking

This method is comparatively simple, lacks the basic robustness that may be expected in any watermarking applications. It can survive simple operation such as cropping, any addition of noise. However lossy compression is going to defeat the watermark. An even better attack is to set all the LSB bits to '1' fully defeating the watermark at the cost of negligible perceptual impact on the cover object. Furthermore, once the algorithm was discovered, it would be very easy for an intermediate party to alter the watermark.

2.6 ADVANTAGES OF DWT

The watermarking method has multi resolution characteristics and is hierarchical. It is usually true that the human eyes are not sensitive to the small changes in edges and textures of an image but are very sensitive to the small changes in the smooth parts of an image. With the DWT, the edges and textures are usually to the high frequency sub bands, such as HH,LH, HL etc. Large frequencies in these bands usually indicate edges in an image.

The watermarking method robust to wavelet transform based image compressions, such as embedded zero-tree wavelet(EZW) image compression scheme, and as well as to other common image distortions, such as additive noise ,rescaling / stretching, and half toning.

COMPARING RESULTS

For Cover Image and

Payload Image



Fig 2.22

LSB EMBEDDING



Fig 2.23

LSB RECOVERY

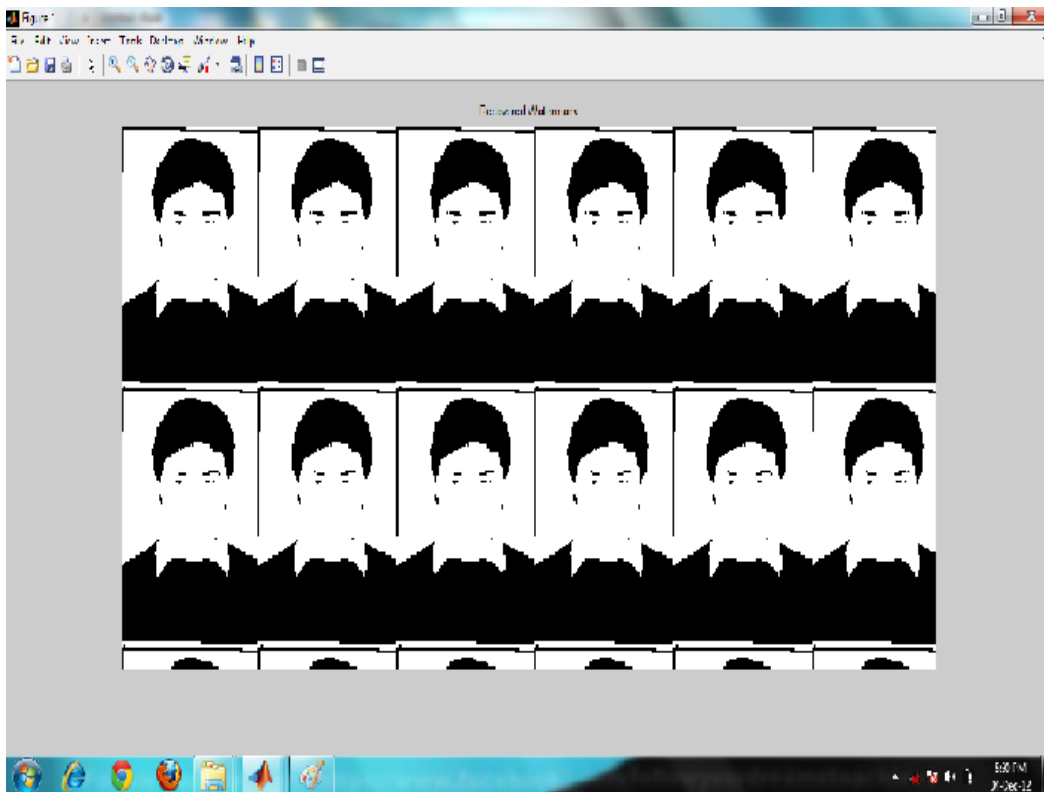


Fig 2.24

DWT EMBEDDING(GAINFACTOR=0.01)

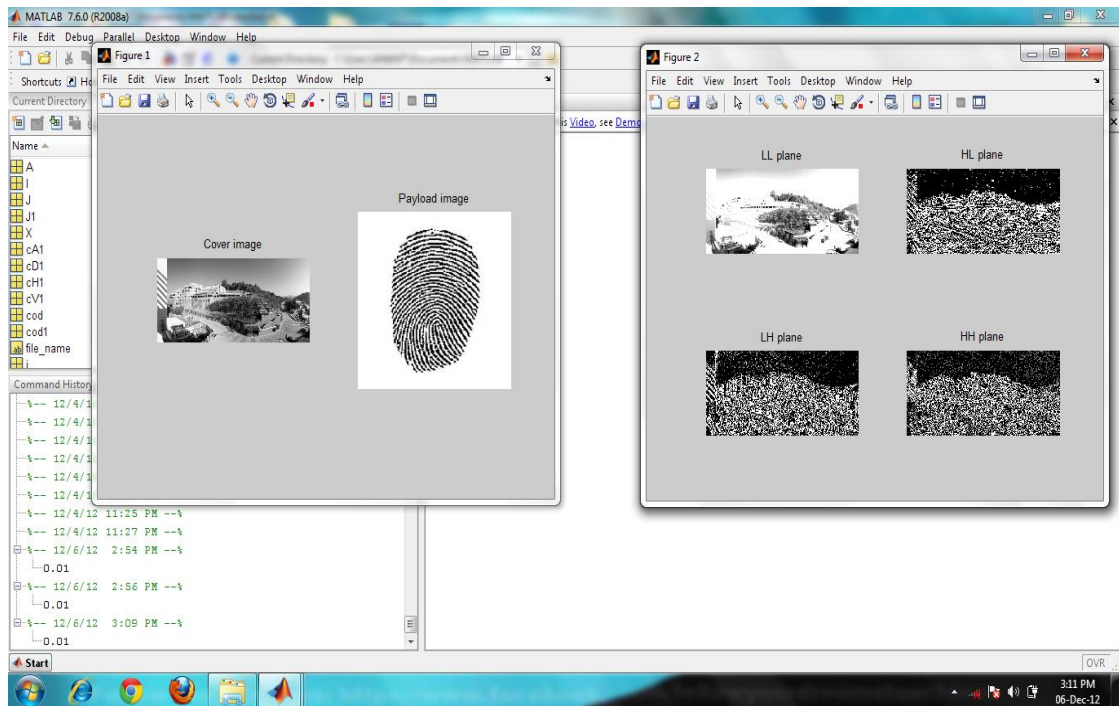


Fig 2.25

DWT RECOVERY(GAIN FACTOR=0.01)

