INFORMATION HIDING USING STEGANOGRAPHY

A PROJECT REPORT

Submitted By

Namitha K	**312211104064**
Natha Manoj Kumar	**312211104066**
Neela Niranjani V	**312211104067**

in partial fulfillment for the award of the degree

of

BACHELOR OF ENGINEERING

IN

COMPUTER SCIENCE AND ENGINEERING

SSN COLLEGE OF ENGINEERING

KALAVAKKAM 603110

ANNA UNIVERSITY :: CHENNAI - 600025

April 2015

ANNA UNIVERSITY : CHENNAI 600025

BONAFIDE CERTIFICATE

Certified that this project report titled **"INFORMATION HIDING USING STEGANOGRAPHY"** is the *bonafide* work of "**Namitha K (312211104064)**, **Natha Manoj Kumar (312211104066)**, and **Neela Niranjani V (312211104067)**" who carried out the project work under my supervision.

Dr. Chitra Babu
Head of the Department
Professor,
Department of CSE,
SSN College of Engineering,
Kalavakkam - 603 110

Ms. S. Lakshmi Priya
Supervisor
Assistant Professor,
Department of CSE,
SSN College of Engineering,
Kalavakkam - 603 110

Place:
Date:

Submitted for the examination held on. . . . . .

Internal Examiner **External Examiner**

ACKNOWLEDGEMENTS

We thank GOD, the almighty for giving us strength and knowledge to do this project.

We would like to thank and express our deep sense of gratitude to our guide **S. LAKSHMI PRIYA**, Assistant Professor, Department of Computer Science and Engineering, for her valuable advice and suggestions as well as her continued guidance, patience and support that helped us to shape and refine our work.

Our sincere thanks to **Dr. CHITRA BABU**, Professor and Head of the Department of Computer Science and Engineering, for her words of advice and encouragement and we would like to thank our project Coordinator **Dr. S. SHEERAZUDDIN**,Associate Professor, Department of Computer Science and Engineering for his valuable suggestions throughout this project.

We express our deep respect to the founder **Dr. SHIV NADAR**, Chairman, SSN Institutions. We also express our appreciation to our **Dr. S. SALIVAHANAN**, Principal, for all the help he has rendered during this course of study.

We would like to extend our sincere thanks to all the teaching and non-teaching staffs of our department who have contributed directly and indirectly during the course of our project work.

Finally, We would like to thank our parents and friends for their patience, cooperation and moral support throughout our life.

Namitha K **Natha Manoj Kumar** **Neela Niranjani V**

ABSTRACT

Steganography is a branch of information hiding which allows people to communicate in a secure way. As more information is transferred electronically the need for confidentiality of this information increases. The secret message is hidden in a Cover Image using Least Significant Bit (LSB) Replacement technique to obtain the stego image. After hiding the secret text it is important that a ratio called as the Peak Signal to Noise Ratio (PSNR) is high to ensure that the secret message is properly retrieved back. To increase the PSNR value, the stego image is fused with carrier image. For this, the stego image is classified into one of the four categories based on three coefficients - brightness, texture and variation which are calculated using the wavelet coefficients obtained by performing Haar Wavelet Transform. A set of carrier images are selected that belong to the same category as that of the stego image. An iterative fusion algorithm is then used to select the appropriate fusion parameter to choose the best carrier image for hiding the stego image. The average value of PNSR(Cover Image, Stego Image) is 57.75 and the average of PNSR(Cover Image, Fused Image) is 76.81. Thus PSNR value of Stego image increases after fusion. After transmission, the stego image can be retrieved from the fused image and then, the secret message that is present in the stego image can be recovered.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

Introduction

1.1 Image Processing

Image processing is a type of signal processing where the input is an image and the output is either an image or are parameters that describe the image. It converts an image into digital form and performs some operations on it, in order to get an enhanced image or to extract some useful information from it.

Nowadays, with the expansion of internet and its applications, it is possible to transmit information digitally. Because of this, it has become extremely convenient to access and share the information from anywhere in the world. Although it has a lot of advantages, there are some drawbacks as well. The main issue being that the security of the information is compromised. It becomes possible for the attacker to easily access the information and tamper with it. Since the information may be vital, it becomes necessary to use image hiding technologies to secure it.

1.2 Applications of Image Processing

1. **Image Segmentation:** To partition the images into smaller segments so that it becomes more meaningful and easier to analyse.
2. **Image Recognition:** To distinguish the objects present in an image.
3. **Image Retreival:** To retrieve the image of interest.

1.3 Steganography

In regard to the secure transmission of information, we have several techniques to hide information. One such technique is cryptography which encodes information in such a way that only the person who holds the key can read it. But the problem in cryptography is that the hidden message is always visible because information is present in the form of plain text.

Hence we deploy another method called steganography where the information is hidden in a cover media so that others will not be able to notice it. While cryptography is about protecting the content of messages, steganography is about concealing their very existence. Steganography works by replacing bits of useless or unused data in regular computer files (such as graphics, sound, text, HTML) with bits of invisible information. The cover medium is usually chosen keeping in mind the type and the size of the secret message. Digital images are the most popular carrier/cover files that can be used to transmit secret information. The hidden information can be plain text, cipher text or even images.

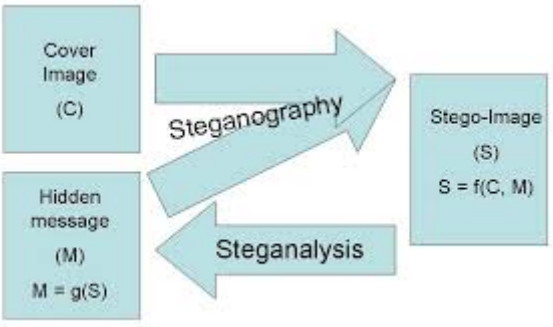

FIGURE 1.1: Steganography Flow Diagram

CHAPTER 2

Literature Survey

Information security is the process of protecting information. Cryptography is one of the essential techniques used for secure transmission of information.

It is related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation.

Data confidentiality may be provided by one of two categories of encryption algorithm, namely symmetric cryptography and asymmetric cryptography. Symmetric, or conventional, cryptography requires that the sender and receiver share a key, which is an item of secret information used to encrypt and decrypt data. The process by which sender and receiver agree upon a key over an insecure medium can be problematic as, until the key is agreed, it is not possible to communicate the secret. Asymmetric, or Public Key, cryptography solves the key exchange problem by using two keys, either of which may be used to encrypt a message. The encrypted data may then only be decrypted by means of the other key. Messages may be received securely by publishing one of the keys (for example, in the footer of an e-mail message) as a Public Key and keeping the second, the Private Key, secret. Anyone wishing to send a secure communication may then encrypt the message with the recipients Public Key and, providing the Private Key has not been disclosed, only the intended recipient will be able to decrypt the encrypted text and recover the original message. But as we have discussed above, steganography is a safer technique than cryptography for secure transmission of information as in case of cryptography only the message is hidden but its existence is not concealed.

S.no.	Context	Steganography	Cryptography
1	Host Files	Image, Audio, Text, etc.	Mostly Text Files
2	Hidden Files	Image, Audio, Text, etc.	Mostly Text Files
3	Result	Stego File	Cipher Text
4	Cipher Text	Steganalysis	Cryptanalysis

TABLE 2.1: Comparision between Steganography and Cryptography

Steganalysis : Analysis of a file with a objective of finding whether it is stego file or not.

In the realm of this digital world, various image hiding techniques have created an atmosphere of corporate vigilance that has spawned various interesting applications. Since Cyber-crime is believed to benefit from this digital revolution, an immediate concern is to find out best methods that preserve the information that needs to be transmitted.

Hence, it becomes necessary to use image hiding techniques for:

- reducing the degradation of the visual quality of the stego image
- being able to completely recover the original image and information.

In general, image hiding techniques can be classified as:

- Substitution
- Masking and Filtering
- Transform Technique

The method of substitution generally does not increase the size of the file. Depending on the size of the hidden image, it can eventually cause an unnoticeable change in the modified version of the image. (eg) Least Significant Bit (LSB) insertion technique is an approach for embedding information in a cover image. In this case, every least significant bit of some or all of the bytes inside an image is changed according to the bits of the information to be hidden. When using a 24-bit image, one bit of each of the primary color components can be used for the above purpose.

The masking and filtering techniques starts with the analysis of the image. Next, we find the significant areas, where the hidden message will be more integrated to cover the image and lastly we embed the data in that particular area.

In addition to the above two techniques for message hiding, transform techniques has also been employed in embedding the message by modulating coefficients in a transform domain. (eg) the Discrete Cosine Wavelet transforms, Haar wavelet transforms , etc.

As stated above, one of the image hiding techniques is steganography which is the art of sending information through original files in a manner that the existence of the message is concealed. Steganalysis is the process of detecting messages hidden using steganograpy. The goal of steganalysis is to identify suspected packages, determine whether or not they have a message encoded into them, and, if possible, recover that message. Unlike cryptanalysis, where it is obvious that intercepted data contains a message (though that message is encrypted), steganalysis generally starts with a pile of suspect data files, but little information about which of the files, if any, contain a hidden message.

Some of the simplest techniques used for steganography are First component altering technique and LSB Steganography.

- First Component Alteration Technique[1]:

  In a computer, images are represented as arrays of values.These values represent the intensities of the three colors R(Red), G (Green) and B (Blue), where a value for each of three colors describes a pixel. Each pixel is combination of three components(R, G, and B).In this scheme, the bits of first component (blue component) of pixels of image have been replaced with data bits, which are applied only when valid key is used. Blue channel is selected because a research reveals that the visual perception of intensely blue objects is less distinct that the perception of objects of red and green.

- LSB Steganography[2,3,7]:

  LSB steganography is a method in which the lowest bit of a bitmap image is used to convey the secret data because the eye cannot detect the very small perturbations it introduces into an image. Some of the LSB steganographic techniques to hide information are LSB matching and LSB Replacement.

  In LSB matching each pixel of the cover image is considered (possibly in a pseudo-random order generated by a shared secret key): if the LSB of the next cover pixel matches the next bit of secret data, do nothing; otherwise, choose to add or subtract one from the cover pixel value, at random.LSB replacement is very similar, except that the LSBs of the cover pixels are overwritten by the secret bit stream. Both LSB replacement and LSB matching leave the LSB unchanged if the message bit matches the LSB. When the message bit does not match the LSB, LSB replacement replaces

the LSB with the message bit; LSB matching randomly increments or decrements the data value by one. LSB matching is also known as 1 embedding.

But LSB replacement is a very simple technique to hide the message inside an image because only half the number of LSB bits get changed on an average. Because of this, there is hardly any noticeable difference between the cover image and the stego image which contains the secret message

In the case of still grayscale images of type bitmap, every pixel is represented using 8 bits, with 11111111 (=255) representing white and 00000000 (=0) representing black. Thus, there are 256 different grayscale shades between black and white which are used in grayscale bitmapimages. In LSB stegonography, the LSBs of the cover image is to be changed. As the message bit to be substituted in the LSB position of the cover image is either 0 or 1, one can state without any loss of generality that the LSB's of about 50 percent pixel changes. There are three possibilities:

1. Intensity value of any pixel remains unchanged.

2. Even value can change to next higher odd value

3.Odd Value change to previous lower even value

To make sure that the message is retrieved back safely it is important to increase the PSNR value. To do this, we fuse the stego image with another image called the carrier image. So the concept of image hiding is introduced. With respect to image hiding two different aspects are considered. First, with a view to the security, the transparence of hiding image has to be improved, that is to make sure the hiding image is invisible to human. Even if it is detected, the hidden information also cannot be extracted by the attacker.

Second, after the fusion image is received, the hidden information shall be extracted with as high quality as possible.

There are various procedures to choose the carrier image for image hiding single iterative blending, multiple iterative blending, chaotic real number sequences, etc

- The single iterative blending algorithm deals only with a single carrier image. Though the blending parameter and the carrier image act as private keys, it becomes easy for the attacker to recover the secret image.

- An improvised version of the single iterative blending algorithm is the multiple iterative blending algorithm where multiple carrier images are used to hide the image. The blending images and the blending parameters and the sequences of images blended can act as private keys. It is impossible for an attacker to get all the blending images and blending parameters, even if the attacker manages to get all the blending images and parameters, he still cannot recover the secret image due to the lack of process of building. So it becomes difficult for the attacker to recover the image. However, due to multiple fusion parameters, the truncation error gets enlarged after every iteration. Hence, the extracted result is not good.

- Another scheme in image hiding involves the usage of chaotic real number sequences (obtained from chaotic dynamical systems) as fusion parameters. In this way, the security of image hiding is improved. However, when the fusion parameter varies in the range of (0,1), the truncation errors are magnified and thus, extracting the original image becomes difficult.

- Another technique used is the hiding image is scrambled via Arnold or chaotic scrambling before hiding. Digital image scrambling can make an image into a completely different meaningless image during transformation, and it is a preprocessing during hiding information of the digital image, which is also known as information disguise. Therefore, the information of hiding image is encrypted in advance. The conventional scrambling ways of Arnold transform are by disordering the pixel positions to get a totally visual difference from the original images. But this kind of method doesnt take into account image hiding effect and extracting quality.

