Steganography in Medical Imaging: Comparative Analysis and FFT-Based Algorithm Enhancement

A project report submitted

to

MANIPAL ACADEMY OF HIGHER EDUCATION

For Partial Fulfillment of the Requirement for the

Award of the Degree

of

Bachelor of Technology

in

Information Technology

by

Saurav Kumar

Reg. No. 200911254

Under the guidance of

Dr. Raviraja Holla M
Assistant Professor - Senior Scale
Department of I & CT
Manipal Institute of Technology
Manipal, India

MANIPAL INSTITUTE OF TECHNOLOGY
MANIPAL
(A constituent unit of MAHE, Manipal)

July 2024

I dedicate my thesis to my friends and family.

DECLARATION

I hereby declare that this project work entitled **Steganography in Medical Imaging: Comparative Analysis and FFT-Based Algorithm Enhancement** is original and has been carried out by me in the Department of Information and Communication Technology of Manipal Institute of Technology, Manipal, under the guidance of **Dr. Raviraja Holla M**, **Assistant Professor - Senior Scale**, Department of Information and Communication Technology, M. I. T., Manipal. No part of this work has been submitted for the award of a degree or diploma either to this University or to any other Universities.

Place: Manipal

Date :03-07-24

Name

Saurav Kumar

MANIPAL INSTITUTE OF TECHNOLOGY
MANIPAL
(A constituent unit of MAHE, Manipal)

CERTIFICATE

This is to certify that this project entitled **Steganography in Medical Imaging: Comparative Analysis and FFT-Based Algorithm Enhancement** is a bonafide project work done by **Mr. Saurav Kumar (Reg.No.:200911254)** at Manipal Institute of Technology, Manipal, independently under my guidance and supervision for the award of the Degree of Bachelor of Technology in Information Technology.

For report

Dr.Raviraja Holla M	Dr.Smitha N Pai
Assistant Professor - Senior Scale	Professor & Head
Department of I & CT	Department of I & CT
Manipal Institute of Technology	Manipal Institute of Technology
Manipal, India	Manipal, India

ACKNOWLEDGEMENTS

I would like to express my heartfelt gratitude to all these individuals for mentoring and supporting me in completing the project **Steganography in Medical Imaging: Comparative Analysis and FFT-Based Algorithm Enhancement**.

My guide and mentor **Dr. Raviraja Holla M**, for providing me with invaluable insights, knowledge, and direction for the project.

Our esteemed **HOD Dr. Smitha N Pai** for fostering an environment of learning and creativity within our department. Special thanks to **Dr. Manjula C Belagavi** for her coordination and administrative support.

To my parents and my friends, their constant encouragement, support, and understanding have been the pillars of my successful completion of this project.

Thank you everyone for shaping this project and enhancing my learning experience.

ABSTRACT

In the world of medical image security, the need for secure and robust techniques for protection of sensitive data such as laryngeal images has become increasingly important . This project focusses on the application of steganography, specifically focusing on methods to conceal laryngeal images within other images. Four main steganographic techniques , Least Significant Bit (LSB) embedding, Discrete Cosine Transform (DCT), Edge based embedding, and Fast Fourier Transform (FFT were evaluated for their effectiveness in hiding text data inside images. Building upon this foundation , the study progresses to assess their efficacy in concealing laryngeal images within another image.

The evaluation metrics used are Peak Signal to Noise Ratio (PSNR) , Structural Similarity Index (SSIM) , and some steganalysis techniques to assess both the stego pictures' security and visual quality. Based on the evaluation criteria, FFT proved to be the most effective algorithm among the strategies studied for hiding laryngeal pictures within images.

Keywords: Steganography, Medical Image Security, Laryngeal Images, Fast Fourier Transform (FFT), Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSIM), Steganalysis

Contents

List of Tables

List of Figures

ABBREVIATIONS

LSB :	Least Significant Bit
DCT :	Discrete Cosine transform
FFT :	Fast Fourier transform
PSNR :	Peak Signal to Noise Ratio
SSIM :	Structural Similarity Index
JPEG :	Joint Photographic Experts Group
PNG :	Portable Network Graphics
RS Analysis :	Regular-Singular Analysis

NOTATIONS

O_i	:	Observed frequency in Chi-Square test
E_i	:	Expected frequency in Chi-Square test
χ^2	:	Chi-Square statistic
μ_x, μ_y	:	Mean values of images x and y
σ_x, σ_y	:	Standard deviations of images x and y
σ_{xy}	:	Covariance between images x and y
$C1, C2$	:	Constants for SSIM calculation

Chapter 1

Introduction

1.1 Introduction

This chapter gives an overview of the project, which is focussed on analyzing and evaluating steganographic methods for safely and securely embedding data into medical image, specifically , laryngeal images. The critical nature of medical data and the growing need of secure transmission and storage makes the topic of medical image security crucial.

1.1.1 Area of Work

The study's main objective is to look into various steganographic techniques for information hiding. Hiding text inside laryngeal images and laryngeal images inside another cover image are involved in this. Three different methods are used in this project : the Fast Fourier Transform, the Discrete Cosine Transform, and the Least Significant Bit embedding. Using predetermined criteria , the effectiveness of various methods in guaranteeing the security and integrity of the embedded data is evaluated.

1.1.1.1 Motivation

This initiative is driven by the urgent need to safeguard medical images against alteration and illegal access. When it comes to offering strong security for medical data—especially photos that could be used for diagnosis—current approaches frequently fall short. By using steganographic techniques to address these issues , patient privacy and healthcare data security can be greatly improved. While many of the solutions used in previous research work have limits regarding data capacity and security , this is still an essential topic for improvement.

1.1.1.2 Objectives

The main objectives of this project are:

- Compare and Evaluate steganography techniques like LSB, DCT and FFT for embedding text inside laryngeal images and laryngeal images in other cover images.
- Use standard metrics such as Structural Similarity Index (SSIM), the Peak Signal to Noise Ratio (PSNR), and histogram plots to find the efficiency of the strategies and the statistical differences..
- Utilize steganalysis to verify the detection capability, robustness and security against attacks..
- Investigate the probable application and limitations of steganography in medical field context.

The final result is significant because it has the potential to offer a reliable technique for the safe transfer and storage of private medical photographs, strengthening the security framework in healthcare environments as a whole

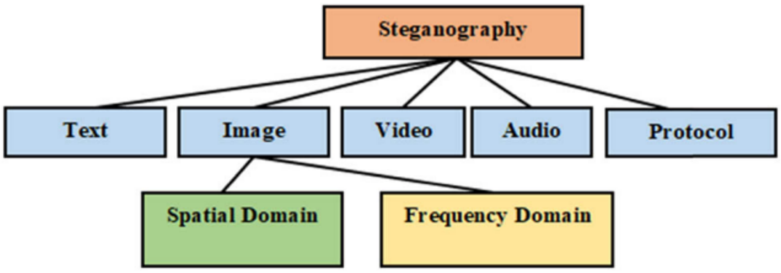


Figure 1.1: Conceptual Diagram of Embedding Information within Laryngeal Images and Laryngeal Images within Cover Images

Chapter 2

Literature Survey

The art of steganography, or hiding data in other media, is a rapidly developing topic that has attracted attention from a variety of industries, including the transmission and preservation of medical data. Data hiding in laryngeal pictures is one of the least investigated areas in this field. Laryngeal image have great medical utility and are essential for detecting and tracking disorders affecting the voice box. This study [1] established a novel method called Integer Wavelet Transformation Technique (IWT), which combines steganography and image compression to conceal data in medical photos. To meet this end IWT generates numbers that are integers thus reducing the space occupied by memory leading to better quality of hidden information. This kind of method allows for effective transmission and saving of many pictures even when network capacity is quite limited; besides, it has been done by means of C-language that will enable real-time working. PSNR as well calculations dealing with duration for different figures treated during IWT process have been calculated.

Finding a balance between robustness and quality alteration is very important when it comes to medical images. In this study [2] the usage of Image steganography for hiding text labels inside medical images where it cannot be accessed by unauthorized users. It involves removing text from its template by matching patterns, separating it from surrounding text processing and putting it back into images in the form of pixels' average brightness i.e., mean value so that very slight modifications will occur. Its key idea is insertion capacity versus noise immunity tradeoff that lets in much information while making any alteration inconspicuous enough for a person while assessing the credibility of an image used for the official documentation.