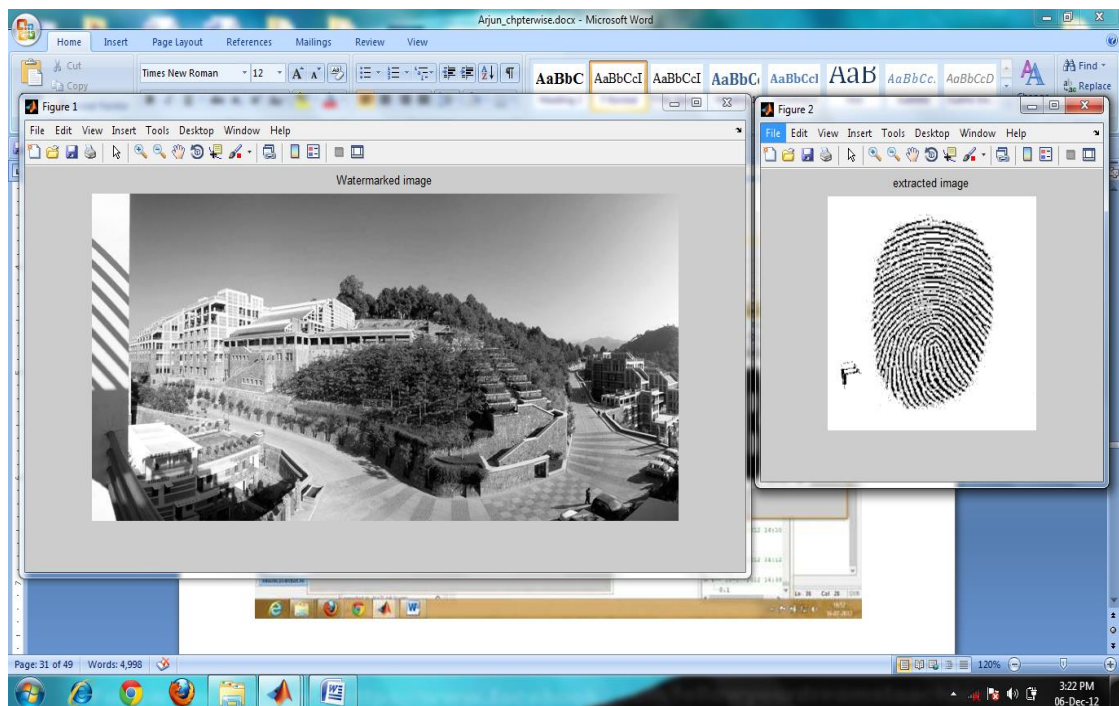


Fig 2.26

For Cover Image2

and

Payload Image2



Fig 2.27

LSB embedding



Fig 2.28

LSB RECOVERY



Fig 2.29

DWT EMBEDDING

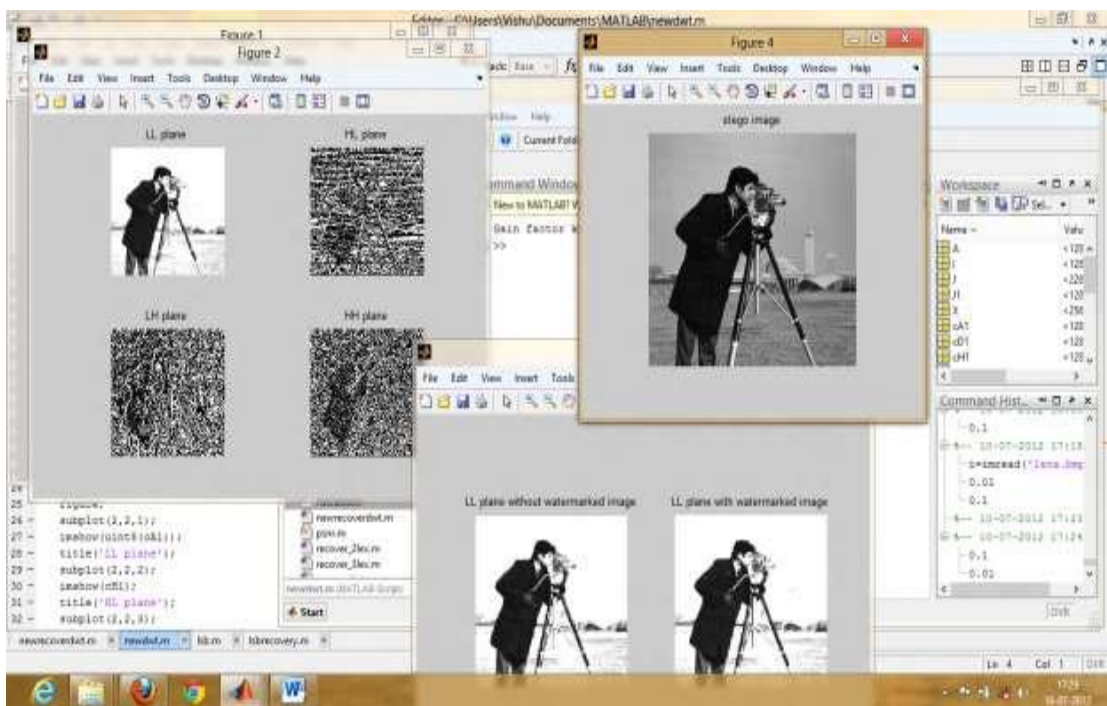


Fig 2.30

DWT RECOVERY



Fig 2.31

2.7 SINGULAR VALUE DECOMPOSITION

In linear algebra, the singular value decomposition (SVD) is a factorization of a real or complex matrix, with several applications in signal processing [2]. The SVD can be seen as a generalization of the spectral theorem to arbitrary, not necessarily square matrices. The basic idea behind SVD is taking high dimensional highly variable set of data points and reducing it to a lower dimensional space that exposes the substructure of the original data more clearly. Suppose M is an m -by- n matrix. Then there exists a factorization for M of the form $M=U \Sigma V^T$ where, U is an m -by- m unitary matrix, a diagonal matrix Σ is m -by- n with non-negative numbers in descending order and V^T denotes the conjugate transpose of V , an n -by- n unitary matrix. Such a factorization is called a singular value decomposition of M .

A matrix is orthogonal if $UTU=VTV=I$

- 1) The matrix V thus contains a set of orthonormal input vector directions for the matrix M .
- 2) The matrix U thus contains a set of orthonormal output basis vector directions for the matrix M .
- 3) The matrix Σ contains the singular values, which can be thought of as scalar gain controls by which each corresponding input is multiplied to give a corresponding output.

2.7.1 DCT DOMAIN WATERMARKING

Discrete Cosine Transform (DCT) method is used to convert time domain signal into frequency domain signal. Using DCT, an image is easily split into pseudo frequency bands and in this work watermark is inserted into middle band frequencies because as we discussed in all frequency domain watermarking schemes, there is a conflict between robustness and transparency. A DCT is a Fourier related transform similar to 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 Fourier transform of real and even function is real and even).

2.7.2 DWT DOMAIN WATERMARKING

Wavelet transform has been widely studied in signal processing in general and image compression in particular. Here DWT2 (Two dimensional Discrete Wavelet Transform) method is used to decompose the image into four sub bands namely LL, LH, HL & HH. LL-Low frequency band LH-Horizontal high frequency band HL-Vertical high frequency band HH-Diagonal high frequency band Wavelet coding schemes are especially suitable for applications where scalability and

tolerable degradation are important.