To make sure that the security of image hiding is improved and also, extraction is more efficient, we go for image classification in which the stego image is categorised into one of the four classes based on its brightness, texture and frequency features which are obtained from the wavelet coefficients after performing Haar transform. For all the images from the selected class, iterative fusion algorithm is applied to choose the optimum carrier image

CHAPTER 3

Exisitng System

1) LSB Steganography

LSB steganography is a technique where higher bits of the information to be hidden are stored in least significant bits of the cover image. This is more secure as only the LSB bits of the image is changed , thus giving rise to an almost identical stego image.

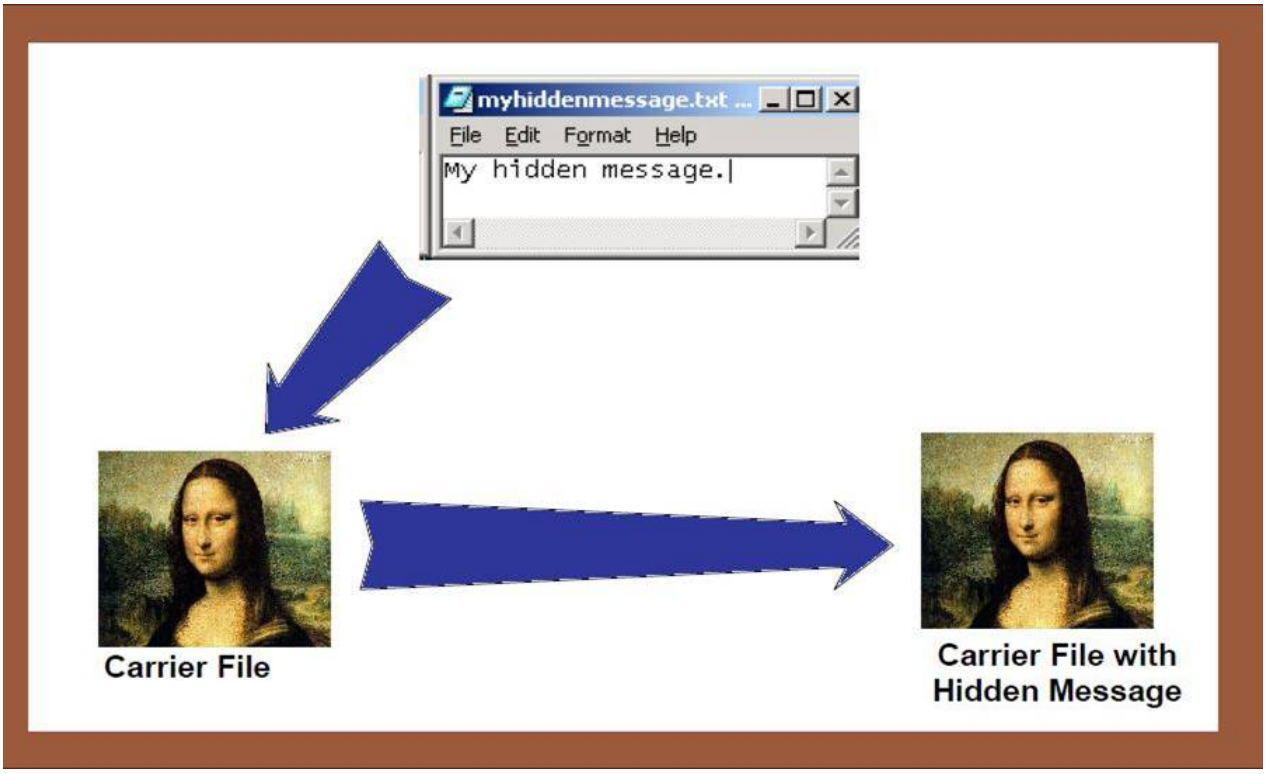

FIGURE 3.1: Abstract LSB Steganography

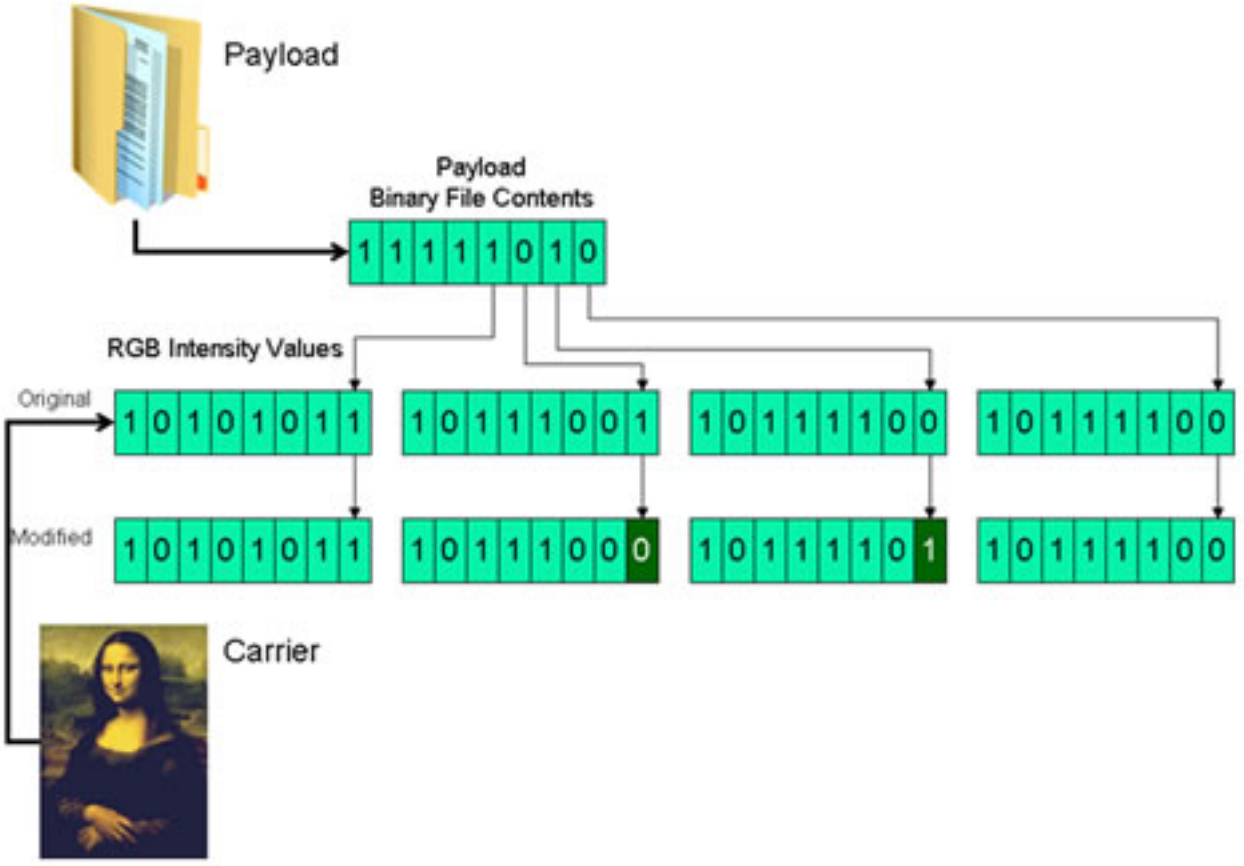

FIGURE 3.2: LSB Steganography Method

LSB Replacement:

The LSB Steganography method generally used is LSB Replacement.LSB replacement method simply replaces the LSB bitplane of a cover image with the corresponding bits of a hidden message. The image with encoded bits is called stego image. This can be done for all pixels in the image or only for a pseudo randomly chosen portion, when the embedding rate is less than one, i.e. the length of the hidden message is less than the number of pixels in the image. The effectiveness of the technique is credited to the fact that LSB replacement is inherently asymmetric, i.e. an even valued pixel will either retain its value or be

incremented by one. However, it will never be decremented. The converse is true for odd-valued pixels. The stego key used contains the length of the message. In

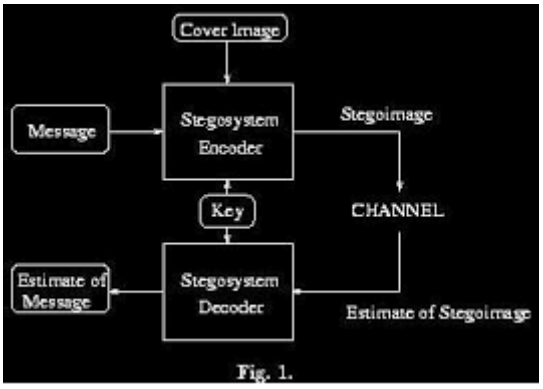

FIGURE 3.3: LSB Replacement process

the receiver side to decode the message the LSB bits are taken from the stego image and represent the bit values of the encoded message. Thus the secret message is obtained. However it is necessary that for efficient retrieval of the information the Peak Signal to Noise Ratio (PSNR) value needs to be high.

2) Image Hiding:

Image hiding is a technique to hide an image within another image(carrier image).It is necessary that for efficiently hiding an image an optimum carrier image needs to be chosen.Only when an optimum carrier image is chosen the image is efficiently hidden so that it is not visible to the outside world and also the PSNR value is high. For any other carrier other than an optimum carrier the hidden image is visible within the fused image. Hence to find the optimum carrier the image is classified into one of the four categories. Then the optimum carrier is selected from a set of carrier images from the same category.

Image classification:

Image classification refers to the task of extracting information classes from an image. Images with similar features are categorized into the same classes. Human eyes have characteristics as follows:

- Human eye is less sensitive to noise in high brightness region than low brightness region.
- Human eye is less sensitive to noise in texture region than smooth region.
- Human eye is less sensitive to noise in high frequency region than low frequency region.

In our approach , we classify images into four categories based on the images brightness , texture and frequency features. Information about these features are obtained from the wavelet coefficients obtained after performing one scale two dimensional Haar wavelet transform. This transform is similar to other transforms like cosine transform , fourier transform , etc.Haar wavelet transforms are advantageous in many ways they are fast and memory efficient because they can be calculated in place without a temporary array . Also , its possible to recover the exact image back without the edge effects which is a problem with other transforms.

One Dimensional Haar Transform:

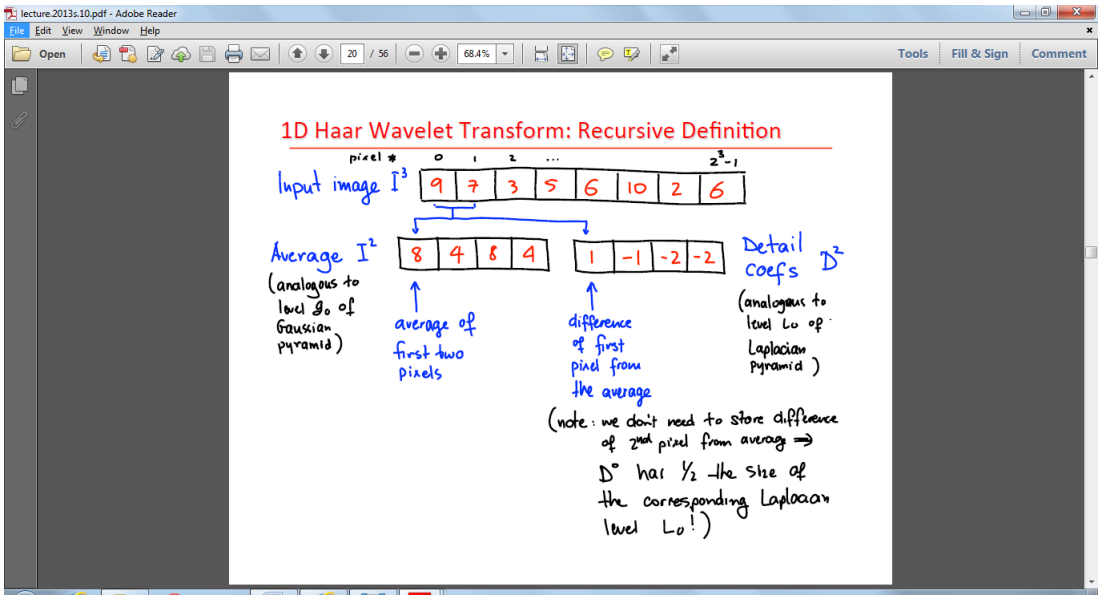

FIGURE 3.4: One Dimensional Haar Transform part 1

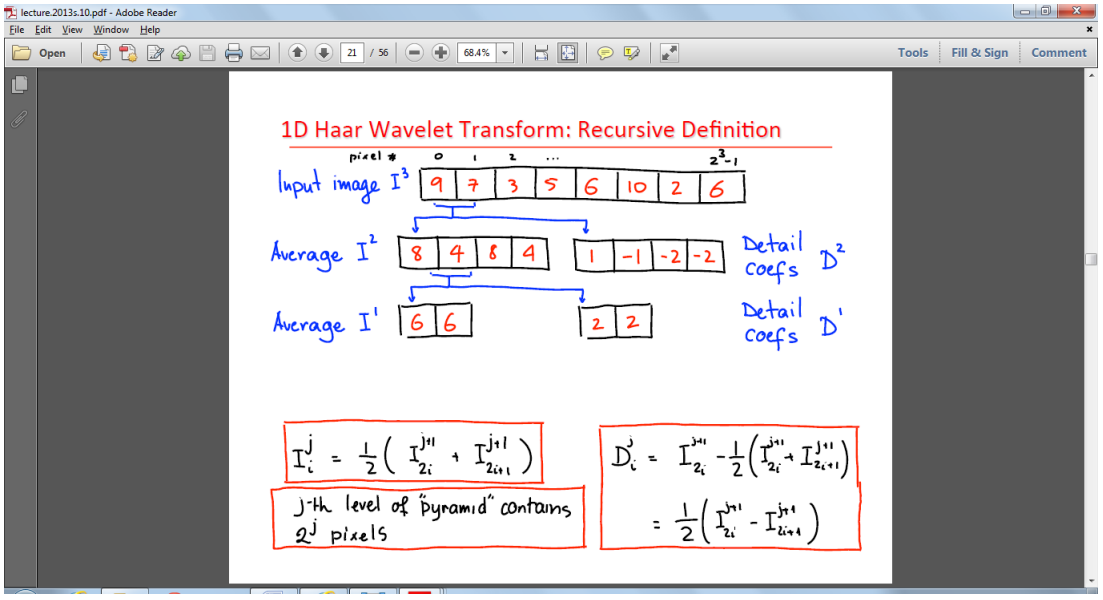

FIGURE 3.5: One Dimensional Haar Transform part 2

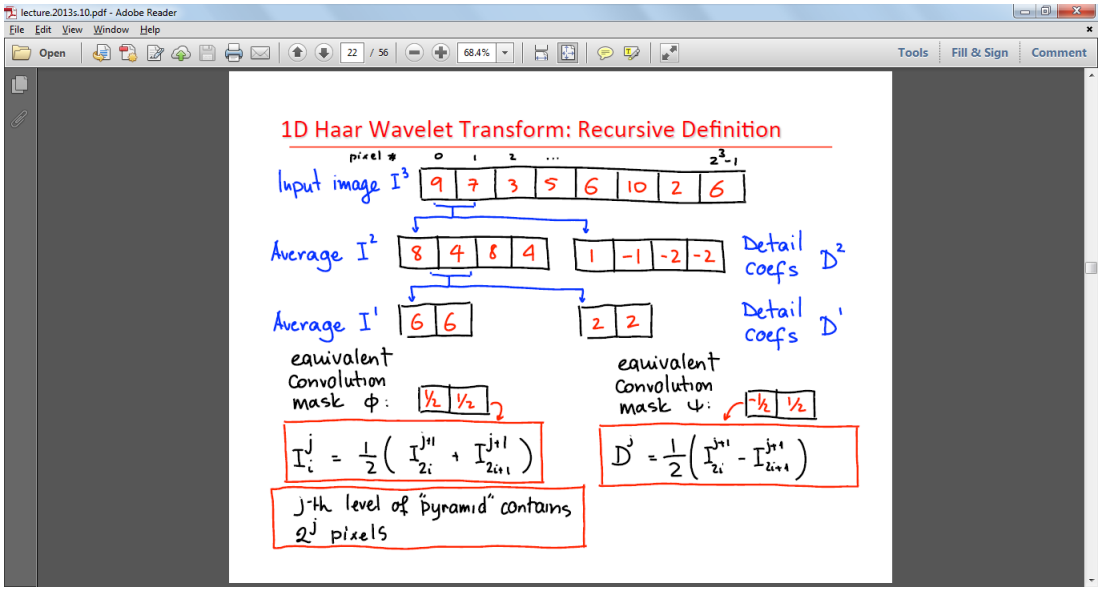

FIGURE 3.6: One Dimensional Haar Transform part 3

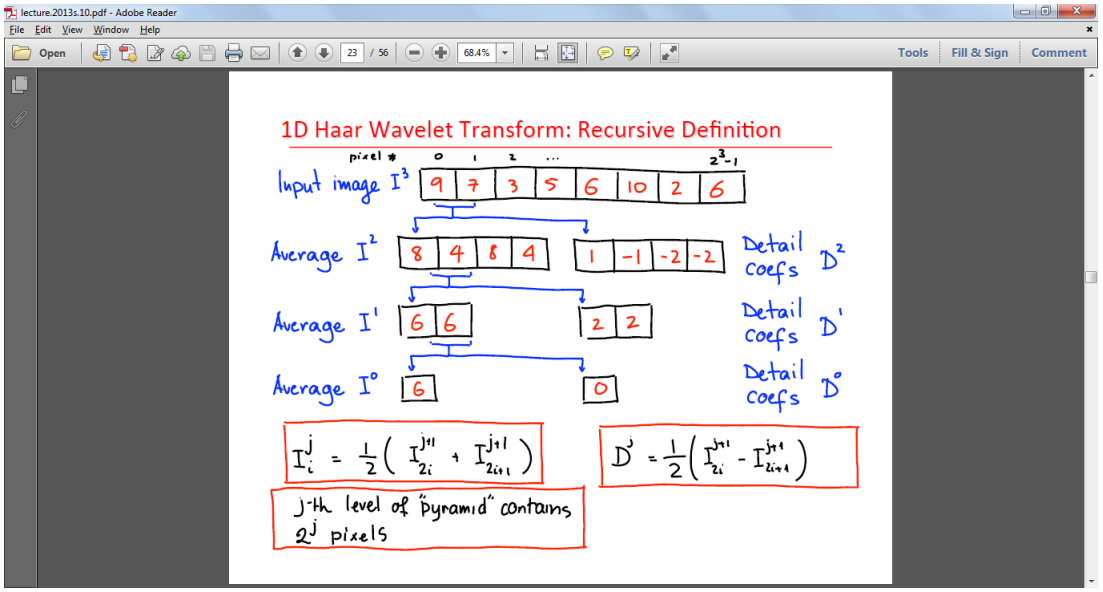

FIGURE 3.7: One Dimensional Haar Transform part 4

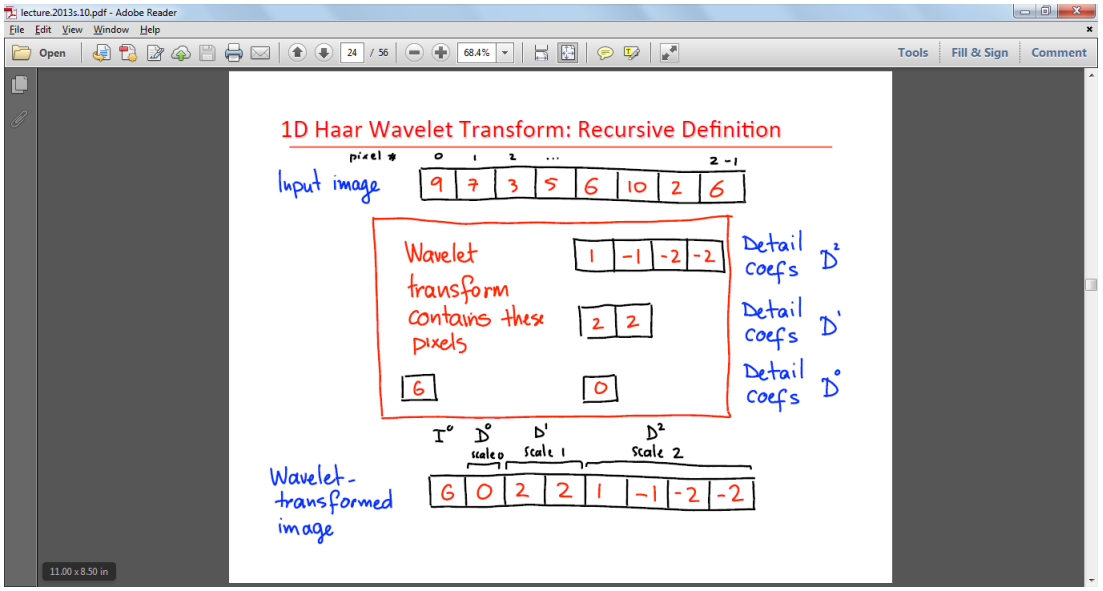

FIGURE 3.8: One Dimensional Haar Transform part 5

Two dimensional haar transform is performed by applying one dimensional haar transform on first the rows and then on the columns of the matrix. From the wavelet coefficients obtained from haar transform brightness coefficient,texture coefficient and variation coefficient are computed. Based on these three coefficients two more parameters are calculated namely sum of coefficients (σ) and the smooth judgment operator(z).

Based on σ and z the image is classified:

- The images in the first category have more even distributed textures and the background is not smooth.
- The images of the second class have uneven distributed texture and smooth background.
- If the image has little texture and dark background, it belongs to the third category.

- The fourth category has images that have particularly rich texture.

Examples for Images from the four classes:

FIGURE 3.9: Image of class 1 and class 2

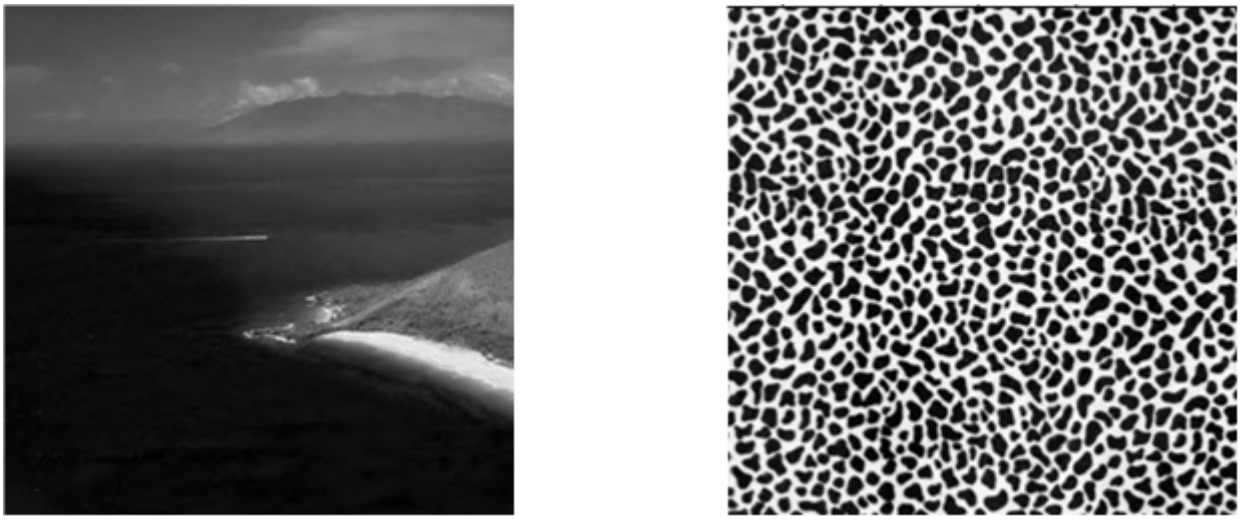

FIGURE 3.10: Image of class 3 and class 4

Iterative Fusion:

After the image is classified an iterative fusion algorithm is applied to all the images in the category to choose the optimum carrier.Then the image is fused with this optimum carrier image.

CHAPTER 4

Proposed System

For secure transmission of the information, the PSNR value must be as high as possible to decrease the noise interference during information transmission. This is achieved by fusing the stego image with a suitable carrier image which is taken under the same category as that of the stego image using image classification. Thus we make use of the existing technique LSB steganography to effectively hide the information inside a cover image, thus obtaining the stego image. To increase the PSNR value, image classification is done which selects a suitable carrier image from a suitable class to yield the fused image which is transmitted securely to the receiver side.