The work in [3] introduces a novel, safe method of MRI image concealing using the Arnold transform and integer wavelet transform (IWT). The resistance, visual quality, and image handling capacity of the encrypted version of the patient's diagnosis image are enhanced when a healthy image serves as the container, beyond the capabilities of other techniques. On the contrary, even with their enlargement, they seem better than others. Later on, this kind of application may also be useful for banking needs.

A higher level of security can be reached by merging steganography and encryption. Medical images are encrypted in the paper [4] using a one-time pad encryption algorithm , and then the LSB technique is used to embed the encrypted images into cover images. In terms of MSE and PSNR values, this multi-layer secure technique outperforms steganography alone in improving secrecy and integrity. Stego photos will be transformed into QR codes in the future for further authentication.

Cryptography and Steganography are combined again in [5]. This work explores the topic of embedding hidden data in a wide range of frequency bands., which led to less image degradation in higher frequency channels . Results favor rectangular strips over circular strips for embedding, showing increase in image quality measured by PSNR. The study emphasizes balancing hidden data and image quality , recommending higher frequency bands and rectangular shapes for better performance.

This paper [6] provides an advanced medical image steganography algorithm to securely embed patient's confidential data. Using integer wavelet technique and encryption with Arithmetic coding and DES , the algorithm achieves greater level of confidentiality and embedding space. Evaluation metrics confirm better performance , which in turn allows for higher level of data embedding with minimal distortion on image quality , enhancing patient data security in healthcare.

In this paper [7], we compare LSB-based with DCT-based steganography methods by looking at two distinct areas - spatial domain and transform domain. In LSB, text hiding is done using those bits of an image that are least significant, and this poses challenges when images are changed into different formats. The DCT method hides texts within direct current (DC) coefficients meaning more image details will be retained even though the method can hold less data. PSNR analysis shows that use of DCT is much less distorted for any given quality level than employing methods based on LSB.

This paper [8] suggests a strong DCT-based watermarking system to preserve intellectual property rights against JPEG compression and noise assaults, which conceals watermarks in mid-frequency DCT blocks by using low-frequency components and a secret key for their incorporation: its endurance is verified through performance analysis as it makes use of the properties of DCT technique so that it can handle block artefacts common in block-based approaches.

For secure communication, striking a balance between imperceptibility, robustness, and high capacity is crucial. This paper [9] employs FFT domain frequency entropy, in contrast to traditional techniques that conceal data in the least important portions of the image, to provide both robustness and high information capacity. Security is improved in frequency domain encryption with a randomized key vector. The experimental results demonstrate higher bits per pixel and an enhanced signal-to-noise ratio compared to previous results.

The techniques for embedding and detecting secret information in digital photos are described in this article [10] as image steganography and steganalysis.It covers key concepts, background information, and a comparison of steganography versus watermarking. Methods for recognizing and encoding communications are looked at, along with the tools available. Strong steganalysis techniques are necessary for digital forensics and security, as demonstrated by the potential for unauthorized use of steganography tools.

Chapter 3

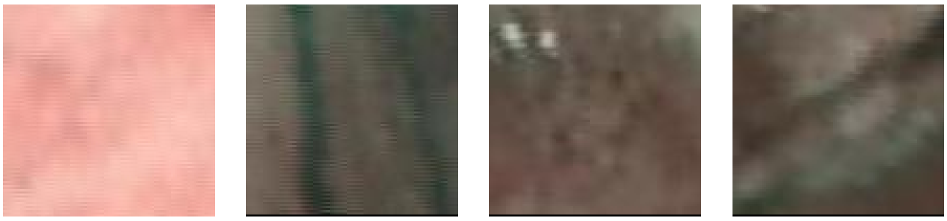
Dataset and Tools

3.1 Dataset

The dataset that was used in this project was sourced from zenodo and is labeled as **”Laryngeal dataset”**. It has images of 1320 patches , each of dimensions 100 x 100 pixels, of both healthy and early stage laryngeal tissues with the presence of cancer. These patches were extracted manually from 33 narrow band laryngoscopic images from 33 different patients diagnosed with laryngeal squamous cell carcinoma following histopathological examination.

Specifically, four tissue classes were considered (330 patches/tissue class):

- He (healthy tissue)
- Hbv (tissue with hypertrophic vessels)
- Le (tissue with leukoplakia)
- IPCL (tissue with intrapapillary capillary loops)



(a) He (b) Hbv (c) Le (d) IPCL

Figure 3.1: Sample images from the dataset.

The dataset was developed to evaluate the method proposed in [11]. The folder of the dataset includes three subfolders (fold1 1, fold2, fold 3), which are utilized for cross validation in tissue classification performance assessment. Within each subfolder are four folders corresponding to the four tissue classes: Le, He, Hbv, and IPCL.

3.2 Tools Used

Python and Matlab were used as the major programming language. Python is used for implementing the spatial domain techniques namely LSB and Edge Based Variation of LSB and Matlab was used for implementing transform domain tenchniques.

- **Python** : Primary choice for embedding steganographic algorithms in spatial domain through LSB and edge based modification of LSB technique , data preprocessing and analysis.
- **Matlab** : Preferred for embedding steganography algorithms in transform domain through DCT, FFT; also used for basic image manipulation and results visualisation.
- **NumPy**: Library for python used to support large array with numerical operations effectively. .
- **OpenCV** : Tool kit in python mainly for solving problems related to image processing.
- **scikit image**: Library in python mainly focused on solving issues during image processing operations.
- **Matplotlib**: Tool used in python programming language mainly applied on visualisation of data as well as plots..
- **Pandas** : python library used for data manipulation and for analysis.
- **TeXStudio/LaTeX** : Mainly employed to document and write the project report.

Chapter 4

Methodology

4.1 Algorithms

4.1.1 Least Significant Bit (LSB) Embedding

Description: The LSB method works by concealing data in an image's least significant bits (LSBs). This method is widely used due to its simplicity and ease of application.

Methodology:

1. **Change the secret text/image and the cover image into binary form**:
   - **Cover image** : RGB values represents each individual pixel present in the cover image. Each RGB pixle has to be changed to binary equivalent , where the red, green and blue color channels are each represented by eight bits.
   - **Secret text/image** : Use ASCII or Unicode encoding to change each character in text into its binary representation.For images translate each pixel value into its binary representation (e.g., 8-bit, 24-bit) according to the color depth..
2. **Incorporate the hidden text/image within the cover image's LSBs** :
   - Continue this process for every pixel in the cover image.
   - Pick the bits from the secret text/image data to replace the RGB values least significant bits for each pixel.This process is responsible for the changes the visual appearance of the cover image while inserting the hidden data.
   - Make careful replacement of the LSB to minimize discernible change in the appearance of the stego image.
3. **Reconstruct the modified image** :

- After inserting the secret data, reconstruct the modified pixel values into a new image .
- The resulting image is known as stego image , which resembles the cover image but contains hidden informatio embedded within the least significant bits of its pixels.

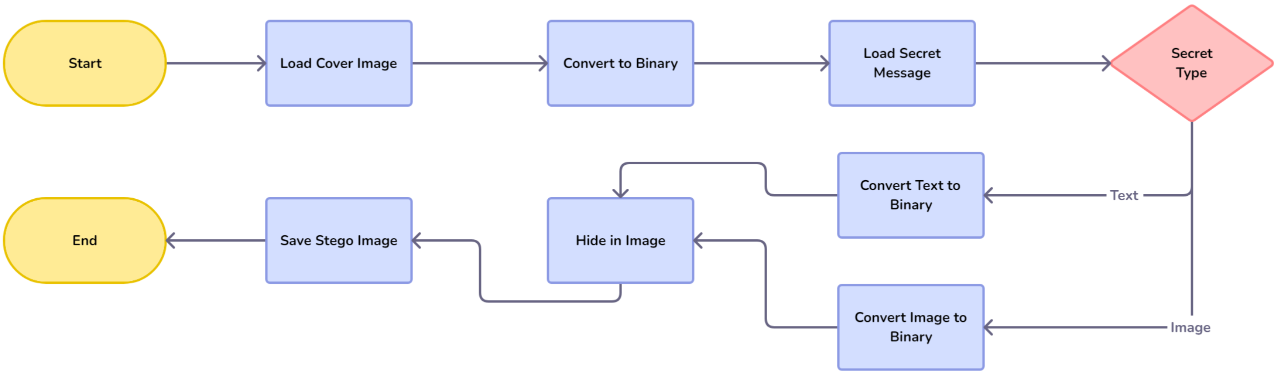


Figure 4.1: Flowchart depicting the LSB embedding methodology.