2.7.3 Characteristics of DWT

- 1) The wavelet transform decomposes the image into three spatial directions i.e. horizontal, vertical and diagonal. Hence wavelets reflect the anisotropic properties of HVS more precisely.
- 2) Watermark detection at lower resolutions is computationally effective because at every successive resolution level there are few frequency bands involved.
- 3) As LL band contains largest wavelet coefficients, scale factor is chosen accordingly up to 0.05 for LL and 0.005 for other bands. For this pair of values, there is no degradation in watermarked image.
- 4) High resolution sub bands helps to easily located and texture pattern sinan image .

2.8 DCT-SVD BASED WATERMARKING

Robustness, capacity and imperceptibility are the three important requirements of an efficient watermarking scheme. SVD based watermarking scheme has high imperceptibility. Although the SVD based scheme withstands certain attacks, it is not resistant to attacks like rotation, sharpening etc. Also SVD based technique has only limited capacity [4]. These limitations have led to the development of a new scheme that clubs the properties of DCT and SVD. This particular algorithm proves to be better than ordinary DCT based watermarking and ordinary SVD based watermarking scheme.

2.9 DWT-SVD BASED WATERMARKING

The above mentioned SVD-DCT scheme has enormous capacity because data embedding is possible in all the sub-bands. Watermark was found to be resistant to all sorts of attacks except rotation and achieved good imperceptibility. Disadvantage is that the embedding and the recovery are time consuming process because the zigzag scanning to map the coefficients into four quadrants based on the frequency. Alternatively if we apply DWT we get the four frequency sub-bands directly namely; approximation, horizontal, vertical and diagonal bands. So the time consumption will be greatly reduced [15]. Also, SVD is a very convenient tool for watermarking in the DWT domain.

2.10 DWT-DCT-SVDBASED WATERMARKING

This method utilizes the wavelet coefficients of the cover image to embed the watermark. Any of the three high frequency sub bands of wavelet coefficients can be used to watermark the image. The DCT coefficients of the wavelet coefficients are calculated and singular values decomposed. The singular values of the cover image and watermark are added to form the modified singular values of the watermarked image. Then the inverse DCT transform is applied followed by the inverse DWT. This is the algorithm that clubs the properties of SVD, DCT and DWT. Watermark embedded using this algorithm is highly imperceptible. This scheme is robust against all sorts of attacks. It has very high data hiding capacity. . The new method was found to satisfy all the requisites of an ideal watermarking scheme such as imperceptibility or fidelity, robustness and good capacity. Also, the method is robust against different kinds of mentioned attacks. This method can be used for authentication and data hiding purposes.

2.11 SVD

In linear algebra, the singular value decomposition (SVD) is a factorization of a real or complex matrix, with many useful applications in signal processing and statistics.

Formally, the singular value decomposition of an $m \times n$ real or complex matrix M is a factorization of the form

$$M = U \Sigma V^*$$

where U is a $m \times m$ real or complex unitary matrix, Σ is an $m \times n$ rectangular diagonal matrix with nonnegative real numbers on the diagonal, and V^* (the conjugate transpose of V) is an $n \times n$ real or complex unitary matrix.

2.11.1 Digital Image Processing

An image can be defined as a two dimension function $f(x, y)$ (2D image), where x and y are spatial coordinates, and the amplitude of f at any pair of (x, y) is gray level of the image at that point. For example, a grey level image can be represented as:

$$f_{ij} \text{ Where } f_{ij} = f(x_i, y_j)$$

When x , y and the amplitude value of f are finite, discrete quantities, the image is called “a digital image”. The finite set of digital values is called picture elements or pixels. Color images are formed by a combination of individual 2D images. Many of the image processing techniques for monochrome images can be extend to color image (3D) by processing the three components image individually. Digital Image Processing (DIP) refers to processing a digital image by mean of a digital computer, and the study of algorithms for their transformation. Since the data of digital image is in the matrix form, the DIP can utilize a number of mathematical techniques. The essential subject areas are computational linear algebra, integral transforms, statistics and other techniques of numerical analysis.

In particular, digital image processing is the practical technology for area of:

- Image compression
- Classification
- Feature extraction
- Pattern recognition
- Projection
- Multi scale signal analysis

2.11.2 Theory of Singular Value Decomposition

2.11.2.1 Process of Singular Value Decomposition

Singular Value Decomposition (SVD) is said to be a significant topic in linear algebra by many renowned mathematicians. SVD has many practical and theoretical values; special feature of SVD is that it can be performed on any real (m, n) matrix. Let's say we have a matrix A with m rows and n columns, with rank r and $r \leq n \leq m$. Then the A can be factorized into three matrices:

$$A = USV^T$$

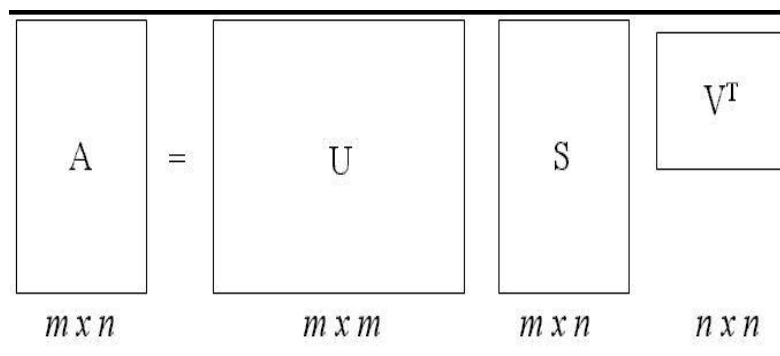


Illustration of Factoring A to USV

Where Matrix U is an $m \times m$ orthogonal matrix

$$U = [\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_r, \mathbf{u}_{r+1}, \dots, \mathbf{u}_m]$$

column vectors \mathbf{u}_i , for $i = 1, 2, \dots, m$, form an orthonormal set:

$$\mathbf{u}_i^T \mathbf{u}_j = \delta_{ij} = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}$$

And matrix V is an $n \times n$ orthogonal matrix

$$V = [V_1, V_2, \dots, V_r, V_{r+1}, \dots, V_n]$$

column vectors \mathbf{v}_i for $i = 1, 2, \dots, n$, form an orthonormal set:

$$V_i^T V_j = \delta_{ij} = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}$$

Here, S is an $m \times n$ diagonal matrix with singular values (SV) on the diagonal. The matrix S can be showed in following

$$S = \begin{bmatrix} \sigma_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & \sigma_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \sigma_r & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & \sigma_{r+1} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & \sigma_n \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{bmatrix}$$

For $i = 1, 2, \dots, n$, σ_i are called Singular Values (SV) of matrix A. It can be proved that

$$\sigma_1 \geq \sigma_2 \geq \dots \geq \sigma_r > 0,$$

and

$$\sigma_{r+1} = \sigma_{r+2} = \dots = \sigma_n = 0.$$

For $i = 1, 2, \dots, n$, σ_i are called Singular Values (SVs) of matrix A. The \mathbf{v}_i 's and \mathbf{u}_i 's are called right and left singular vectors of A [1].