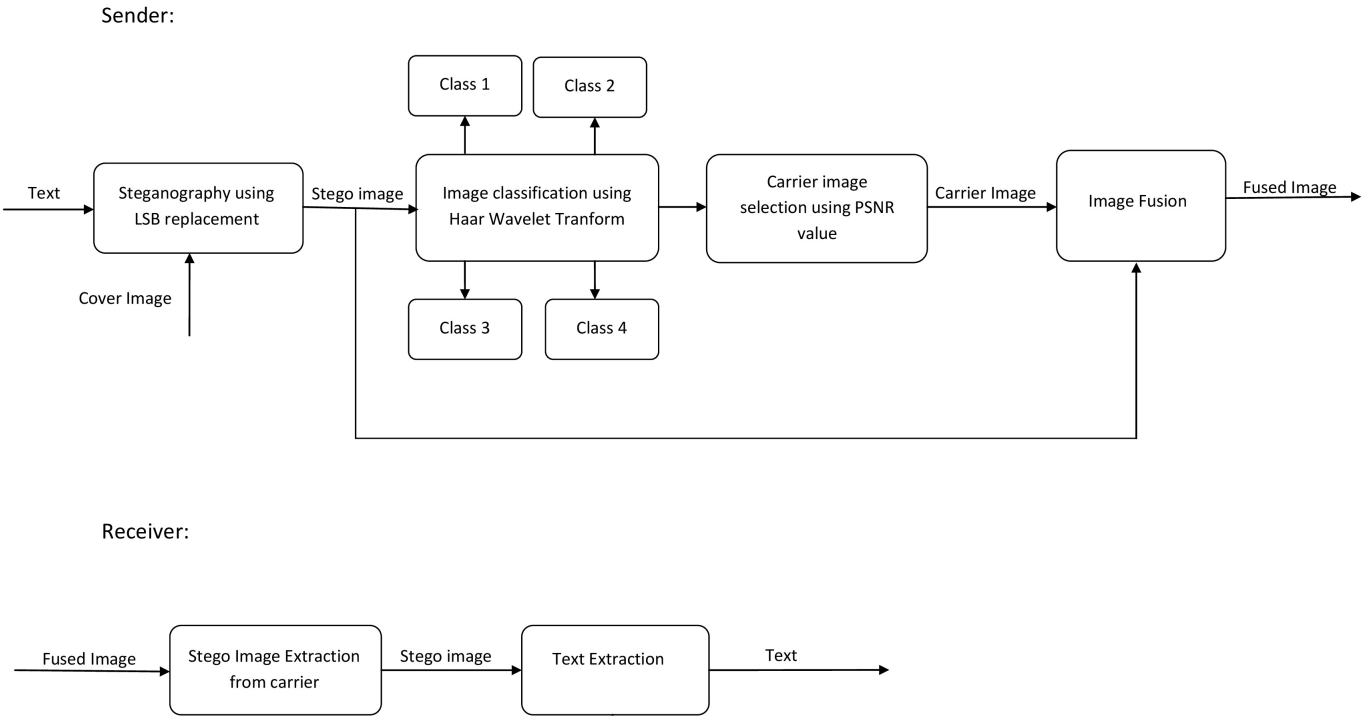

FIGURE 4.1: Architecture Diagram

Sender Side:

- In Steganography using LSB Replacement the information to be hidden and the stego key (length of text to be hidden)is encoded in the LSB pixels of the cover image to obtain the stego image.
- Now Haar transform is performed on this stego image to obtain the wavelet coefficients.
- From the wavelet coefficients the brightness, texture and variation coefficients are obtained.
- From these two more parameters called sum of coefficients (α) and smooth judgement operator (z) are obtained.
- Based on these values the stego image is classified into one of the 4 classes.
  If $4 \leq \Sigma \leq 25$, $Z < 0.5$, then I ε I_1 ;
  If $4 \leq \Sigma \leq 25$, $Z > 0.5$, then I ε I_2 ;
  If $\Sigma < 4$, then I ε I_3 ;
  If $\Sigma > 25$, then I ε I_4 ;
- After classification each image from that class is fused with the stego image with a random value for fusion parameter between 0 and 1.
- The PSNR value of the stego image and retrieved image is compared with a threshold value and accordingly the fusion parameter is adjusted.
- Now with the obtained fusion parameter the stego image is fused with all the images from the class and the image with maximum value of PSNR for fused and carrier image is designated as the optimum carrier.

- Now the stego image is fused with the optimum carrier.

Receiver Side:

- From the fused image the stego image is obtained.
- From the stego image the hidden information is retrieved by taking the LSB bits from the stego image.

CHAPTER 5

Algorithms

5.1 LSB Replacement Technique

In LSB steganography, the least significant bits of the pixels of the cover image are used to conceal the message. This technique flips the last bit of each of the pixel values to reflect the message that needs to be hidden[12]. For instance, consider an 8-bit image where each pixel is stored as a byte. Suppose the first eight pixels of the original image have the following greyscale values:

10010001

11010011

10100010

11001001

10110001

01110010

10100101

00011001

To hide the letter N whose binary value is 01001110, we would replace the LSBs of these pixels to have the following new greyscale values:

10010000

11010011

10100010

11001000

10110001

01110011

10100101

00011000

Algorithm for LSB Replacement Technique

Input: Cover Image, Secret Text

Output: Stego Image

STEP 1: Extract the pixels of the cover image.

STEP 2: Extract the characters from the input text.

STEP 3: Create a stego key which contains the length of the input text.

STEP 4: Convert the ASCII values of each character into their respective binary values.

STEP 5: Encode the contents of the stego key in the LSB position of the first pixel of the cover image.

STEP 6: Store the binary values of each character in the LSB positions of the pixels of the cover image starting from the second pixel.

STEP 7: Repeat STEP 6 for all characters of the input text.

The message embedding procedure can be illustrated as[5]:

If the LSB of the pixel value of cover image C(i,j) is equal to the message bit m of secret message to be embedded, C(i,j) remain unchanged; if not, set the LSB of C(i,j) to m.

$S(i,j) = C(i,j) - 1$, if $LSB(C(i,j)) = 1$ and $m = 0$

$S(i,j) = C(i,j)$, if $LSB(C(i,j)) = m$

$S(i,j) = C(i,j) + 1$, if $LSB(C(i,j)) = 0$ and $m = 1$

where LSB(C(i, j)) stands for the LSB of cover image C(i,j) and S(i,j) is the stego image.

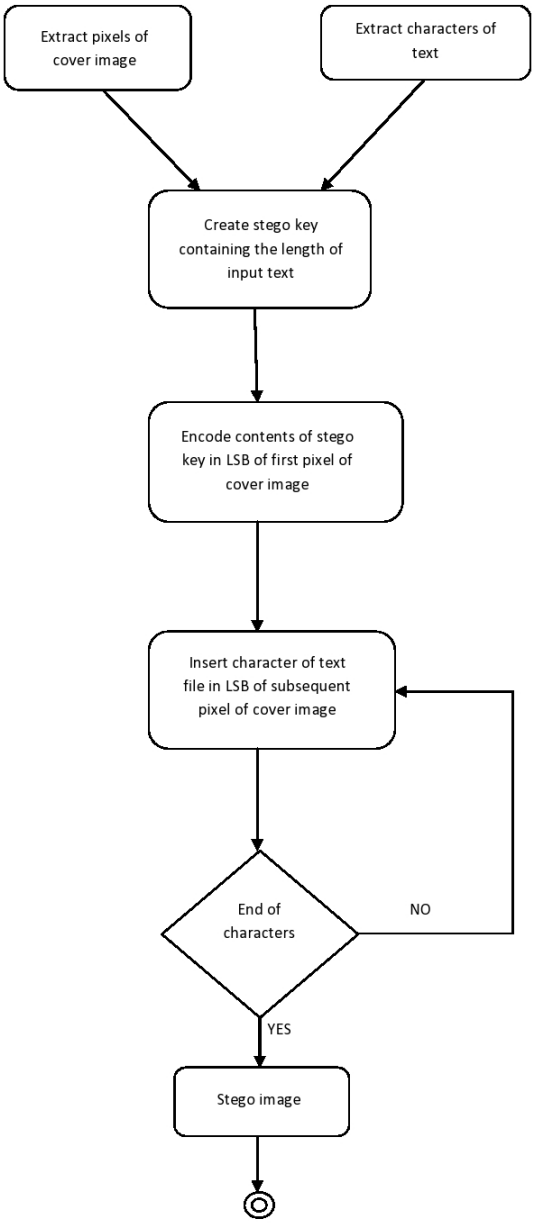

FIGURE 5.1: Steganography using LSB

Description:

The pixels of cover image and characters of input text are extracted. The stego key is created containing length of input text and is encoded in LSB of first pixel of cover image. The characters of text are encoded in the LSB of subsequent pixels till end of characters are reached. The encoded image is the stego image.

5.2 One Scale Two Dimensional Haar Wavelet Transform

2D Haar transform is done by carrying out 1D Haar transform on the rows and columns of the image matrix. This 1D process for an array of n samples is explained as [4]:

1. Find the average of each pair of samples. (n/2 averages)

2. Find the difference between each average and the sample it was calculated from. (n/2 differences)

3. Fill the first half of the array with averages.

4. Fill the second half of the array with differences.

5. Repeat the process on the first half of the array.

Algorithm for Calculating the coefficients of the Stego Image
Input: Stego Image
Output: Class number to which Stego Image belongs to

STEP 1: The stego image is compressed using 2D Haar transform.

1.1: Perform the averaging and differencing process on the entire row of the image matrix.

1.2: Now, perform the same process for the entire column of the image matrix.

1.3: Split the matrix of size M X N obtained into 4 sub matrices of size M/2 X N/2 LL(upper left), LH(upper right), HL(lower left) and HH(lower right).

STEP 2: Calculate the brightness coefficient 'bri' using the formula[10]:

$$bri = \sum_i \sum_j LL_{\frac{M}{2}\times\frac{N}{2}}(i,j)$$

STEP 3: Similarly calculate the texture coefficient 'tex' using the formula

$$tex = \sum_i \sum_j \left[\left| LH_{\frac{M}{2}\times\frac{N}{2}}(i,j) \right| + \left| HL_{\frac{M}{2}\times\frac{N}{2}}(i,j) \right| + \left| HH_{\frac{M}{2}\times\frac{N}{2}}(i,j) \right| \right]$$

STEP 4: Also calculate the variation coefficient 'var' using the formula:

$$var = \frac{var_{LH} + var_{HL} + var_{HH}}{3}$$

$$where, \quad var_{LH} = \frac{1}{\frac{M}{2}\times\frac{N}{2} - 1} \sum_i \sum_j \left(LH_{\frac{M}{2}\times\frac{N}{2}}(i,j) - \mu^{LH}_{\frac{M}{2}\times\frac{N}{2}} \right)^2$$

$$\mu^{LH}_{\frac{M}{2}\times\frac{N}{2}} = \frac{\sum_i \sum_j LH_{\frac{M}{2}\times\frac{N}{2}}(i,j)}{\frac{M}{2}\times\frac{N}{2}}$$

μ is the average value of wavelet transform coefficient LH

Similarly, we can calculate the other two coefficients HL and HH.

STEP 5: Based on the values of bri, tex and var , two more factors , namely coefficient sum 'Σ' and the smooth judgment operator 'zeta' are calculated using the formula :

$$bmax = max(elements\ in\ LL\ matrix)$$
$$tmax = max(elements\ in\ LH, HL\ and\ HH\ matrix)$$
$$vmax = max(elements\ in\ LH, HL\ and\ HH\ matrix)$$

$$\Sigma = \frac{bri}{bmax} + \frac{tex}{tmax} + 20\frac{var}{vmax}$$

$$zeta = \frac{count(elements\ in\ LH, HL\ and\ HH\ matrix\ whose\ absolute\ value < 1)}{3 \times \frac{M}{2} \times \frac{N}{2}}$$

STEP 6: According to these value, the image I is classified as belonging to a particular category.

If $4 \leq \Sigma \leq 25$, zeta < 0.5 , then I ε class 1;

If $4 \leq \Sigma \leq 25$, zeta > 0.5 , then I ε class 2;

If $\Sigma < 4$, then I ε class 3;

If $\Sigma > 25$, then I ε class 4;

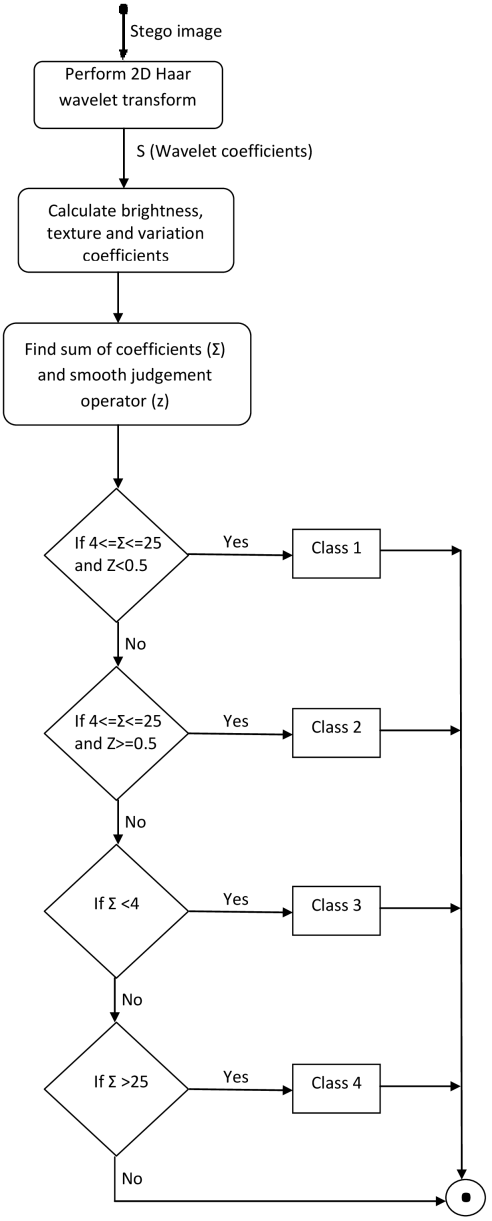

FIGURE 5.2: Haar Wavelet Transform

Description:

The brightness, texture and variation coefficients are obtained from the wavelet coefficients after performing haar transform. Based on these coefficients sum of coefficients (α) and the smooth judgement operator (z) are obtained. Based on α and z the image is classified into one of the 4 classes.

5.3 Digital Image Fusion

Algorithm for Iterative Image Fusion

Input: Stego Image, Carrier Images Dataset

Output: Fused Image

STEP 1: Classify the stego image into one of the four categories class 1, class 2, class 3, class 4.

STEP 2: Set the original parameters t, pre and α. Set t=370dB by default. 'pre' is the precision of fusion parameter, set to 0.01 by default and α is set at will in (0,1).