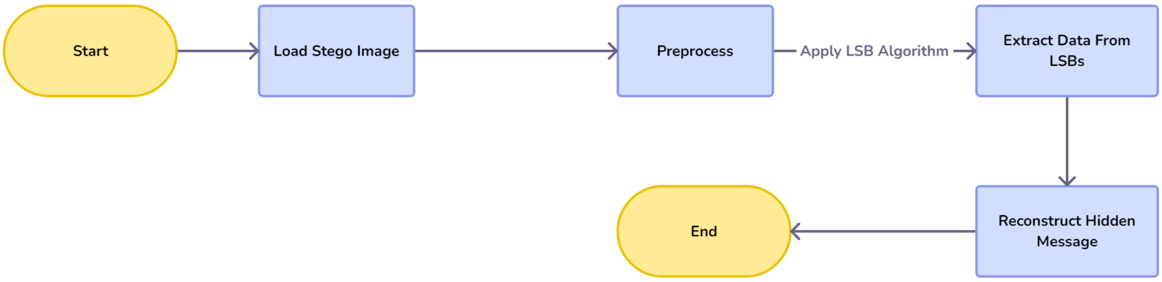


Figure 4.2: Flowchart depicting the LSB extraction methodology.

4.1.2 Discrete Cosine Transform(DCT) based Steganography

Description : DCT based steganography involves converting the cover image into its frequency domain using Discrete Cosine Transform.The secret text or image is then embedded into the transformed coefficients.

Methodology :

1. Convert the cover image and the secret text/image into binary format :
   - **Cover Image** : Each pixel in the cover image is represented by RGB values.Convert each RGB value into binary format where each color component (Red, Green, Blue) is represented by 8 bits.
   - **Secret text/image** : For text convert each character into its binary representation using ASCII or Unicode encoding.For images convert each pixel value into its binary representation based on number of color channels present (e.g 8 bits , 24 bits).
2. Apply DCT to the cover image :
   - Divide image into 8x8 blocks .
   - Apply the DCT to each and every block to transform the image from spatial domain to the frequency domain.
   - Quantize the DCT coefficients to reduce the amount of data .
3. Embed the secret text/image into the DCT coefficient :
   - Replace the least significant bit of the DCT coefficient with the bits of the secret text/ image..
   - Ensure that the changes made to the DCT coefficients are not minimised to maintain the visual quality of the image .
4. Use inverse DCT to reconstruct the modified stego image :
   - Apply the Inverse dct to each and every 8x8 blocks to change the image back to t spatial domain .
   - Reconstruct the modified image from the transformed block.

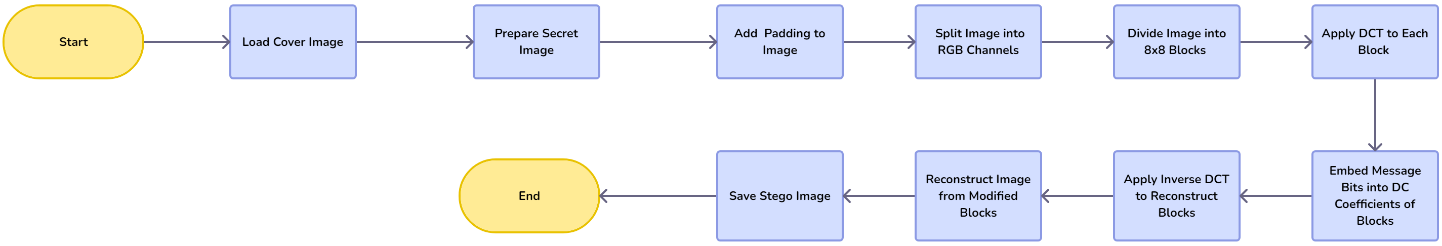

Start
Load Cover Image
Prepare Secret Image
Add Padding to Image
Split Image into RGB Channels
Divide Image into 8x8 Blocks
Apply DCT to Each Block
Embed Message Bits into DC Coefficients of Blocks
Apply Inverse DCT to Reconstruct Blocks
Reconstruct Image from Modified Blocks
Save Stego Image
End

Figure 4.3: Flowchart depicting the DCT embedding methodology.

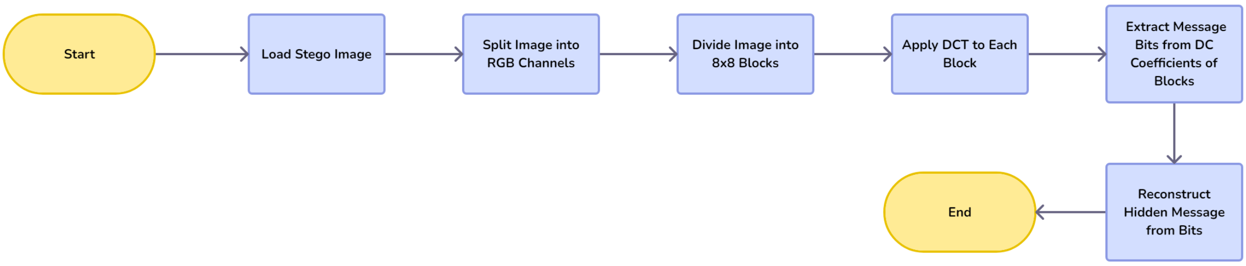

Start
Load Stego Image
Split Image into RGB Channels
Divide Image into 8x8 Blocks
Apply DCT to Each Block
Extract Message Bits from DC Coefficients of Blocks
Reconstruct Hidden Message from Bits
End

Figure 4.4: Flowchart depicting the DCT extraction methodology.

4.1.3 Fast Fourier Transform (FFT)

Description: Fast Fourier Transform (FFT) is a technique used in steganography to transform images into the frequency domain, allowing for embedding data in less noticeable frequency coefficients.

4.1.3.1 Methodology for Hiding Text Inside Image

Embedding Process :

The original cover image is loaded ,which will act as the cover medium for hiding textual data. The hidden text is then converted to an image to make it visible in form of pictures . The RGB values are normalised for original cover image. After that fast fourier transform algorithm is applied to this image turning it from spatial domain to its frequency domain.This means that all images can be manipulated through frequency components enabling embedding without too much change in the appearance of the image. Simultaneously a format suitable for embedding must be set for the text images. As such within each orig-

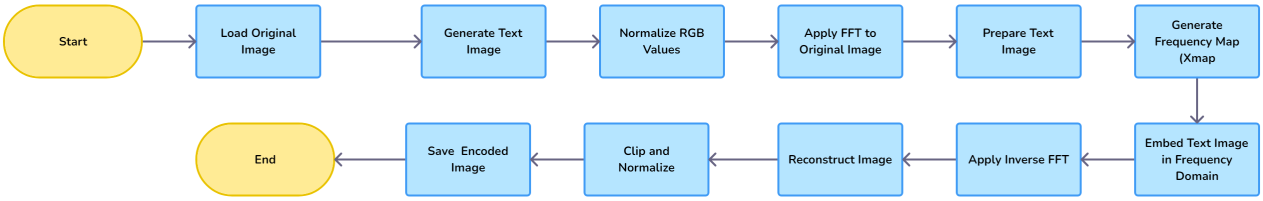


Figure 4.5: Flowchart depicting FFT embedding methodology for text in image.

inal components frequency position ,a frequency map is made on which it shows where exactly should text image be embedded. According to this xmap, text image should be embedded in original frequency domain of text Image. Following the frequency map the text image is embedded into the frequency domain of the original image. Once embedded,the inverse FFT is applied to convert the modified frequency domain image back to the spatial domain,reconstructing the image while hiding the text within its pixel values. The reconstructed image's pixel values are then clipped and normalized to ensure they fall within an acceptable range for image display. The final encoded image, now containing the hidden text, is saved, completing the embedding process.