2.11.3 Example

Consider the 4×5 matrix

$$M = \begin{bmatrix} 1 & 0 & 0 & 0 & 2 \\ 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 & 0 \end{bmatrix}$$

A singular value decomposition of this matrix is given by $\mathbf{U}\mathbf{\Sigma}\mathbf{V}^*$

$$\mathbf{U} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

$$\mathbf{\Sigma} = \begin{bmatrix} 4 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & \sqrt{5} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$\mathbf{V}^* = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ \sqrt{0.2} & 0 & 0 & 0 & \sqrt{0.8} \\ 0 & 0 & 0 & 1 & 0 \\ -\sqrt{0.8} & 0 & 0 & 0 & \sqrt{0.2} \end{bmatrix}$$

Notice $\mathbf{\Sigma}$ is zero outside of the diagonal and one diagonal element is zero. Furthermore, because the matrices \mathbf{U} and \mathbf{V}^* are unitary, multiplying by their respective conjugate transposes yields identity matrices, as shown below. In this case, because \mathbf{U} and \mathbf{V}^* are real valued, they each are an orthogonal matrix.

$$\mathbf{U}\mathbf{U}^* = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \equiv \mathbf{I}_4$$

And

$$\begin{aligned}
\mathbf{V}\mathbf{V}^* &= \begin{bmatrix} 0 & 0 & \sqrt{0.2} & 0 & -\sqrt{0.8} \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & \sqrt{0.8} & 0 & \sqrt{0.2} \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ \sqrt{0.2} & 0 & 0 & 0 & \sqrt{0.8} \\ 0 & 0 & 0 & 1 & 0 \\ -\sqrt{0.8} & 0 & 0 & 0 & \sqrt{0.2} \end{bmatrix} \\
&= \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \equiv \mathbf{I}_5
\end{aligned}$$

This particular singular value decomposition is not unique. Choosing \mathbf{V} such that

$$\mathbf{V}^* = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ \sqrt{0.2} & 0 & 0 & 0 & \sqrt{0.8} \\ \sqrt{0.4} & 0 & 0 & \sqrt{0.5} & -\sqrt{0.1} \\ -\sqrt{0.4} & 0 & 0 & \sqrt{0.5} & \sqrt{0.1} \end{bmatrix}$$

2.11.4 Properties of the SVD

There are many properties and attributes of SVD, here we just present parts of the properties that we used in this project.

1. The singular value s_1, s_2, \dots, s_n are unique, however, the matrices \mathbf{U} and \mathbf{V} are not unique.

2. Since $A^T A = V S^T S V^T$, so V diagonalizes $A^T A$, it follows that the \mathbf{v}_j 's are the eigenvectors of $A^T A$.

3. Since $A A^T = U S S^T U^T$, so it follows that U diagonalizes $A A^T$ and that the \mathbf{u}_i 's are the eigenvectors of $A A^T$.

4. If A has rank of r then $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_r$ form an orthonormal basis for range space of A^T , $R(A^T)$, and $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_r$ form an orthonormal basis for range space A , $R(A)$.

5. The rank of matrix A is equal to the number of its nonzero singular values.

2.11.5 METHODOLOGY OF SVD APPLIED TO IMAGE PROCESSING

2.11.5.1 SVD Approach for Image Compression

Image compression deals with the problem of reducing the amount of data required to represent a digital image. Compression is achieved by the removal of three basic data redundancies:

- 1) coding redundancy, which is present when less than optimal;
- 2) interpixel redundancy, which results from correlations between the pixels;

3) psychovisual redundancies, which is due to data that is ignored by the human visual.

The property 5 of SVD in section 2 tells us “the rank of matrix A is equal to the number of its nonzero singular values”. In many applications, the singular values of a matrix decrease quickly with increasing rank. This propriety allows us to reduce the noise or compress the matrix data by eliminating the small singular values or the higher ranks.

When an image is SVD transformed, it is not compressed, but the data take a form in which the first singular value has a great amount of the image information. With this, we can use only a few singular values to represent the image with little differences from the original.

To illustrate the SVD image compression process, we show detail procedures:

$$A = USV^T = \sum_{i=1}^r \sigma_i \mathbf{u}_i \mathbf{v}_i^T$$

That is A can be represented by the outer product expansion:

$$A = \sigma_1 \mathbf{u}_1 \mathbf{v}_1^T + \sigma_2 \mathbf{u}_2 \mathbf{v}_2^T + \cdots + \sigma_r \mathbf{u}_r \mathbf{v}_r^T$$

When compressing the image, the sum is not performed to the very last SVs, the SVs with small enough values are dropped. (Remember that the SVs are ordered on the diagonal.)

The closet matrix of rank k is obtained by truncating those sums after the first k terms:

$$A_k = \sigma_1 \mathbf{u}_1 \mathbf{v}_1^T + \sigma_2 \mathbf{u}_2 \mathbf{v}_2^T + \cdots + \sigma_k \mathbf{u}_k \mathbf{v}_k^T$$

The total storage for k A will be

$$k(m + n + 1)$$

The integer k can be chosen confidently less than n , and the digital image corresponding to k A still have very close the original image. However, the chose the different k will have a different corresponding image and storage for it.

For typical choices of the k , the storage required for k A will be less the 20 percentage.

2.11.6 PROPOSED ALGORITHM USING DWT AND SVD TECHNIQUES

2.11.6.1 Embedding Watermark

- Use three level Haar DWT to decompose the image A in to four sub bands (i.e., $LL3$, $LH3$, $HL3$, and $HH3$)
- Apply SVD to $HL3$ sub band i.e.,
 $A_i = U_i S_i$, Where $A_i = HL3$
- Apply SVD to the watermark i.e.,
 $W = U_w S_w$, Where $W = \text{Watermark}$

- Modify the singular value of A_i by embedding singular value of W such that

$$S_{iw} = S_i + \alpha \times S_w$$

Where S_{iw} is modified singular matrix of A_i and α denotes the scaling

Factor is used to control the strength of watermark signal

- Then apply SVD to this modified singular matrix S_{iw} i.e.,

$$S_{iw} = U_{S_{iw}} S_{S_{iw}} V_{S_{iw}}^T$$

- Obtain the modified DWT coefficients, i.e.,

$$A_{iw} = U_i \times S_{S_{iw}} \times V_i^T$$

- Obtain the watermarked image A_w by applying inverse DWT using one modified and other non modified DWT coefficients.

2.11.6.2 Watermark Extraction

- Apply three level haar DWT to decompose the watermarked image A_w in to four sub bands (i.e., $LL3$, $LH3$, $HL3$, and $HH3$).

- Apply SVD to $HL3$ sub band i.e.,

$$T A_{iw} = U_{iw} S_{iw} V_{iw}$$

Where $A_{iw} = H$ Compute $S_w = (S_{iw} - S) / \alpha$, Where S_w singular matrix of extracted watermark (possibly extorted).