STEP 3: The fused image F is obtained from the carrier image C and the stego image S using the formula :

$S = \alpha F + (1 - \alpha)G \quad \alpha \in [0,1]$

STEP 4: Calculate the Mean Squared Error (MSE) value using :

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(C_{i,j} - F_{i,j}\right)^2$$

STEP 5: Obtain the Peak Signal to Noise Ratio (PSNR) using the MSE value as :

$PSNR = 20\log_{20} \frac{255}{\sqrt{MSE}}$

STEP 6: The stego image can be extracted (E) from fused image using formula :

$$E = \frac{F - \alpha C}{1 - \alpha}$$

STEP 7: To obtain the optimum fusion parameter value:

7.1:Select the carrier image in category I' one by one.

7.2:Hide image and calculate PSNR(G,G').

7.3:While(PSNR(S,E) $>$ t)

$\alpha = \alpha +$ pre ;

Based on current α , hide image and

calculate PSNR(S,E) ;

End while

7.4:While(PSNR(S,E) $<$ t)

$\alpha = \alpha -$ pre ;

Based on current α , hide image and

compute PSNR(S,E) ;

End while

STEP 8: To obtain the optimum carrier:

8.1: According to the currently determined fusion parameter α, calculate PSNR(F,C) .

8.2: Analyze the computed results; the image with maximum PSNR(F,C) is the optimal carrier image.

8.3: Hide image in accordance with the optimal carrier image by expression :

$S = \alpha F + (1 - \alpha)G \quad \alpha \in [0,1]$

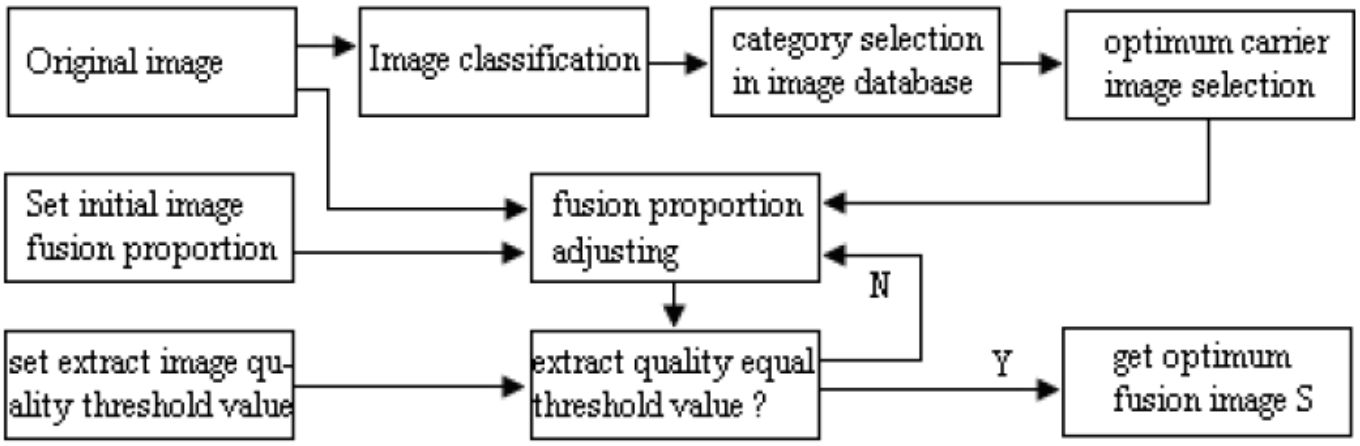

FIGURE 5.3: Digital Image Fusion (Block Diagram)

Description:

1) Here input image is the stego image. This image is classified.

2) Initial value is set for the fusion parameter and the threshold value is also set.

3) For each image in the selected category fusion parameter is adjusted by comparing with the threshold value.

4) Hence optimum carrier image is obtained.

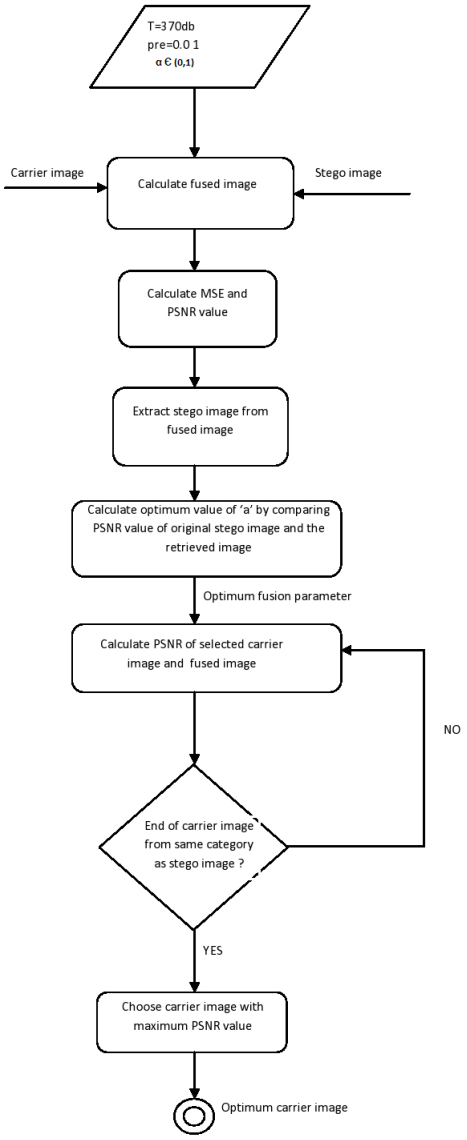

FIGURE 5.4: Digital Image Fusion

Description:

The initial parameters are set for fusion and the stego image and all the images from the selected category are fused.MSE and PSNR are calculated. Fusion parameter is adjusted by comparing PSNR value of stego image and extracted image with the threshold. Now with the obtained fusion parameter the image with the maximum PSNR of fused and carrier images is selected as optimum carrier.

CHAPTER 6

Implementation

6.1 Dataset used

The dataset consists of a set of carrier images which are classified into 4 classes. Also, each class consists of 20 images. Our dataset also contains 20 greyscale cover images in which data can be hidden.

6.2 Outcomes

Sender Side:

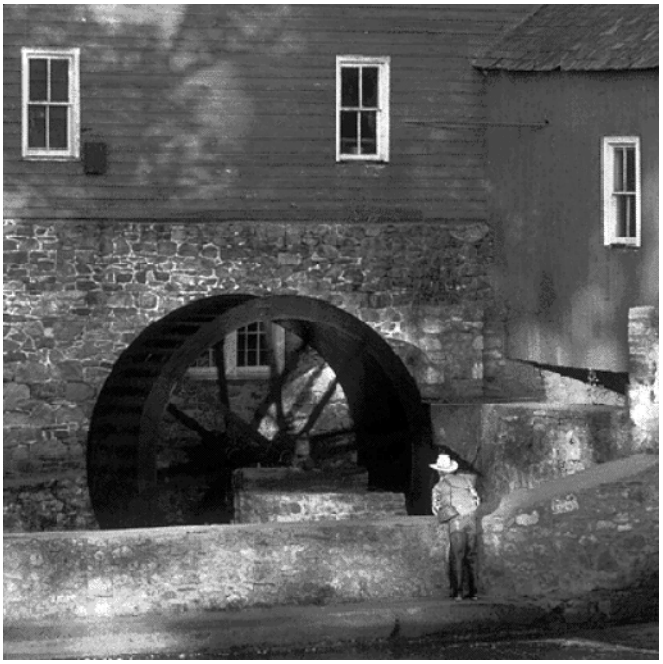

FIGURE 6.1: Cover Image

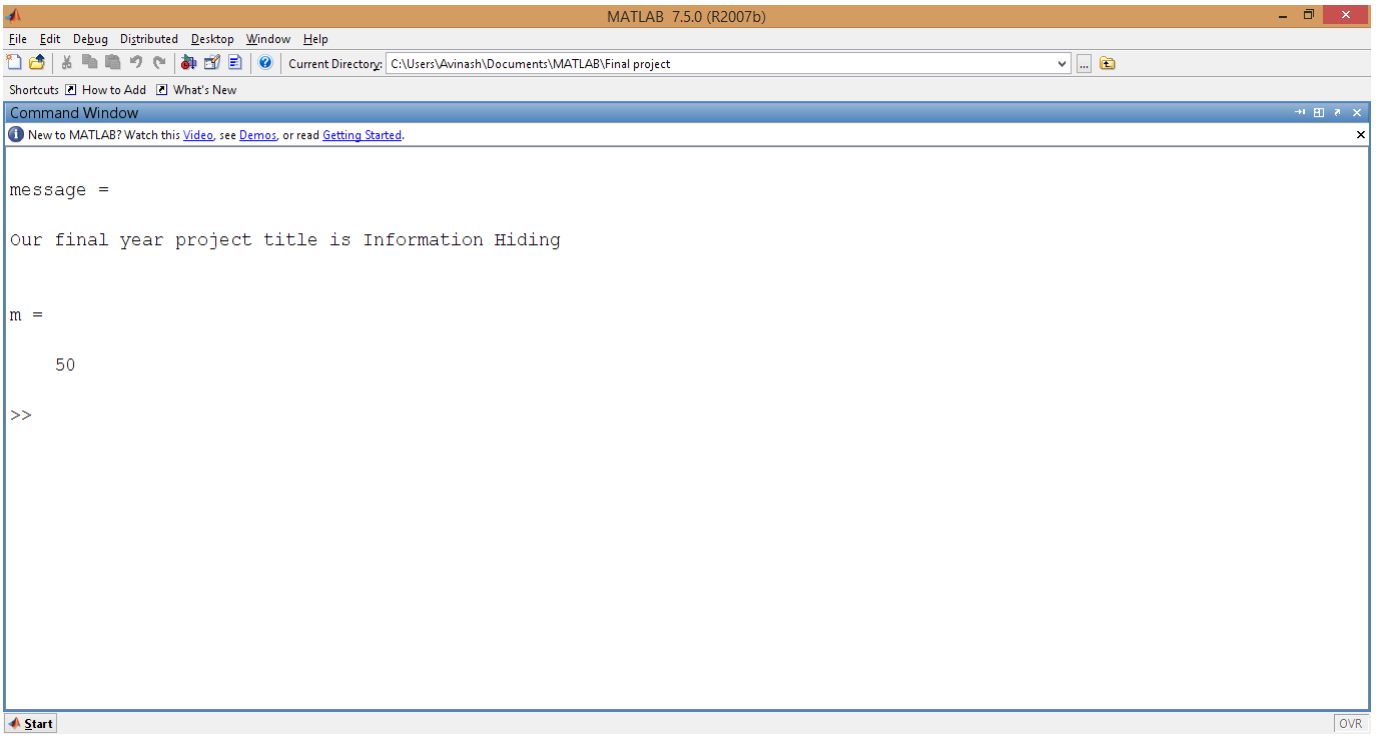

FIGURE 6.2: LSB (Sender Side) output

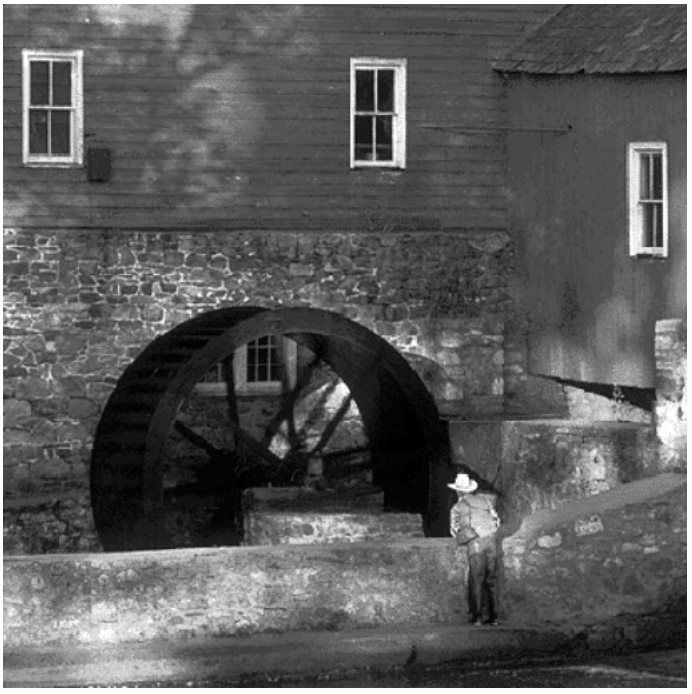

FIGURE 6.3: Stego Image

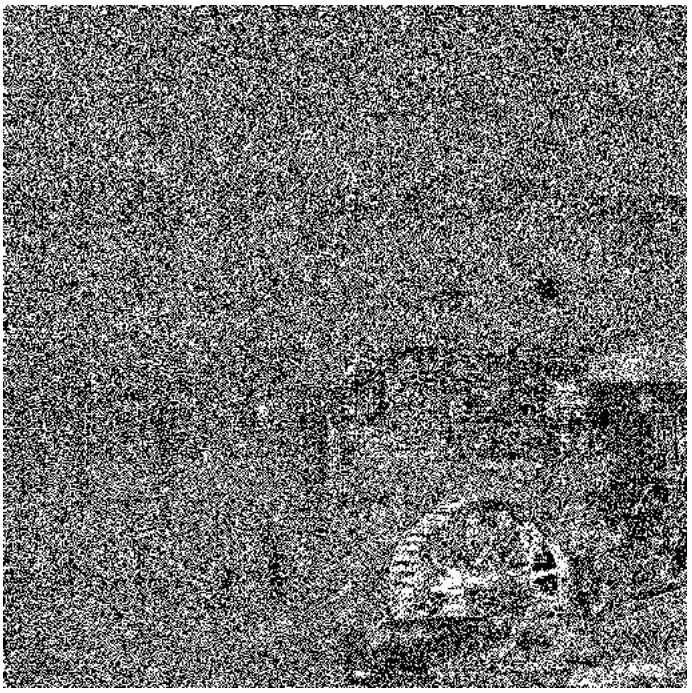

FIGURE 6.4: Haar Wavelet Transform Output

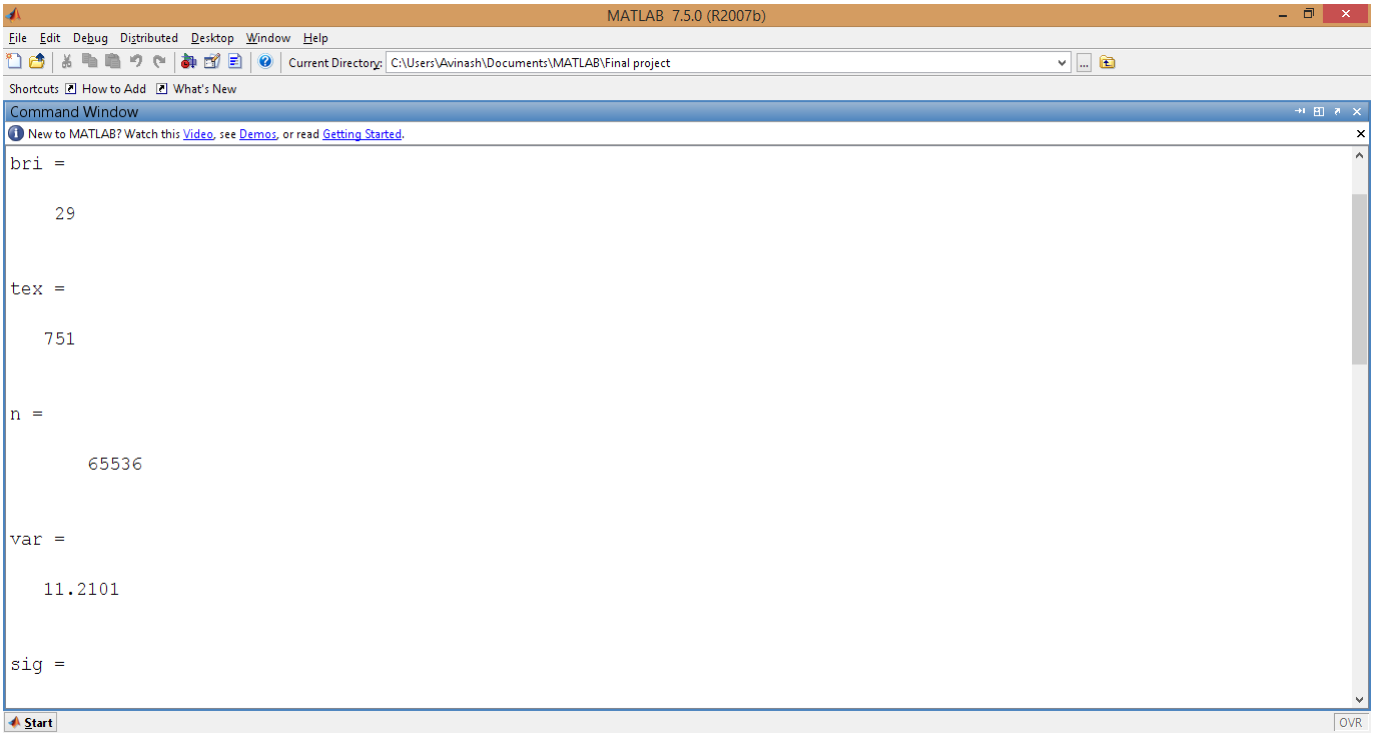

FIGURE 6.5: Haar Wavelet Coefficients output

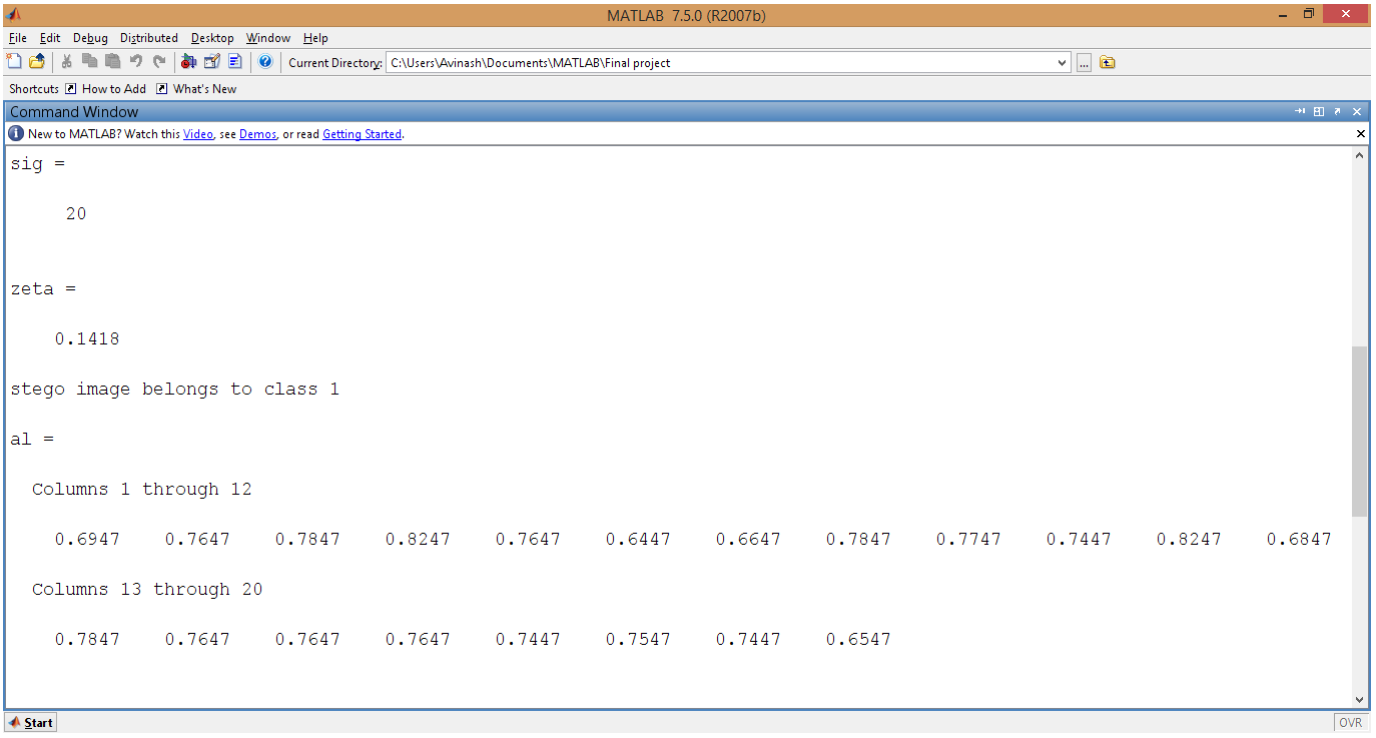

FIGURE 6.6: Image Classification output

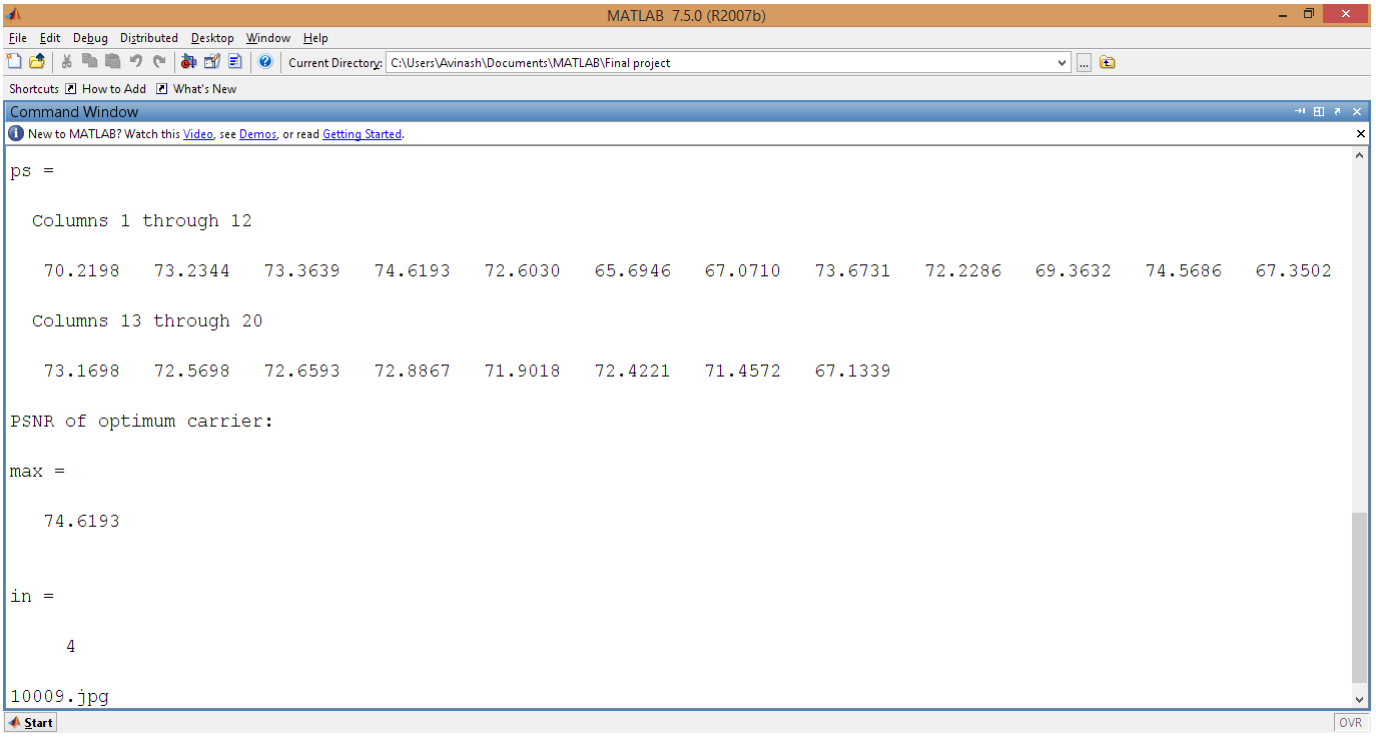

FIGURE 6.7: Image Classification output

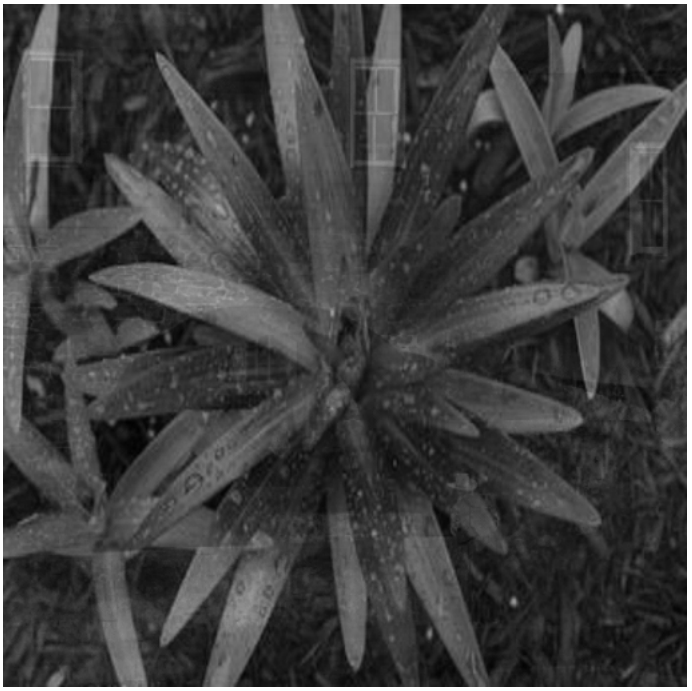

FIGURE 6.8: Fused Image

Receiver Side:

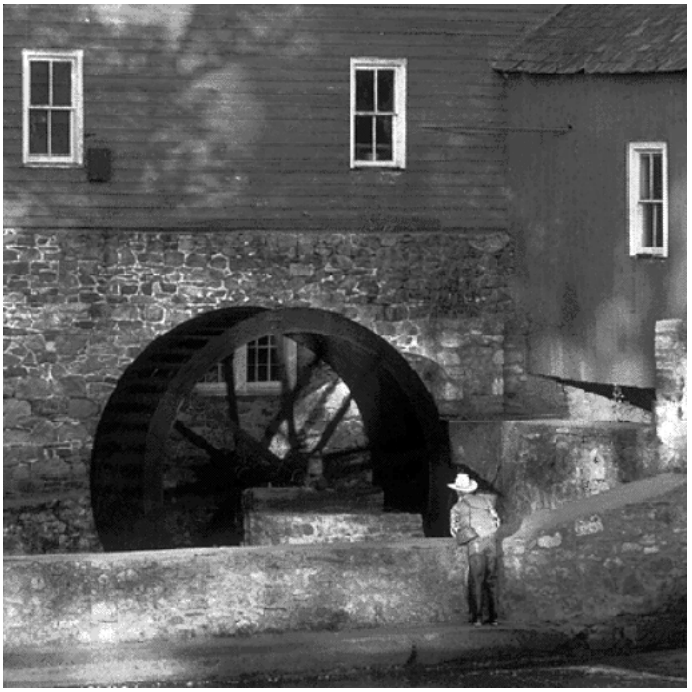

FIGURE 6.9: Retreived Image

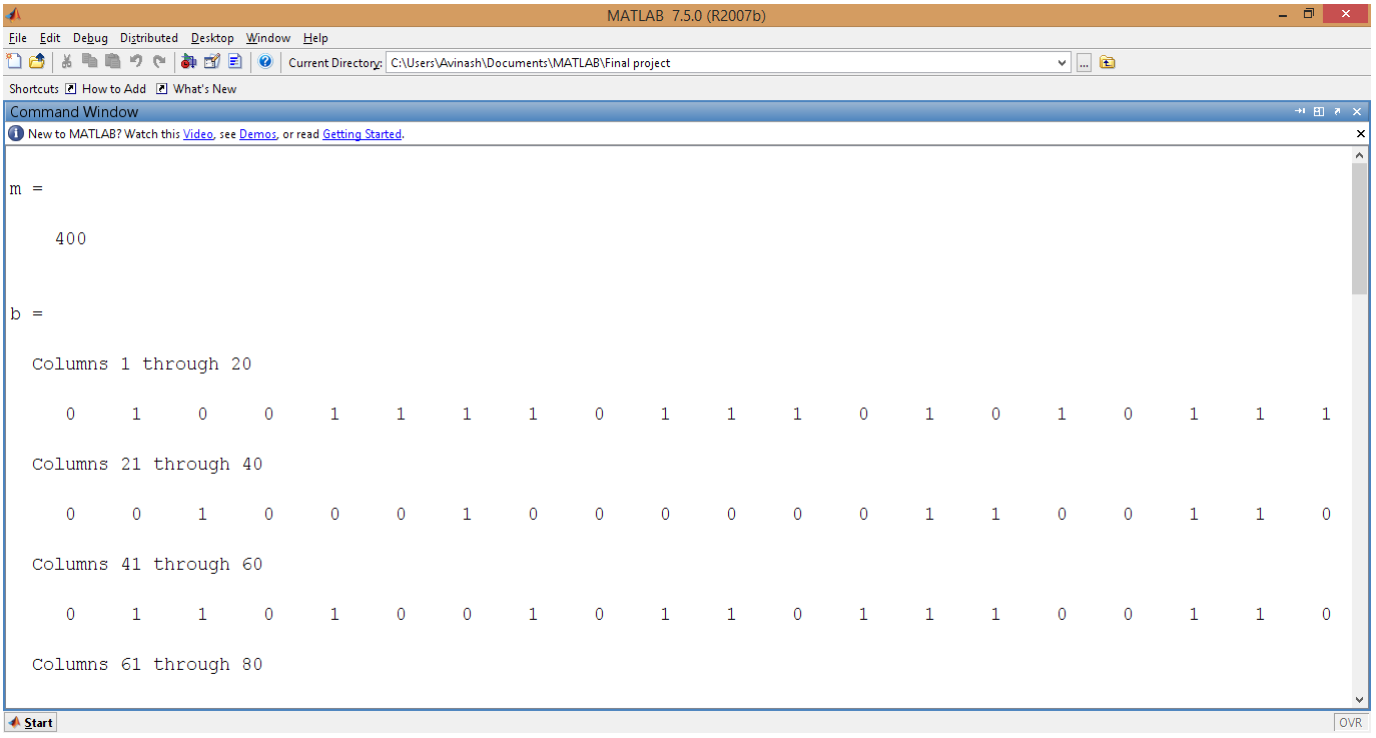

FIGURE 6.10: LSB (Receiver Side) output - bits of the recovered text

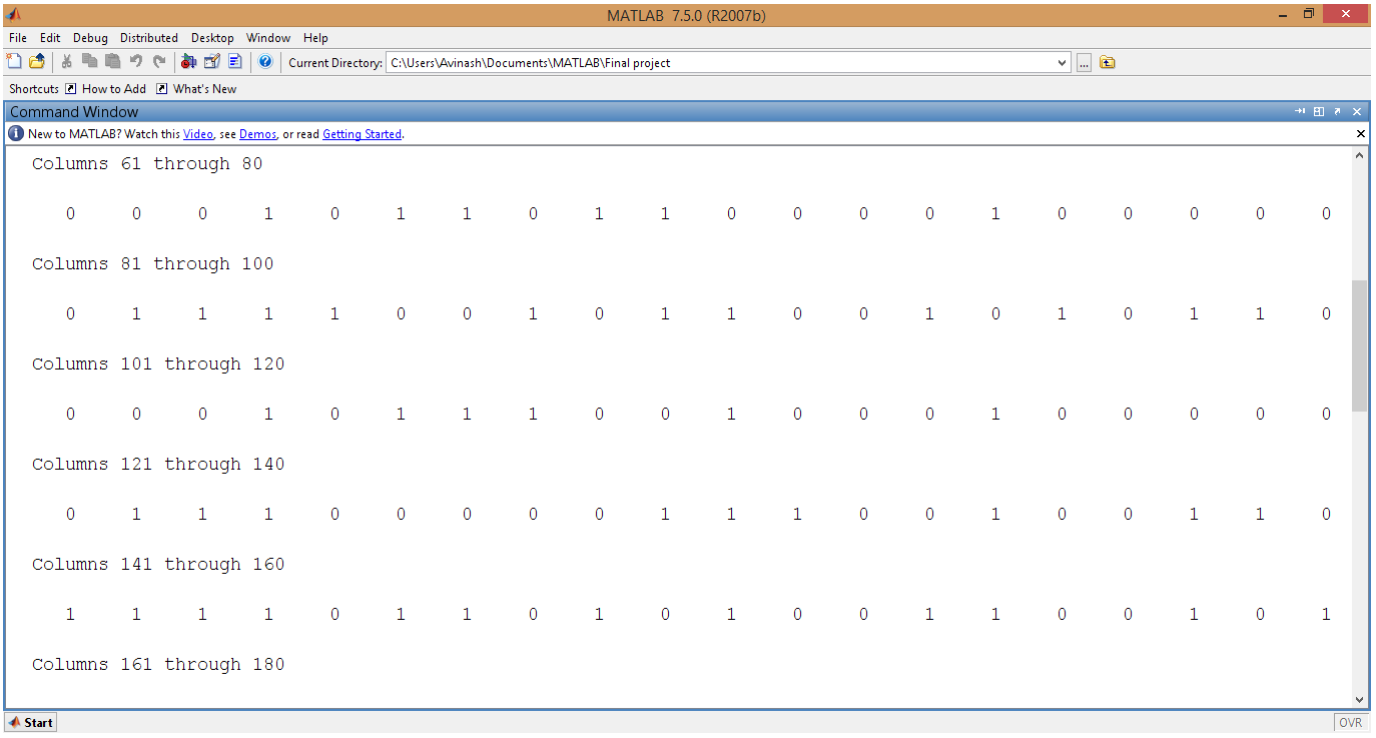

FIGURE 6.11: LSB (Receiver Side) output - bits of the recovered text

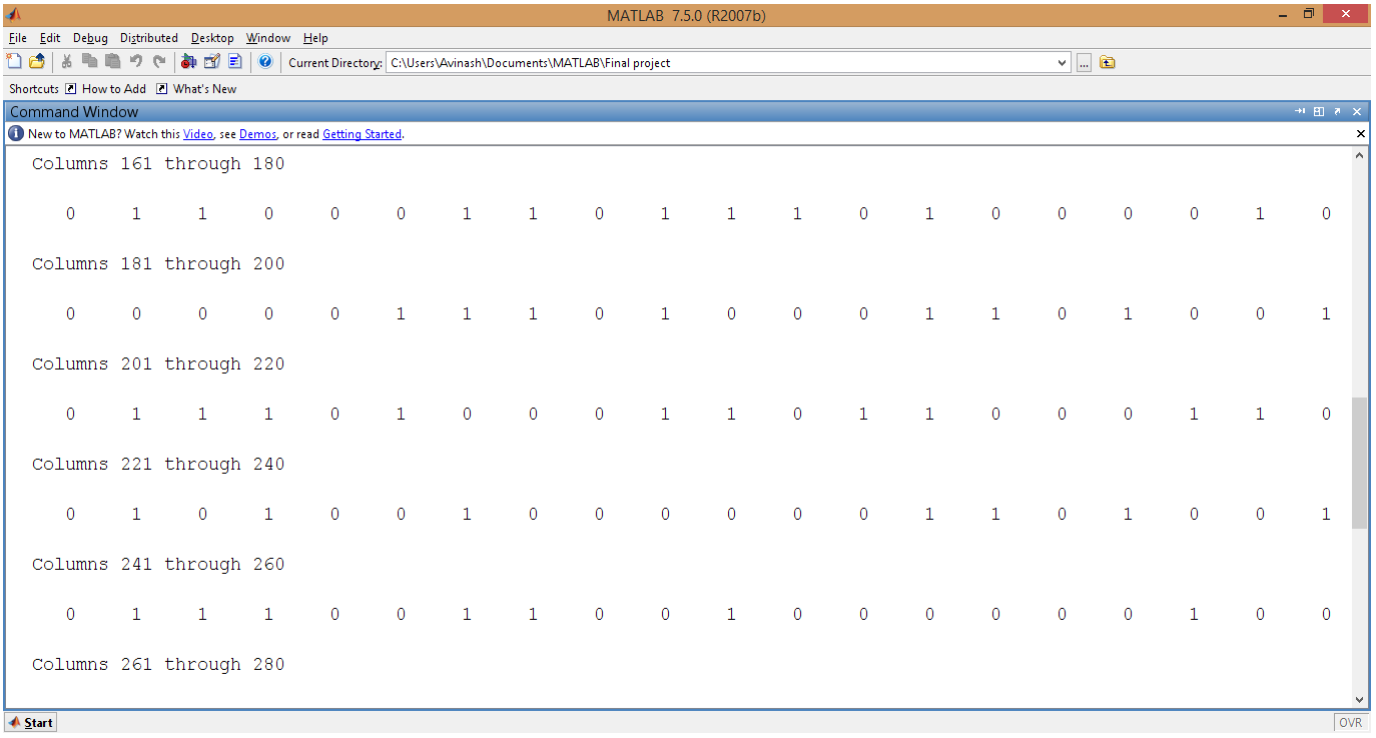

FIGURE 6.12: LSB (Receiver Side) output - bits of the recovered text

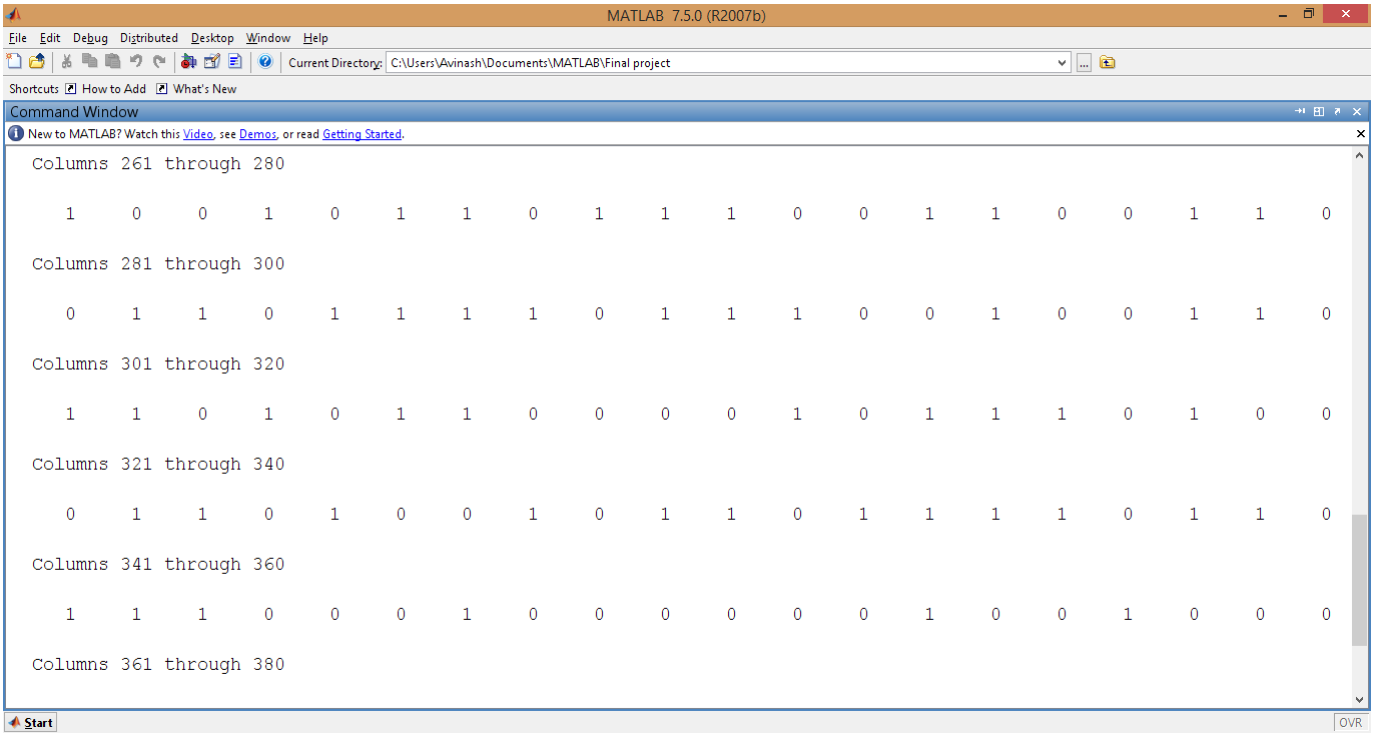

FIGURE 6.13: LSB (Receiver Side) output - bits of the recovered text

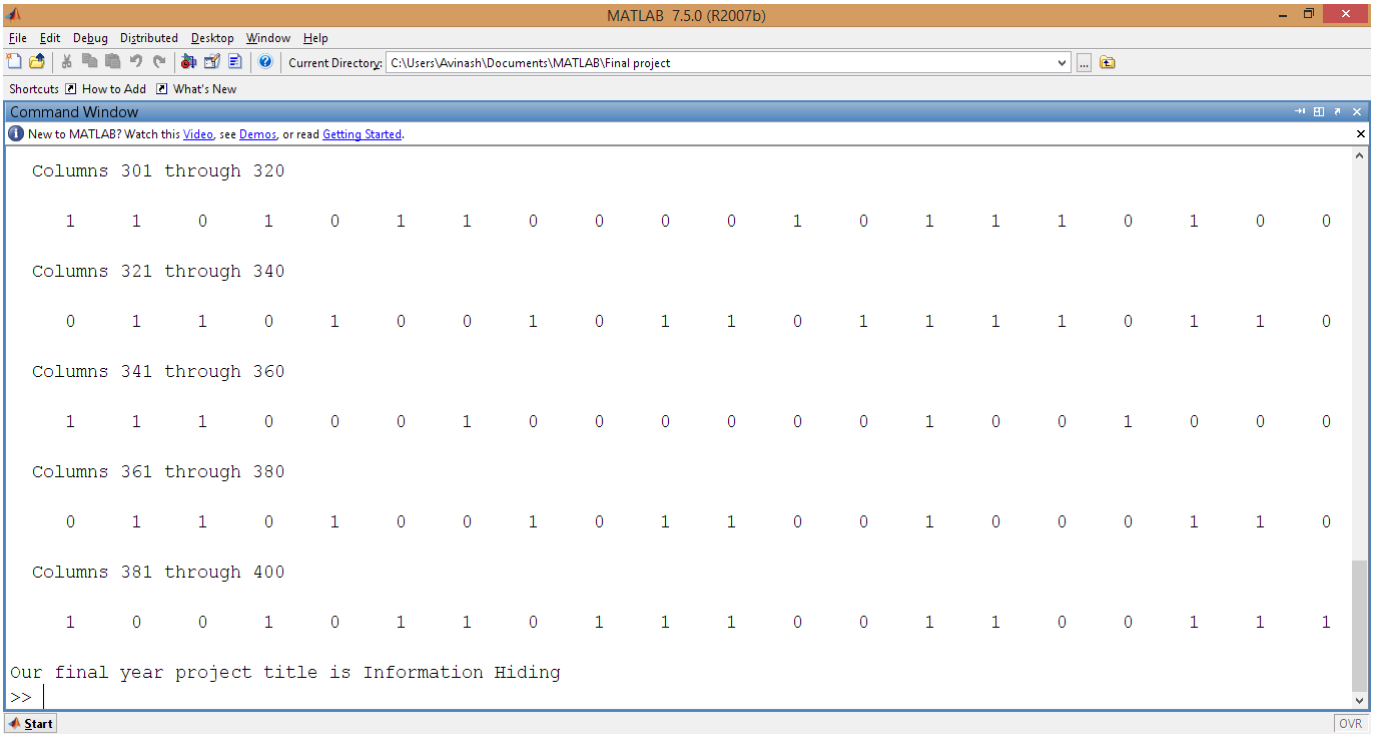

FIGURE 6.14: LSB (Receiver Side) output - bits of the recovered text

CHAPTER 7

Performance measurements

7.1 Optimum Carrier vs Random Carrier

Cover Image 1

FIGURE 7.1: Cover Image 1

Random Carrier: PSNR=71.4963

FIGURE 7.2: Random Carrier and Fused Image 1

Optimum Carrier: PSNR=78.7753

FIGURE 7.3: Optimum Carrier and Fused Image 1

Cover Image 2

FIGURE 7.4: Cover Image 2

Random Carrier: PSNR=65.7650

FIGURE 7.5: Random Carrier and Fused Image 2

Optimum Carrier: PSNR=74.2708

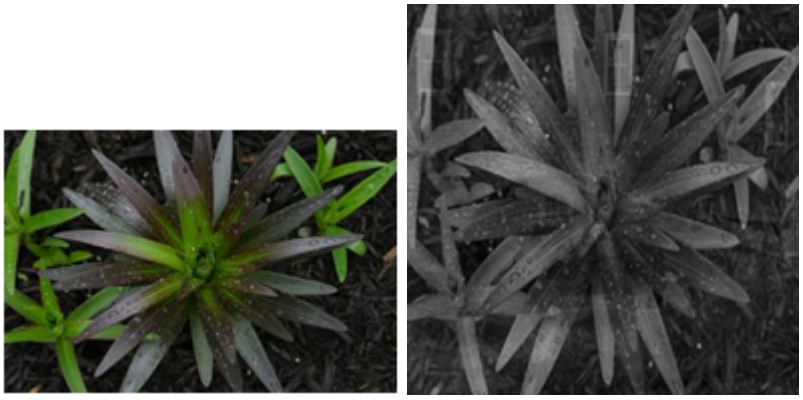

FIGURE 7.6: Optimum Carrier and Fused Image 2

Cover Image 3

FIGURE 7.7: Cover Image 3

Random Carrier: PSNR=73.8697

FIGURE 7.8: Random Carrier and Fused Image 3

Optimum Carrier: PSNR=78.7654

FIGURE 7.9: Optimum Carrier and Fused Image 3

Inference:

The above table illustrates how efficiently image fusion can be carried out when an optimum carrier is chosen based on its maximum PSNR value. When the stego image is hidden using an optimum carrier it is hardly noticeable to the intruder whereas in the case of a random carrier image the presence of stego image is easily visible. Also for a random carrier image the psnr value is less.

7.2 Change in PSNR values for the Carrier Image and Fused Image

After finding the PSNR values for a sample of 20 Test Images, the average value found for the PNSR(Cover Image, Stego Image) is 57.75 and the average for PNSR(Cover Image, Fused Image) is 76.81. Thus we can conclude that the PSNR value of Stego image increases after fusion. Below is a table which shows PNSR values for 5 sample images.

Cover Image	PSNR(Cover Image, Stego Image)	PSNR(Cover Image, Fused Image)
Image 1	59.54	80.10
Image 2	58.71	74.82
Image 3	58.63	78.14
Image 4	57.71	76.78
Image 5	60.02	76.13

TABLE 7.1: PSNR values for a sample of test Images

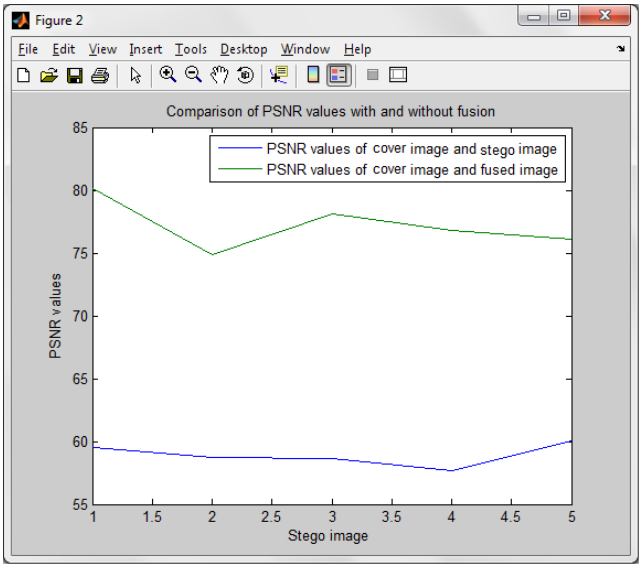

FIGURE 7.10: Graph of PSNR values for carrier image and fused image

Inference:

By comparing the values of PSNR(cover image, carrier image) and PSNR(cover image, fused image), the ratio value is higher when we fuse the cover image with a suitable optimum carrier image than by simply hiding the text inside the cover image to obtain the stego image. So, information can also be sent securely with relatively lesser interference of noise.

7.3 Lengths of Input Text vs PSNR value

Text Length	PSNR value
50	71.4761
100	71.1895
150	71.2244
200	70.9515

TABLE 7.2: Varying PSNR values for different lengths of the input text which is hidden

Inference:

Thus from the above table, we can infer that there is a very small appreciable difference in the PSNR values when the length of the information to be sent is varied . This is because the value does not depend on the length of the input text but the bits that match with the pixel bits of the cover image. If the bits of the cover image and the text are the same, then there is no change in the bit value. Else, there is a change.

7.4 Other Test Images:

Image 1 and It's Fused image

FIGURE 7.11: Image 1 and It's Fused Image

Image 2 and It's Fused image

FIGURE 7.12: Image 2 and It's Fused Image