4.1.3.2 Methodology for Extracting Hidden Text from an Image

Extraction Process :

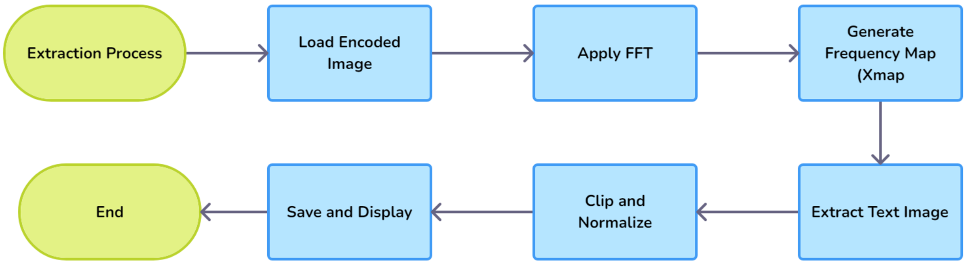


Figure 4.6: Flowchart depicting FFT extraction methodology for text in image.

The encryption algorithm starts by loading the disguised image that carries a steganographic message. In order to change it from a spatial one to frequency domain, the Fast Fourier Transform (FFT) is applied. Frequency map is generated and this will help find where the text image was embedded within the frequency components. Then it retrieves the text image from among all other frequency representations of the encoded image using this same map. The extracted text image is then clipped and normalized so that it can be readable. Lastly, save and show the hidden text in the picture after extracting it in this manner. By employing FFT as a tool for unveiling undisclosed information while adhering to an unchanged appearance of a base photo, this operation recreates all stages taken for hiding some data using these techniques.

4.1.3.3 Methodology for Hiding an Image Inside Another Image

Embedding Process:

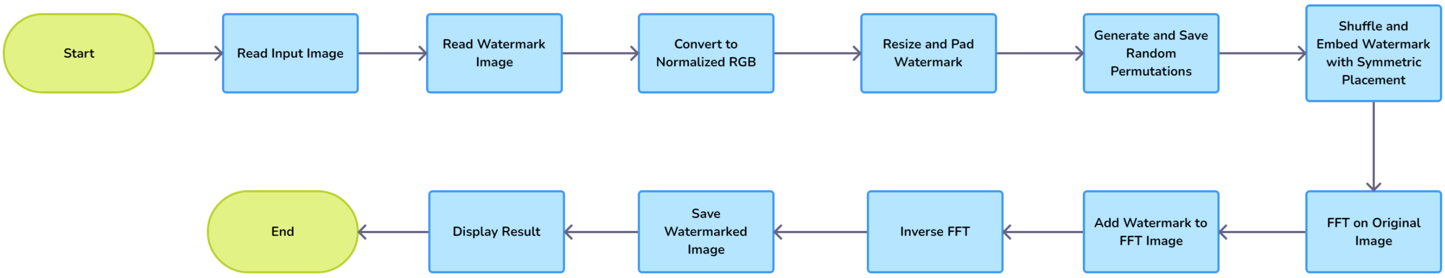

Start
Read Input Image
Read Watermark Image
Convert to Normalized RGB
Resize and Pad Watermark
Generate and Save Random Permutations
Shuffle and Embed Watermark with Symmetric Placement
FFT on Original Image
Add Watermark to FFT Image
Inverse FFT
Save Watermarked Image
Display Result
End

Figure 4.7: Flowchart depicting FFT embedding methodology for image in image.

Embedding a watermark (hidden image) into the original image by Fast Fourier Transform (FFT) involves following steps. Firstly, the system loads an original image that will consist of the mark to be embedded in it. At the same time also load the picture to be used as a watermark. Then both images are changed into normalized RGB values so that they are standardized. The next step is resizing and padding of watermarked image so that it matches in size with the original. Next, randomizing permutations are created and stored for future use during embedding and extracting processes. Designing these permutations guarantees that watermark is hidden. After this, using those saved permutations, watermark image becomes shuffled and placed symmetrically inside frequency components of original image. An FFT is performed on the initial picture converting it from space domain to frequency domain. After shuffling, then place symmetrically where we add watermarking, within FFT of primary photo along with its transformed information.. An inverse FFT will then be applied on modified domain frequency picture to convert it back into spatial domain thereby resulting in its pixel values as marked containing watermarks inside them.The final product was saved after hiding this mask in pictures' pixels.

4.1.3.4 Methodology for Extracting a Hidden Image from an Image

Extraction Process:

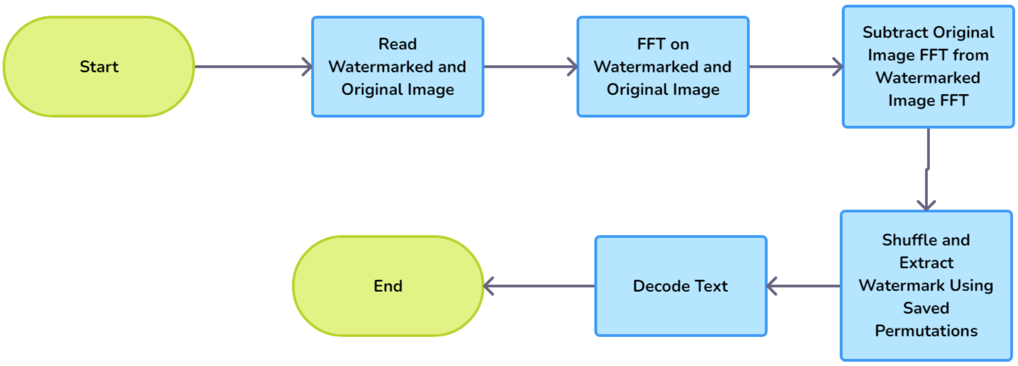

Start
Read Watermarked and Original Image
FFT on Watermarked and Original Image
Subtract Original Image FFT from Watermarked Image FFT
Shuffle and Extract Watermark Using Saved Permutations
Decode Text
End

Figure 4.8: Flowchart depicting FFT extraction methodology for image in image.

The procedure begins by loading the original image and watermarked image. The spatial domain of both images is transformed to frequency domain by the use of FFT.The watermark can be separated from the rest of the frequency components in a watermarked image by subtracting original image frequency components from them. Shuffling and extracting the watermark are done in the frequency domain using permutations saved before.At last, extraction process ends when the watermark is decoded and displayed.

Chapter 5

Results Analysis

5.1 Visual Analysis

In this section , the stego images are compared visually with the cover images.

5.1.1 Text Inside Image

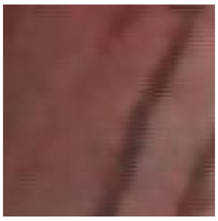
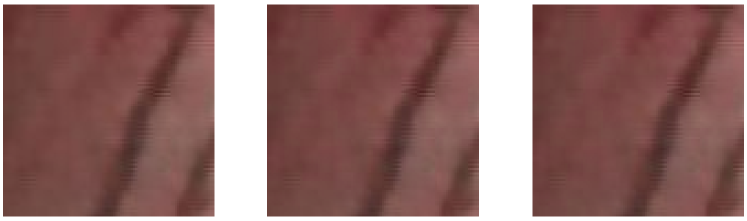


Figure 5.1: Cover Image used for hiding text inside image.

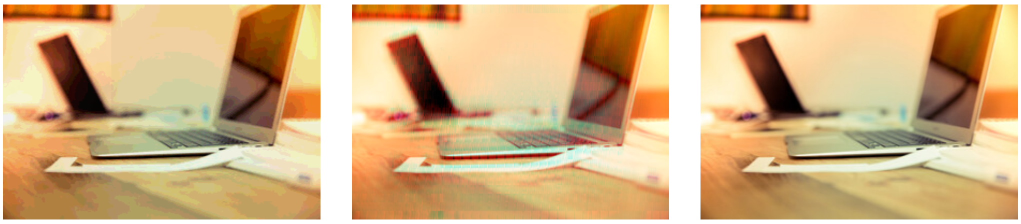


(a) LSB Text Stego (b) DCT Text Stego (c) FFT Text Stego

Figure 5.2: Comparison of stego images with cover image (image2.png) for text inside image.

5.1.2 Image Inside Image

Figure 5.3: Cover Image used for image inside image.



(a) LSB Image Stego

(b) DCT Image Stego

(c) FFT Image Stego

Figure 5.4: Comparison of stego images with cover image for image inside image.