Apply SVD to S_w i.e.,

$$S_w = U_{S_w} S_{S_w} V_{S_w}^T$$

- Now Compute extracted watermark W i.e.,

$$W = U_w \times S_{S_w} \times V_w^T$$

2.12 DISCRETE WAVELET TRANSFORM-SINGULAR VALUE DECOMPOSITION HYBRID CODE

```
%  
  
clear;  
  
clc  
  
image= imread('lena.bmp');  
  
image=imresize(image,[256 256]);  
  
[M,N]=size(image);  
  
image=double(image);  
  
[op1,az1,qw1,er1]=dwt2(image,'haar');  
  
[op2,az2,qw2,er2]=dwt2(op1,'haar');  
  
[op3,az3,qw3,er3]=dwt2(op2,'haar');  
  
[U1image,S1image,V1image]=svd(op3);  
  
S1image_temp=S1image;  
  
image_wat= imread('juit.bmp');  
  
image_wat=imresize(image_wat,[32 32]);  
  
alfa= input('ALFA VALUE = ');  
  
[x y]=size(image_wat);  
  
image_wat=double(image_wat);  
  
[u11 s11 v11]=svd(image_wat);  
  
S1image =S1image + alfa * s11;  
  
[U_SHL_w1,S_SHL_w1,V_SHL_w1]=svd(S1image);  
  
Wimage1 =U1image* S_SHL_w1 * V1image';
```

```

Wimage2= idwt2(Wimage1,az3,qw3,er3,'haar',[M,N]);
Wimage3= idwt2(Wimage2,az2,qw2,er2,'haar',[M,N]);
Wimage4= idwt2(Wimage3,az1,qw1,er1,'haar',[M,N]);
figure(1)
imshow(uint8(image));
title('ORIGINAL IMAGE ')
figure(2)
imshow(uint8(image_wat));
title('WATERMARK')
figure(3)
imshow(uint8(Wimage4));
title('WATERMARKED IMAGE')
mse=(sum(sum((double(image)-double(Wimage4)).^2))/(M*N))
PSNR=10*log10(255^2./mse);
msg=sprintf('\n\n-----\nWatermark by SVD PSNR=%fdB\n-----
-----\n\n', PSNR);
disp(msg);
nimage=imnoise(uint8(Wimage4),'gaussian');
mse=(sum(sum((double(image)-double(nimage)).^2))/(M*N))
PSNR=10*log10(255^2./mse);
msg=sprintf('\n\n-----\nWatermark by SVD PSNR with gaussian
noise=%fdB\n-----\n\n', PSNR);
disp(msg);
figure(4);
imshow(nimage);

```



```

n1img=imnoise(uint8(Wimage4) , 'poisson');

mse=(sum(sum((double(image)-double(nimage)).^2))/(M*N))

PSNR=10*log10(255^2./mse);

msg2=sprintf('\n\n-----\nWatermark by SVD PSNR with poisson
noise=%fdB\n-----\n\n', PSNR);

disp(msg2);

figure(5);

imshow(n1img);

J = medfilt2(Wimage4);

r=corr2(Wimage4,J);

msg1=sprintf('\n\n-----\n Correlation Coefficient=%fdB \n-----
-----\n\n',r);

disp(msg1);

%

[op111,az111,qw111,er111]=dwt2(Wimage4,'haar');

[op222,az222,qw222,er222]=dwt2(op111,'haar');

[op333,az333,qw333,er333]=dwt2(op222,'haar');

[U1Wimage S1Wimage V1Wimage]=svd(op333);

Watermark1= (S1Wimage- S1image_temp)/alfa ;

[Uw1 Sw1 Vw1]=svd(Watermark1);

w1=u11*Sw1*v11;

figure(8)

imshow(uint8(w1));

mse=(sum(sum((double(image_wat)-(double(w1))).^2))/(M*N));

PSNR=10*log10(255^2./mse);

```

```
msg=sprintf('\n\n-----\nWatermark by SVD PSNR=%f dB\n-----\n\n', PSNR);  
  
disp(msg);
```

OUTPUT:

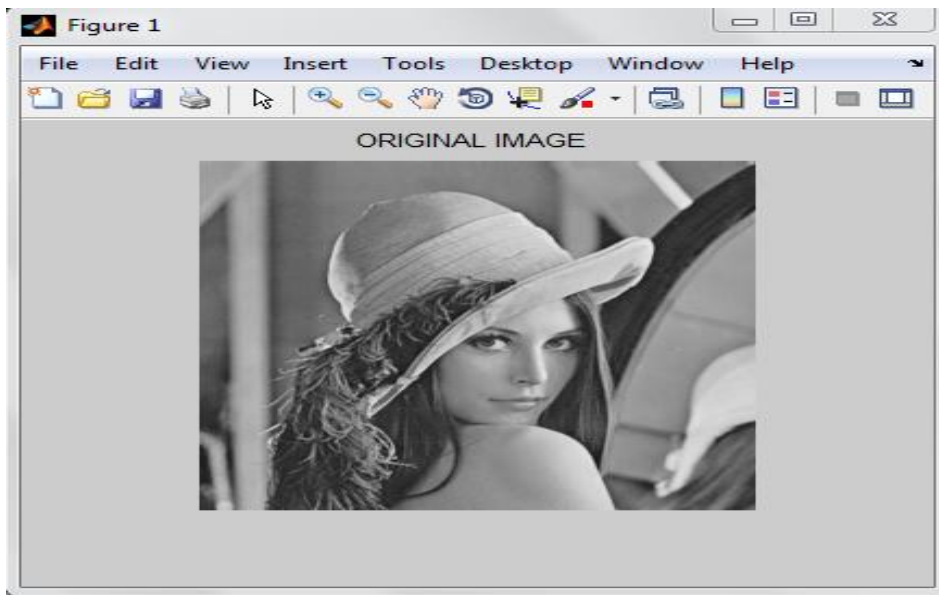


Fig 2.32: ORIGINAL IMAGE

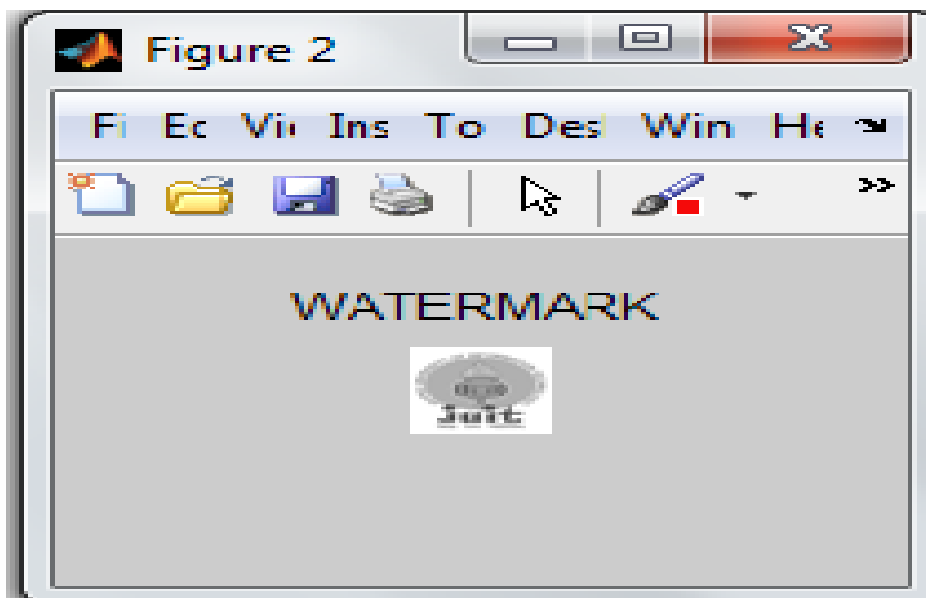


Fig 2.33: WATERMARK

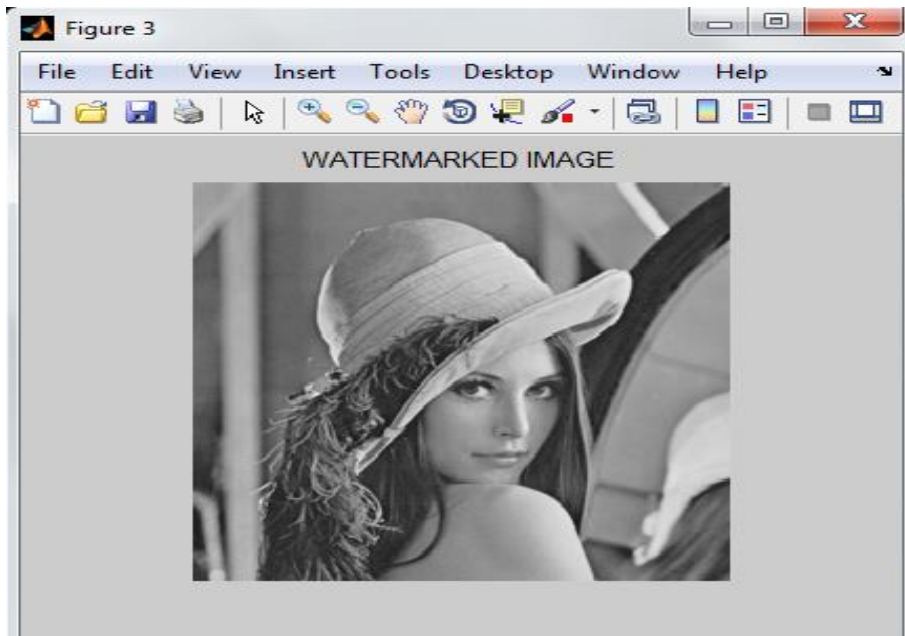


Fig 2.34 :WATERMARKED IMAGE

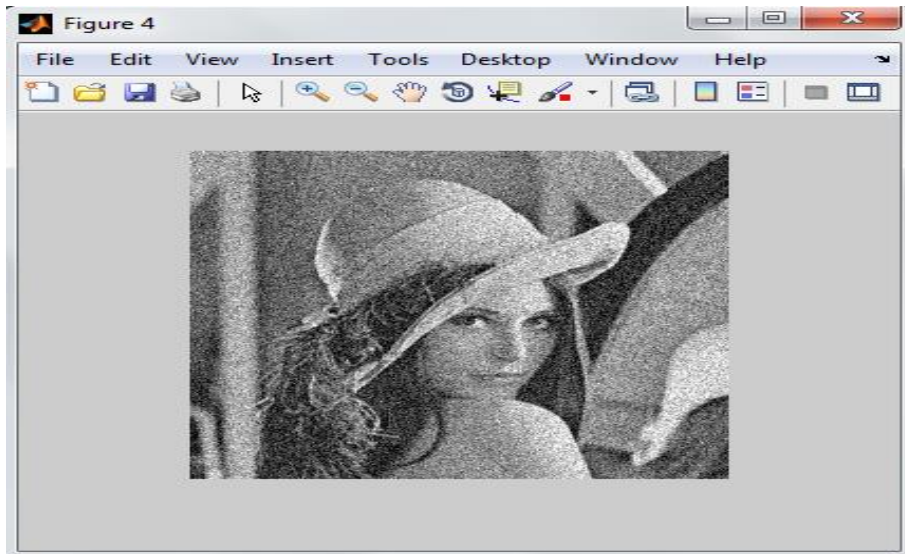


Figure 2.35:Gaussian noise

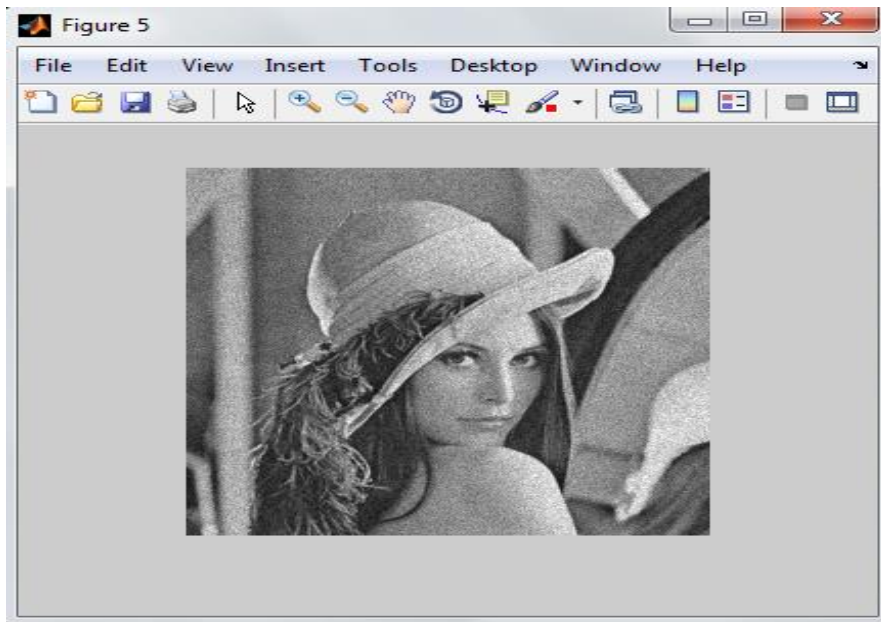


Figure 2.36:Poisson Noise

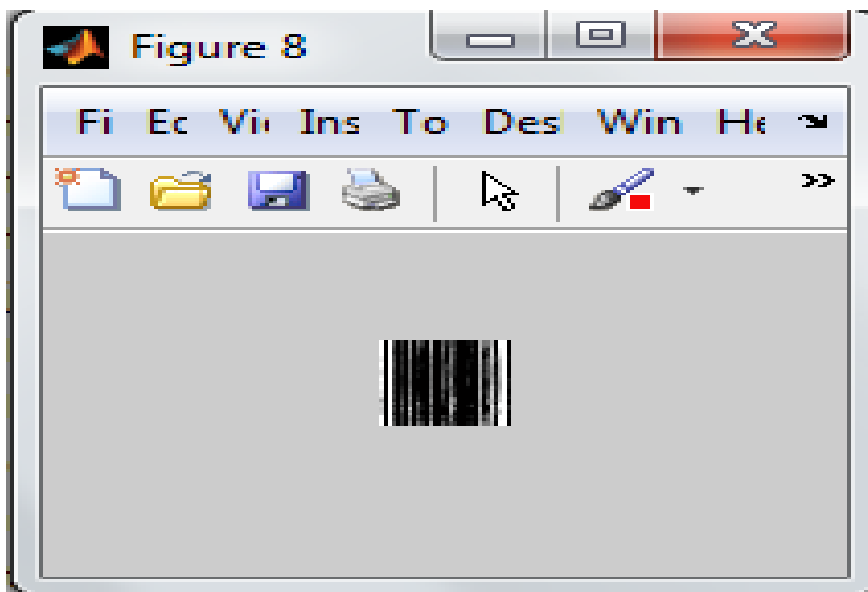


Fig 2.37:Recovery Image

CHAPTER 3

3.1 HARDWARE AND SOFTWARE REQUIREMENTS

The execution phase was developed based upon three phases that are proposed in the chapter 3 hardware and software requirement section. The different phases are encryption, decryption and implementation phases. We require few hardware and software interfaces for implementing these phases. The software interface which is implemented in this project is done using the MATLAB running in the Windows environment. The main aim of the project is to improve the data security when the data is transmitted using the transmission medium. This can be done by embedding the secret data into the image file and then transmitting the encrypted data through the transmission medium. Then, the carrier image file is decrypted at the destination by using the secret key. For implementing the above procedure, I used the MATLAB framework to create the steganographic application. The proposed method in this project can be used for both “encryption” and “decryption” of the message from the digital image.