Image 3 and It's Fused image

FIGURE 7.13: Image 3 and It's Fused Image

Image 4 and It's Fused image

FIGURE 7.14: Image 4 and It's Fused Image

Image 5 and It's Fused image

FIGURE 7.15: Image 5 and It's Fused Image

CHAPTER 8

Conclusion and Future work

In this a data hiding method by improved LSB substitution and image classification is proposed. The image quality of the stego-image can be greatly improved with low extra computational complexity by fusing it with an optimal carrier. Experimental results show the effectiveness of the proposed method. The results obtained also show significant improvement in PSNR value when the stego image is fused with another image. The algorithm proposed in the current work describes a method such that the stego image which is obtained thereby cannot be proved as stego image using the steganalysis approach. In the proposed algorithm, the computational complexity is reduced. Benefited from the effective optimization, a good balance between the security and the image quality is achieved. Also image extraction is easier owing to the fact that PSNR value is increased.

Our future work will focus on improving the efficiency of the proposed algorithm. Now we are able to hide upto 255 characters in the cover image to obtain the stego image. For future work we can make sure that we increase the capability (length) of the stego key so that more number of characters can be effectively hidden.

REFERENCES

1. Amanpreet Kaur, Renu Dhir, and Geeta Sikka(2009),'A New Image Steganography Based On First Component Alteration Technique', International Journal of Computer Science and Information Security,Vol.6, No.3, pp. 53-56

2. C.P.Sumathi, T.Santanam and G.Umamaheswari(2013),'A Study of Various Steganographic Techniques Used for Information Hiding', International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.6, pp. 11

3. Jun Zhang,Yuping Hu and ZhibinYuan(2009),'Detection of LSB Matching Steganography using the Envelope of Histogram', JOURNAL OF COMPUTERS, VOL. 4, NO. 7, pp. 646-648

4. Kamrul Hasan Talukder and Koichi Harada(2007), 'Haar Wavelet Based Approach for Image Compression and Quality Assessment of Compressed Image', IAENG International Journal of Applied Mathematics, 36:1, IJAM_36_1_9, pp. 1-8

5. Kshetrimayum Jenita Devi(2013), 'A Secure Image Steganography Using LSB Technique and Pseudo Random Encoding Technique' pp. 1-19

6. Li, J. Photography image http://www.stat.psu.edu/ jiali/index.download.html. 52 database [EB/OL].53

7. Masoud Nosrati, Masoud Nosrati, Mehdi Hariri(2011),' An introduction to steganography methods', World Applied Programming, Vol (1), No (3), pp. 191-195

8. Min Li,Ting Liang,Yu-jie He(2013),'Arnold Transform Based Image Scrambling Method', International Conference on Multimedia Technology, pp. 1309-1310

9. S.S. Tamboli1, Dr. V. R. Udupi(2013),'Image Compression Using Haar Wavelet Transform',International Journal of Advanced Research in Computer and Communication Engineering Vol.2, Issue 8, pp. 3166-3169

10. Shengbing Che, Qiangbo Huang, Bin Ma(2008),' Adaptive Image Hiding Algorithm Based on Classifiaction', International Conference on Intelligent System Design and Applications,DOI 10.1109/ISDA, pp. 314-319

11. Shengbing CHENG, Da HUANG, Guang LI(2007),'Semifragile Image Watermarking Based on Visual Features, Journal on Communication', Vol 28,No.10, pp.134-140.

12. Vijay Kumar Sharma, Vishal Shrivasava(2012),' A Steganography Algorithm For Hiding Image in Image By Improved LSB Substitution By Minimize Detection', Journal of Theoretical and Applied Information Technology, 36 No, pp. 1-7