In the visual analysis,it is seen that there are no major visual differences between the stego image (LSB, DCT,FFT) and their corresponding cover images for text embedded inside images (Figure 5.2). However,for image embedding within images (Figure 5.4 a), the LSB stego image shows noticeable visual quality differences compared to its cover image .This suggests that while text embedding methods preserve visual quality well enough, image embedding with LSB technique introduces discernible alterations in visual appearance.

5.2 Statistical Analysis

To measure the quality of the images we employed two evaluation metrics : Peak Signal to Noise Ratio(PSNR) and Structural Similarity Index (SSIM) .PSNR provides a quantitative measure of the distortion between the original and stego image ,while SSIM gives a more comprehensive assessment of structural similarities present between images.

5.2.1 Peak Signal to Noise Ratio (PSNR)

The PSNR is given by the Equation 5.1:

$$\text{PSNR} = 10 \cdot \log_{10}\left(\frac{\text{MAX}^2}{\text{MSE}}\right) \tag{5.1}$$

The PSNR measures the quality of a modified image compared to the original image .It is denoted in decibels(dB) and is expressed as the ratio of the maximum possible strength of signal(MAX) and the Mean squared error(MSE) between the original and the stego image .

Variables:

- MAX: Maximum possible pixel value (e.g 255 for 8 bit image).
- MSE: Mean Squared Error between the original and reconstructed images.

5.2.2 Structural Similarity Index (SSIM)

The SSIM is given by the Equation 5.2:

$$\text{SSIM}(x, y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \tag{5.2}$$

The SSIM measures the structural similarity between two images . It takes into account , luminance,contrast and structure, and provides a value between -1 and 1 where 1 indicates perfect similarity.

Variables:

- x, y: Images being compared.
- μ_x, μ_y: Mean values of images x and y, respectively.
- σ_x, σ_y: Standard deviations of images x and y, respectively.
- σ_{xy}: Covariance between images x and y.
- C_1, C_2: Constants to stabilize the division.

5.2.3 Results

Table 5.1: Metrics for Hiding Text inside Image

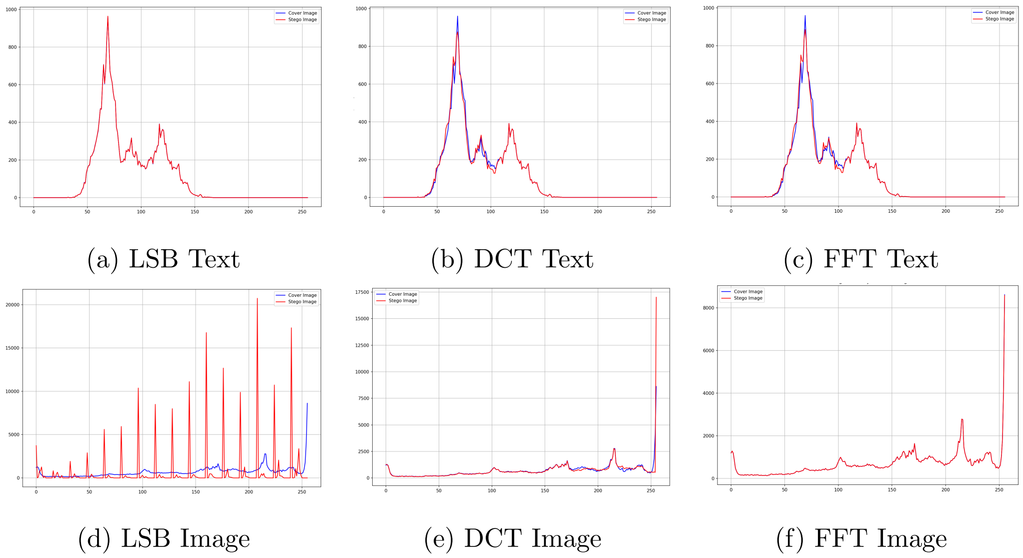
Method	**PSNR**	**SSIM**
LSB	77.06	0.999
DCT	46.23	0.997
FFT	43.49	0.975

Table 5.2: Metrics for Hiding Image inside Image

Method	**PSNR**	**SSIM**
LSB	30.117	0.956
DCT	31.12	0.938
FFT	42.83	0.988

The LSB method demonstrated good performance in preserving image quality and details when it came to hiding text inside image due to its simple embedding process .However its effiecieny diminishes when it came to hiding larger data such as images as shown by lower PSNR and SSIM value.The DCT method shows moderate performance across both tasks offering reasonable quality conservation but being surpassed by LSB for text hiding and FFT for image hiding.On the other hand,the FFT method excels in hiding images within images by exhibiting higher PSNR and SSIM values compared to LSB and DCT methods in this context .These findings shows the importance of selecting steganography methods based on specific application requirements,balancing factors such as data capacity ,quality preservation and computational efficiency.

5.3 Graphical Analysis



(a) LSB Text

(b) DCT Text

(c) FFT Text

(d) LSB Image

(e) DCT Image

(f) FFT Image

Figure 5.5: Histogram analysis of frequency vs. pixel intensity for cover and stego images.

The histogram analysis of stego images created by employing the LSB, DCT, and FFT techniques for both text and image embedding (see figure 5.5), reveals that there are clear trends as far as their fidelity to the original covers is concerned. Although LSB-based steganography is good at being used in text insertion, there are significant differences between it and the original image in terms of their histograms, which means that some changes have already been made in distributing pixel intensities. On the other hand, DCT-based embedding uses a more moderate tactic where histograms have slight variation showing better retention of image features. In fact, the histograms drawn for FFT based steganography show minimal drifts hence it has higher quality when hiding an image into another one making it useful when maintaining the integrity of an initial photo is important. These findings illustrate that there is always a trade-off between capacity for hidden information and accuracy of a resulting picture inherent to diverse methods ensuring successful concealment because they define ecological niches for each method in data protection systems.

5.4 Steganalysis

Steganalysis involves detecting the presence of hidden messages within images.The following parameters were used for analysis :

5.4.1 Chi-Square Test

The Chi-Square test is calculated using the following formula :

$$\chi^2 = \sum \frac{(O_i - E_i)^2}{E_i} \tag{5.3}$$

Where:

- O_i: Observed frequency
- E_i: Expected frequency

5.4.2 RS Analysis

RS Analysis evaluates the regular and singular groups within an image to detect potential steganographic content .

5.4.3 Fusion (Mean)

The Fusion(Mean) method combines the results of multiple steganalysis technique to produce a more robust metric for detection .

5.4.4 Primary Sets and Sample Pairs

Primary Sets and Sample Pairs methods analyze statistical differences in pixel intensity and correlation patterns to detect hidden data.

5.5 Steganalysis Results for Text Inside Image

File name	Above stego threshold?	Primary Sets	Chi Square	Sample Pairs	RS analysis	Fusion (mean)
dcttext	FALSE	0.011314551	null	0.004860684	0.014436202	0.010203813
ffttext	FALSE	0.011314551	null	0.006887706	0.01445808	0.010886779
lsbtext	FALSE	0.013919248	null	0.003822139	0.018133441	0.011958276

Table 5.3: Steganalysis results for text inside image

These results indicate that the images analyzed (dcttext, ffttext, and lsbtext) are below the stego threshold,which suggests no detectable hidden text .The primary sets, chi square, sample pairs, RS analysis and Fusion(mean) values are all within acceptable ranges indicating minimal deviation from normal image statistics.

5.5.1 Steganalysis Results for Image Inside Image

File name	Above stego threshold?	Primary Sets	Chi Square	Sample Pairs	RS analysis	Fusion (mean)
DCTimage	FALSE	0.045422454	null	0.032153821	0.04058253	0.039386268
FFTimage	FALSE	0.023357496	null	0.022014727	0.031055926	0.02547605
LSBimage	FALSE	0.005030685	null	0.013908522	0.017167782	0.012035663

Table 5.4: Steganalysis results for image inside image

The results for image embedding revealed that none of the images(namely DCTimage, FFTimage and LSBimage) exceed the stego limit.The primary sets, chi square, sample pairs, RS analysis and fusion(mean) metrics indicate that cover images are steganographically hidden messages that do not significantly change their statistical properties. The steganalysis results illustrate that the methods of embedding text and images within other images (LSB,DCT and FFT) yield stego-images which do not differ considerably from their respective cover images as per analyzed statistical metrics. This implies that these ways of hiding data could be said to maintain the integrity of cover image thereby making its detection difficult.