FEATURES OF THE PROPOSED METHOD

In this project, the proposed method should provide better security when transmitting or transferring the data or messages from one end to another. The main objective of the project is to hide the message or a secret data into an image which further act as a carrier of secret data and to transmit to the destination securely without any modification. If there are any perceivable changes when we are inserting or embedding the information into the image or if any distortions occur in the image or on its resolution there may be a chance for an unauthorised person to modify the data. So, the data encryption into an image and decryption and steganography plays a major role in the project. The three important sections in the project are: Encryption: In this section for encryption, I have

used LSB (Least Significant bit) algorithm which helped me to build a steganographic application to provide better security. The LSB algorithm provides better security compared to JSteg algorithm with improved data compression and data hiding capacities. Steganography: I have used the image as carrier for transmission of data and by us the “Least Significant bit Algorithm” I have inserted the message bits in to the least significant pixels of an image. Decryption: The decryption process is similar but opposite to the encryption process. When the receiver wants to decrypt the data from the image, it uses same “least significant bit algorithm” for extracting the data from the image by taking password or key as reference.

3.2 SYSTEM REQUIREMENTS

In this section, I like to give a brief description about the requirements for building the proposed system. The external interfaces required for building a steganographic system are, software, hardware, and communication media.

3.3 SOFTWARE REQUIREMENT

MATLAB 2010 is used in the project for developing the application and for execution. MATLAB is a high-level language and interactive environment for numerical computation, visualization, and programming. Using MATLAB, you can analyze data, develop algorithms, and create models and applications.

3.4 HARDWARE REQUIREMENTS

Although the hardware is not mandatory for developing a steganographic application for transferring the data from one end to another, HUBs, LAN and Routers are needed for building the communication media from receiver to the sender.

COMMUNICATION MEDIA:

TCP/ IP protocols and E-mails are used as communication media for transferring data from sender to receiver and vice versa.

3.5 OTHER REQUIREMENTS

The other requirements apart from software and hardware are that it's important that the software should be scalable, available, reliable and usable to the users which are important for providing security for data transmission.

USABILITY

Usability is the factor for any data security system; the software should be flexible for transferring the data between one ends to another. It should provide a friendly interface between customer and user.

SCALABILITY

Scalability is one of the important issues when the software used in large institutions where the security plays a major role. Some systems can provide the high level security when the data to be embedded is large. In that case, Scalability plays major role.

RELIABILITY

The data security software or applications are used in many organizations like in military for securing the critical information, in financial organizations for securing the equities and trade information etc., the application should be consistent when using in different applications and provide better security in order to avoid modifications.

AVAILABILITY

Prevention of unauthorized persons from holding the important information. The program should provide the security from unauthorized modifications, should be available only for authorized persons. The program should be flexible and should be available within a mean time and should work in any operating system.

CHAPTER 4

4.1 ARCHITECTURAL DESIGN

The data hiding patterns using the steganographic technique in this project can be explained using this simple block diagram. The block diagram for steganographic technique is as follows

4.1.1 DATA FLOW DIAGRAMS

Data flow diagrams are the basic building blocks that define the flow of data in a system to the particular destination and difference in the flow when any transformation happens. It makes whole procedure like a good document and makes simpler and easy to understand for both programmers and non-programmers by dividing into the sub process. The data flow diagrams are the simple blocks that reveal the relationship between various components of the system and provide high level overview, boundaries of particular system as well as provide detailed overview of system elements

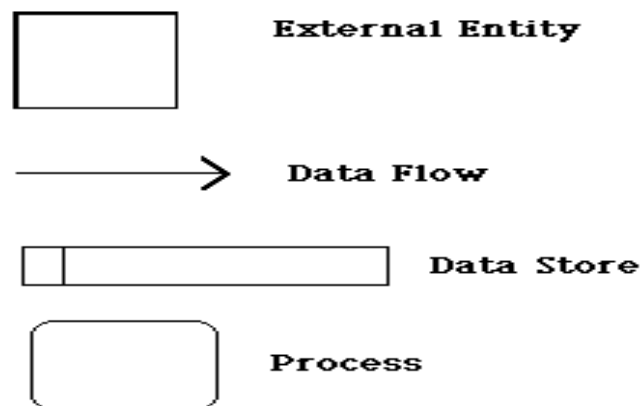


Fig 4.1

PROCESS

Process defines the source from where the output is generated for the specified input. It states the actions performed on data such that they are transformed, stored or distributed.

DATA STORE

It is the place or physical location where the data is stored after extraction from the data source.

SOURCE

It is the starting point or destination point of the data, starting point from where the external entity acts as a cause to flow the data towards destination.

4.1.1.1 DATA FLOW DIAGRAM LEVEL 1

For constructing „DFD level 1“, we need to identify and draw the process that make the level 0 process. In the project for transferring the personal data from source to destination, the personal data is first encrypted and processed and latter decrypted.