Chapter 6

Conclusion and Future Scope

6.1 Summary of Work

The purpose of this research was to look into different steganographic methods that can hide text and image data in digital images.It sought to evaluate the efficiency of Least Significant Bit ,Discrete Cosine Transform and Fast Fourier Transform for embedding capacity and retention of visual quality .The methodology required embedding textual and image data inside the cover images and subsequently conducting extensive analysis using metrics such as PSNR,SSIM, and steganalysis techniques.

6.2 Conclusions

The study yielded several key findings:

- Effectiveness of Steganographic Techniques : Compared to LSB, DCT and FFT approaches had better performance in terms of embedding capacity and visual qauality in image hiding techniques.

- Analysis of visuals and statistics : The quantifiable metrics like SSIM,PSNR and visual inspection indicate that there were almost no detectable differences between the stego image and the cover image in case of DCT and FFT meaning that they provide an enhanced image quality.

- Results of steganalysis : As shown by steganalysis results,it was rather hard to find out whether the hidden information was there or not ,a sign that these techniques were very effective at preserving the integrity of the cover image.

6.3 Future Scope

Future research directions could include:

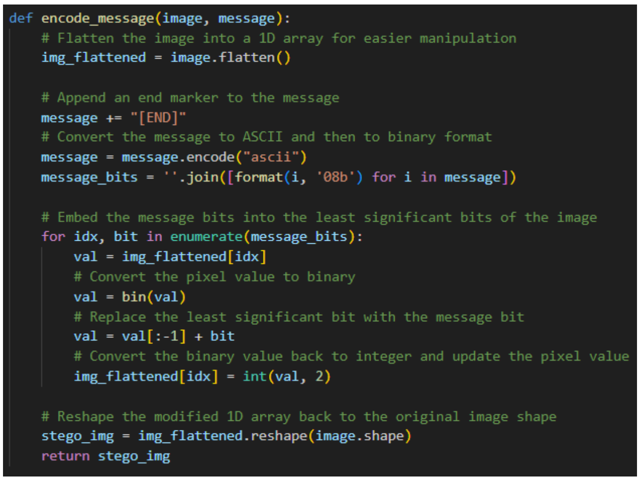
- Enhanced Security Measures : Exploring advanced encryption techniques and combined with steganography to enhance data security and prevent detection.
- Multi Modal Data Hiding : Investigating methods to embed and retrieve multiple kinds of data (text,images, audio) within a single stego object using hybrid steganography techniques.
- Real World Applications : Applying the developed techniques to practical scenarios such as digital watermarking,secure communication channels and data authentication in multimedia environments.

Appendices

Appendix A

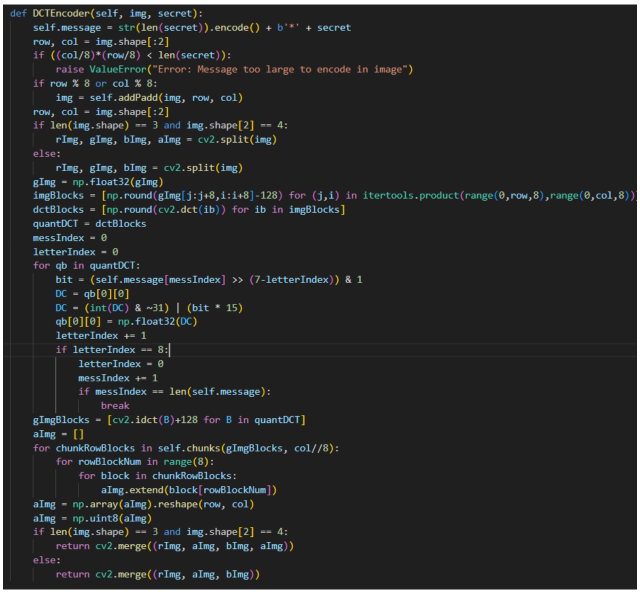
Code

A.1 Text Embedded Images



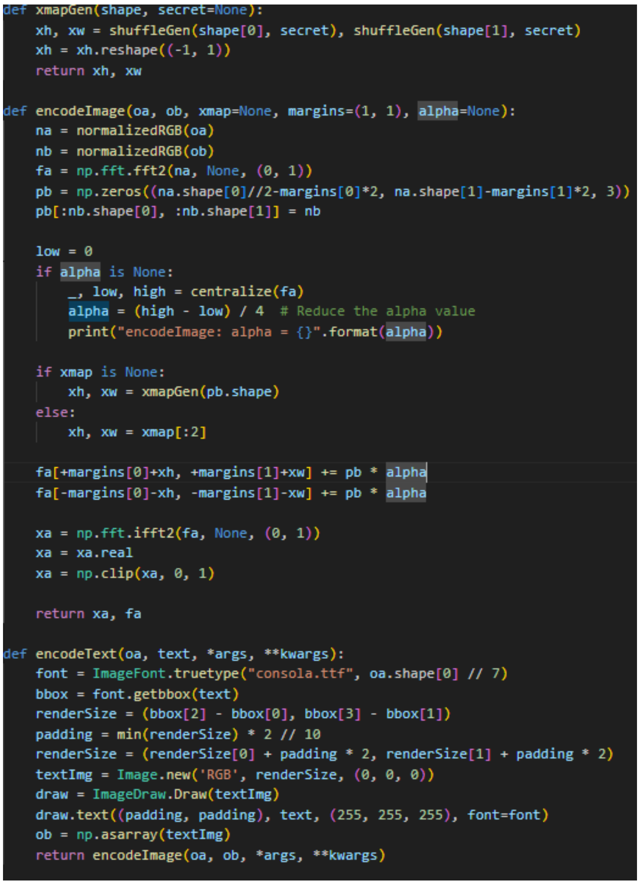
```python
def encode_message(image, message):
    # Flatten the image into a 1D array for easier manipulation
    img_flattened = image.flatten()

    # Append an end marker to the message
    message += "[END]"
    # Convert the message to ASCII and then to binary format
    message = message.encode("ascii")
    message_bits = ''.join([format(i, '08b') for i in message])

    # Embed the message bits into the least significant bits of the image
    for idx, bit in enumerate(message_bits):
        val = img_flattened[idx]
        # Convert the pixel value to binary
        val = bin(val)
        # Replace the least significant bit with the message bit
        val = val[:-1] + bit
        # Convert the binary value back to integer and update the pixel value
        img_flattened[idx] = int(val, 2)

    # Reshape the modified 1D array back to the original image shape
    stego_img = img_flattened.reshape(image.shape)
    return stego_img
```

Figure A.1: LSB Embedding for Text



```python
def DCTEncoder(self, img, secret):
    self.message = str(len(secret)).encode() + b'*' + secret
    row, col = img.shape[:2]
    if ((col/8)*(row/8) < len(secret)):
        raise ValueError("Error: Message too large to encode in image")
    if row % 8 or col % 8:
        img = self.addPadd(img, row, col)
    row, col = img.shape[:2]
    if len(img.shape) == 3 and img.shape[2] == 4:
        rImg, gImg, bImg, aImg = cv2.split(img)
    else:
        rImg, gImg, bImg = cv2.split(img)
    gImg = np.float32(gImg)
    imgBlocks = [np.round(gImg[j:j+8,i:i+8]-128) for (j,i) in itertools.product(range(0,row,8),range(0,col,8))]
    dctBlocks = [np.round(cv2.dct(ib)) for ib in imgBlocks]
    quantDCT = dctBlocks
    messIndex = 0
    letterIndex = 0
    for qb in quantDCT:
        bit = (self.message[messIndex] >> (7-letterIndex)) & 1
        DC = qb[0][0]
        DC = (int(DC) & ~31) | (bit * 15)
        qb[0][0] = np.float32(DC)
        letterIndex += 1
        if letterIndex == 8:
            letterIndex = 0
            messIndex += 1
            if messIndex == len(self.message):
                break
    gImgBlocks = [cv2.idct(B)+128 for B in quantDCT]
    aImg = []
    for chunkRowBlocks in self.chunks(gImgBlocks, col//8):
        for rowBlockNum in range(8):
            for block in chunkRowBlocks:
                aImg.extend(block[rowBlockNum])
    aImg = np.array(aImg).reshape(row, col)
    aImg = np.uint8(aImg)
    if len(img.shape) == 3 and img.shape[2] == 4:
        return cv2.merge((rImg, aImg, bImg, aImg))
    else:
        return cv2.merge((rImg, aImg, bImg))
```