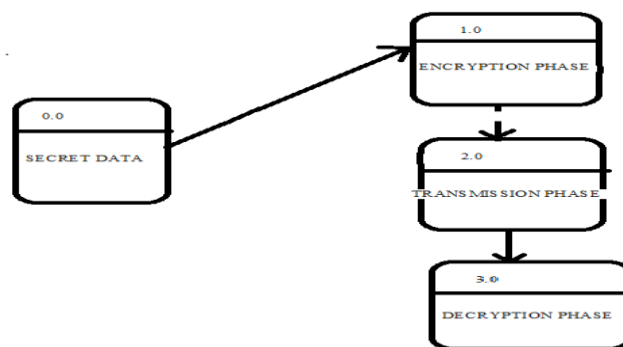


Fig 4.2: DATA FLOW DIAGRAM LEVEL 1

4.1.1.2 DATA FLOW DIAGRAM LEVEL 2

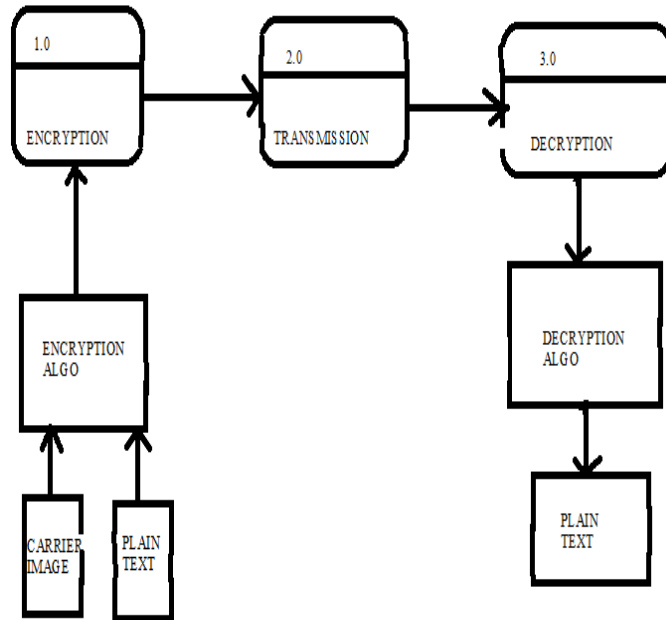


Fig 4.3: DATA FLOW DIAGRAM 2

Image and the text document are given to the encryption phase. The encryption algorithm is used for embedding the data into the image. The resultant image acting as a carrier image is transmitted to the decryption phase using the transmission medium. For extracting the message from the carrier image, it is sent to the decryption section. The plain text is extracted from the carrier image using the decryption algorithm.

4.1.2 ACTIVITY DIAGRAM

The sender sends the message to the receiver using three phases. Since we are using the steganographic approach for transferring the message to the destination, the sender sends text as well as image file to the primary phase i.e., to encryption phase. The encryption phase uses the encryption algorithm by which the carrier image is generated. The encryption phase generates the carrier image as output. The activity diagram explains the overall procedure used for this project.

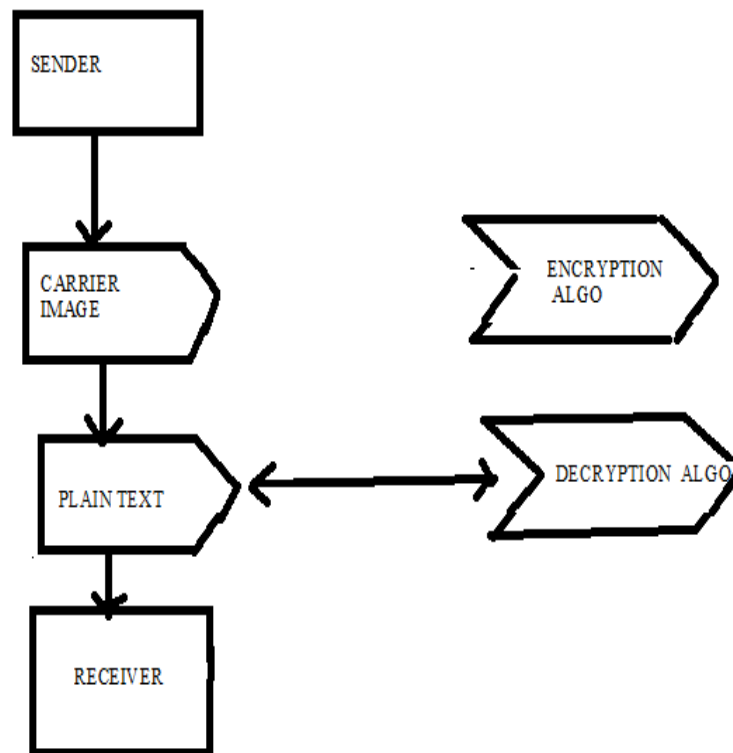


Fig 4.4: ACTIVITY DIAGRAM

CHAPTER 5

5.1 CONCLUSION

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

The benefits of the LSB are its simplicity to embed the bits of the message directly into the LSB plane of cover-image and many techniques using these methods. The LSB does not result in a human perceptible difference because the amplitude of the change is little therefore the human eye the resulting stego-image will look identical to the cover image and this allows high perceptual transparency of the LSB. This report also emphasizes on the fact that digital watermarking provides a comprehensive evaluation algorithm that embeds and extracts the watermarking formation effectively by using DWT. The extraction is done with the help of using original image hence it is an on- blind watermarking scheme. The experimental results show that the scheme is highly robust against various of image processing operations. The observations regarding the implemented watermarking scheme are summarized below:

The primary goal of this report is to bring the SVD to the attention of a broad audience.

The theoretical properties have been described, and close connections were revealed between the SVD and standard topics such as DWT,DCT,LSB.Several applications of the SVD were mentioned, with a detailed discussion.

The computational algorithm for the SVD was also briefly mentioned.

Emphasizing the main themes of the subject has unfortunately meant omitting interesting details and limiting my presentation to general ideas. The reader is encouraged to consult the references for a more thorough treatment of the many aspects of this singularly valuable decomposition.

The simulation results shows that high quality image i.e. watermarked image with high PSNR is obtained by embedding the watermark at low gain, but this will affect the robustness of watermark. The watermark embedding at again above 0.6.

5.2 REFERENCES

[1] Ingemar J. Cox, Joe Killian, Tom Leighton, and TalalShamoon. A secure, robust watermark for multimedia. In Information Hiding. Newton Institute, University of Cambridge, May 1996.

[2] Christian Neubauer and JürgenHerre. Digital watermarking and its inuence on audio quality. In 105th AES Convention, San Francisco, Sep. 1998. preprint 4823.

[3] Christian Neubauer and JürgenHerre. Audio watermarking of MPEG-2 AAC bitstreams.

In 108th AES Convention, Paris, Feb. 2000. preprint 5101.

[4] Daniel Gruhl, Anthony Lu, and Walter Bender. Echo hiding. In Proceedings of the Workshop on Information Hiding, number 1174 in Lecture Notes in Computer Science, Cambridge, England, May 1996. Springer Verlag.

[5] XuChansheng, Wu Jiankang, Sun Quibin, and Xin Kai. Applications of digital watermarking technology in audio signals. Journal of Audio Engineering Society, 47(10):805{812, Oct. 1999.

[6] Jack Wolosewicz. Apparatus and method for encoding supplementary data in analog signals. WO 97/37448, International Application Published under the Patent Cooperation Treaty, Oct. 1997.

- [7] R.A. Willard. ICE identification coding, embedded. In 105th AES Convention, Berlin, Mar. 1993. Audio Engineering Society.
- [8] Laurence Boney, Ahmed H. Tewfik, and Khaled N. Hamdy. Digital watermarks for audio signals. In 1996 IEEE Int. Conf. on Multimedia Computing and Systems, pages 473-480, Hiroshima, Japan, 1996.
- [9] Frank Hartung and Bernd Girod. Watermarking of uncompressed and compressed video. *Signal Processing*, 66(3):283-301, May 1998.
- [10] Ricardo A. Garcia. Digital watermarking of audio signals using a psychoacoustic auditory model and spread spectrum theory. In 107th AES Convention, New York, Sep. 1999. preprint 5073.
- [11] Chong Lee. Method and apparatus for transporting auxiliary data in audio signals. WO 97/09797, International Application Published under the Patent Cooperation Treaty, Mar. 1997.
- [12] Andrew J. Viterbi. *CDMA Principles of Spread Spectrum Communication*. Addison-Wesley, 1995.