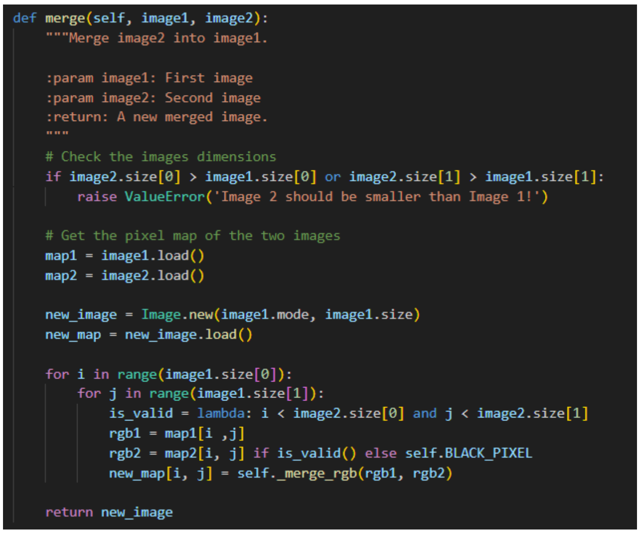
Figure A.2: DCT Embedding for Text



```python
def xmapGen(shape, secret=None):
    xh, xw = shuffleGen(shape[0], secret), shuffleGen(shape[1], secret)
    xh = xh.reshape((-1, 1))
    return xh, xw

def encodeImage(oa, ob, xmap=None, margins=(1, 1), alpha=None):
    na = normalizedRGB(oa)
    nb = normalizedRGB(ob)
    fa = np.fft.fft2(na, None, (0, 1))
    pb = np.zeros((na.shape[0]//2-margins[0]*2, na.shape[1]-margins[1]*2, 3))
    pb[:nb.shape[0], :nb.shape[1]] = nb

    low = 0
    if alpha is None:
        _, low, high = centralize(fa)
        alpha = (high - low) / 4  # Reduce the alpha value
        print("encodeImage: alpha = {}".format(alpha))

    if xmap is None:
        xh, xw = xmapGen(pb.shape)
    else:
        xh, xw = xmap[:2]

    fa[+margins[0]+xh, +margins[1]+xw] += pb * alpha
    fa[-margins[0]-xh, -margins[1]-xw] += pb * alpha

    xa = np.fft.ifft2(fa, None, (0, 1))
    xa = xa.real
    xa = np.clip(xa, 0, 1)

    return xa, fa

def encodeText(oa, text, *args, **kwargs):
    font = ImageFont.truetype("consola.ttf", oa.shape[0] // 7)
    bbox = font.getbbox(text)
    renderSize = (bbox[2] - bbox[0], bbox[3] - bbox[1])
    padding = min(renderSize) * 2 // 10
    renderSize = (renderSize[0] + padding * 2, renderSize[1] + padding * 2)
    textImg = Image.new('RGB', renderSize, (0, 0, 0))
    draw = ImageDraw.Draw(textImg)
    draw.text((padding, padding), text, (255, 255, 255), font=font)
    ob = np.asarray(textImg)
    return encodeImage(oa, ob, *args, **kwargs)
```

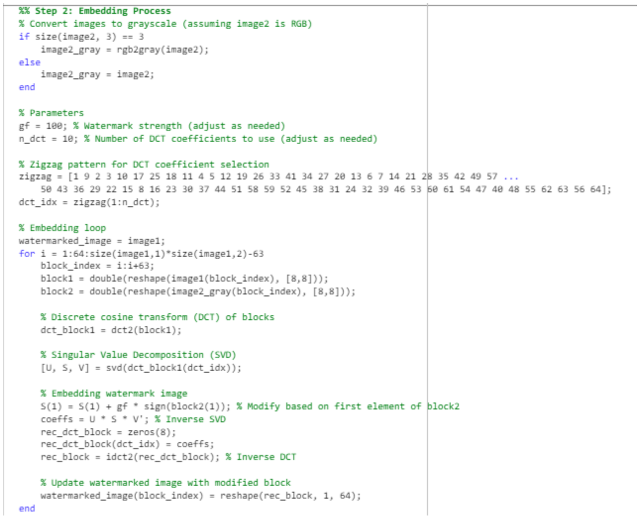
Figure A.3: FFT Embedding for Text

A.2 Image Embedded Images



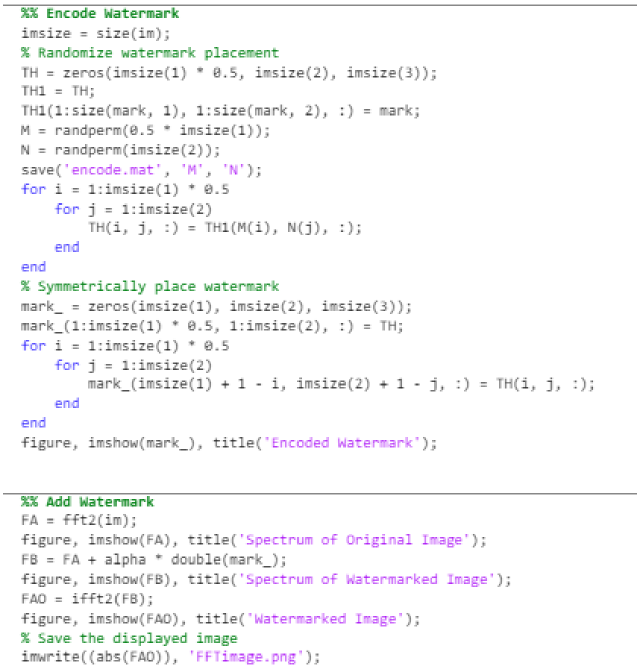
```python
def merge(self, image1, image2):
    """Merge image2 into image1.

    :param image1: First image
    :param image2: Second image
    :return: A new merged image.
    """
    # Check the images dimensions
    if image2.size[0] > image1.size[0] or image2.size[1] > image1.size[1]:
        raise ValueError('Image 2 should be smaller than Image 1!')

    # Get the pixel map of the two images
    map1 = image1.load()
    map2 = image2.load()

    new_image = Image.new(image1.mode, image1.size)
    new_map = new_image.load()

    for i in range(image1.size[0]):
        for j in range(image1.size[1]):
            is_valid = lambda: i < image2.size[0] and j < image2.size[1]
            rgb1 = map1[i ,j]
            rgb2 = map2[i, j] if is_valid() else self.BLACK_PIXEL
            new_map[i, j] = self._merge_rgb(rgb1, rgb2)

    return new_image
```

Figure A.4: LSB Embedding for Image



```matlab
%% Step 2: Embedding Process
% Convert images to grayscale (assuming image2 is RGB)
if size(image2, 3) == 3
    image2_gray = rgb2gray(image2);
else
    image2_gray = image2;
end

% Parameters
gf = 100; % Watermark strength (adjust as needed)
n_dct = 10; % Number of DCT coefficients to use (adjust as needed)

% Zigzag pattern for DCT coefficient selection
zigzag = [1 9 2 3 10 17 25 18 11 4 5 12 19 26 33 41 34 27 20 13 6 7 14 21 28 35 42 49 57 ...
    50 43 36 29 22 15 8 16 23 30 37 44 51 58 59 52 45 38 31 24 32 39 46 53 60 61 54 47 40 48 55 62 63 56 64];
dct_idx = zigzag(1:n_dct);

% Embedding loop
watermarked_image = image1;
for i = 1:64:size(image1,1)*size(image1,2)-63
    block_index = i:i+63;
    block1 = double(reshape(image1(block_index), [8,8]));
    block2 = double(reshape(image2_gray(block_index), [8,8]));

    % Discrete cosine transform (DCT) of blocks
    dct_block1 = dct2(block1);

    % Singular Value Decomposition (SVD)
    [U, S, V] = svd(dct_block1(dct_idx));

    % Embedding watermark image
    S(1) = S(1) + gf * sign(block2(1)); % Modify based on first element of block2
    coeffs = U * S * V'; % Inverse SVD
    rec_dct_block = zeros(8);
    rec_dct_block(dct_idx) = coeffs;
    rec_block = idct2(rec_dct_block); % Inverse DCT

    % Update watermarked image with modified block
    watermarked_image(block_index) = reshape(rec_block, 1, 64);
end
```

Figure A.5: DCT Embedding for Image



```
%% Encode Watermark
imsize = size(im);
% Randomize watermark placement
TH = zeros(imsize(1) * 0.5, imsize(2), imsize(3));
TH1 = TH;
TH1(1:size(mark, 1), 1:size(mark, 2), :) = mark;
M = randperm(0.5 * imsize(1));
N = randperm(imsize(2));
save('encode.mat', 'M', 'N');
for i = 1:imsize(1) * 0.5
    for j = 1:imsize(2)
        TH(i, j, :) = TH1(M(i), N(j), :);
    end
end
% Symmetrically place watermark
mark_ = zeros(imsize(1), imsize(2), imsize(3));
mark_(1:imsize(1) * 0.5, 1:imsize(2), :) = TH;
for i = 1:imsize(1) * 0.5
    for j = 1:imsize(2)
        mark_(imsize(1) + 1 - i, imsize(2) + 1 - j, :) = TH(i, j, :);
    end
end
figure, imshow(mark_), title('Encoded Watermark');

%% Add Watermark
FA = fft2(im);
figure, imshow(FA), title('Spectrum of Original Image');
FB = FA + alpha * double(mark_);
figure, imshow(FB), title('Spectrum of Watermarked Image');
FAO = ifft2(FB);
figure, imshow(FAO), title('Watermarked Image');
% Save the displayed image
imwrite((abs(FAO)), 'FFTimage.png');
```

Figure A.6: FFT Embedding for Image

References

[1] S. Karakus and E. Avci, "A new image steganography method with optimum pixel similarity for data hiding in medical images," *Medical hypotheses*, vol. 139, p. 109691, 2020.

[2] P. Mortazavian, M. Jahangiri, and E. Fatemizadeh, "A low-degradation steganography model for data hiding in medical images," in *Proceeding of the Fourth IASTED International Conference Visualization, Imaging, and Image Processing.* Citeseer, 2004, pp. 914–920.

[3] G. Prabakaran, R. Bhavani, and P. Rajeswari, "Multi secure and robustness for medical image based steganography scheme," in *2013 international conference on circuits, power and computing technologies (ICCPCT).* IEEE, 2013, pp. 1188–1193.

[4] A. Priyadharshini, R. Umamaheswari, N. Jayapandian, and S. Priyananci, "Securing medical images using encryption and lsb steganography," in *2021 international conference on advances in electrical, computing, communication and sustainable technologies (ICAECT).* IEEE, 2021, pp. 1–5.

[5] M. Khalil, "Medical image steganography: study of medical image quality degradation when embedding data in the frequency domain," *International Journal of Computer Network and Information Security*, vol. 9, no. 2, p. 22, 2017.

[6] M. A. Ahmad, M. Elloumi, A. H. Samak, A. M. Al-Sharafi, A. Alqazzaz, M. A. Kaid, and C. Iliopoulos, "Hiding patients' medical reports using an enhanced wavelet steganography algorithm in dicom images," *Alexandria Engineering Journal*, vol. 61, no. 12, pp. 10 577–10 592, 2022.

[7] E. Walia, P. Jain, and N. Navdeep, "An analysis of lsb & dct based steganography," *Global Journal of Computer Science and Technology*, vol. 10, no. 1, pp. 4–8, 2010.

[8] B. Kaur, A. Kaur, and J. Singh, "Steganographic approach for hiding image in dct domain," *International Journal of Advances in Engineering & Technology*, vol. 1, no. 3, p. 72, 2011.

[9] A. Khan and A. Sarfaraz, "Fft-etm based distortion less and high payload image steganography," *Multimedia Tools and Applications*, vol. 78, pp. 25 999–26 022, 2019.

[10] M. Bachrach and F. Y. Shih, "Image steganography and steganalysis," *Wiley Interdisciplinary Reviews: Computational Statistics*, vol. 3, no. 3, pp. 251–259, 2011.

[11] S. Moccia, E. De Momi, M. Guarnaschelli, M. Savazzi, A. Laborai, L. Guastini, G. Peretti, and L. S. Mattos, "Confident texture-based laryngeal tissue classification for early stage diagnosis support," *Journal of Medical Imaging*, vol. 4, no. 3, pp. 034 502–034 502, 2017.

Table A.1: Project Detail

Student Details

Student Name	Saurav Kumar		
Registration Number	200911254	Section/Roll No.	A/66
Email Address	srv.kr1695@gmail.com	Phone No.(M)	9470000110

Project Details

Project Title			
Project Duration	4 Months	Date of Reporting	27-01-2024

Organization Details

Organization Name	Manipal Academy of Higher Education
Full Postal Address	Eshwar Nagar, Manipal, Karnataka - 576104
Website Address	www.manipal.edu

Supervisor Details

Supervisor Full Name	Dr. Raviraja Holla M		
Designation	Assistant Professor - Senior Scale		
Full Contact Address with PIN Code	Eshwar Nagar, Manipal, Karnataka - 576104		
Email Address	raviraj.holla@manipal.edu	Phone No.(M)	9480570768

Internal Guide Details

Faculty Name	Dr. Raviraja Holla M
Full Contact Address with PIN Code	Department of Information and Communication Technology, Manipal Institute of Technology, Manipal-576104
Email Address	raviraj.holla@manipal.edu

FInal_Project_Report_200911254_SauravKumar

ORIGINALITY REPORT

14%	11%	10%	%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.coursehero.com Internet Source	1%
2	impressions.manipal.edu Internet Source	1%
3	mafiadoc.com Internet Source	1%
4	Agneet Chatterjee, Soulib Ghosh, Anuran Chakraborty, Sudipta Kr Ghosal, Ram Sarkar. "A two-phase gradient based feature embedding approach", Journal of Information Security and Applications, 2021 Publication	1%
5	www.researchgate.net Internet Source	1%
6	umpir.ump.edu.my Internet Source	1%
7	www.mdpi.com Internet Source	1%
8	ir.lib.uwo.ca Internet Source	

		1 %
9	zenodo.org Internet Source	1 %
10	dl.lib.uom.lk Internet Source	<1 %
11	Schmidt, Mark Andrew. "Characterization of the molecular epidemiology of Neisseria meningitidis and investigation of two potential risk factors associated with invasive meningococcal disease", Proquest, 20111004 Publication	<1 %
12	www.frontiersin.org Internet Source	<1 %
13	elibrary.tucl.edu.np Internet Source	<1 %
14	"Intelligent Data Communication Technologies and Internet of Things", Springer Science and Business Media LLC, 2021 Publication	<1 %
15	commons.erau.edu Internet Source	<1 %
16	Mostafa Ahmad, Ahmed Ghoneim, Saleh Alshomrani, Ahmed Samak, Nader Omar, Fahad Algarni. "A novel and dependable	<1 %

	image steganography model for strengthening the security of cloud storage", Journal of Intelligent & Fuzzy Systems, 2020 Publication	
17	Nandhini Sivasubramanian, Gunaseelan Konganathan, Yeragudipati Venkata Ramana Rao. "High capacity multi-bit data hiding based on modified histogram shifting technique", ETRI Journal, 2018 Publication	<1 %
18	discovery.researcher.life Internet Source	<1 %
19	"Soft Computing for Problem Solving", Springer Science and Business Media LLC, 2021 Publication	<1 %
20	Arriaga Pazos, Francisco. "In-Between Frame Generation for 2D Animation Using Generative Adversarial Networks", The University of Texas at El Paso, 2024 Publication	<1 %
21	Krishna Kumar, Satyabrata Roy, Umashankar Rawat, Astitv Shandilya. "SOCIET: Second-order cellular automata and chaotic map-based hybrid image encryption technique", Multimedia Tools and Applications, 2023 Publication	<1 %

22	brainmass.com Internet Source	<1 %
23	focus.ti.com Internet Source	<1 %
24	Li, Can. "Conversation Understanding and Realistic Artificial Crash Data Generation With Deep Learning", University of Missouri - Columbia, 2024 Publication	<1 %
25	Yucheng Pan, Yongjun Wang, Hui Xu, Xiaoyuan Niu, Jun Li, Xinyu Liu. "Image Registration SIFT Algorithm Based on Adaptive Adjustment of Grayscale Weight", 2019 18th International Conference on Optical Communications and Networks (ICOCN), 2019 Publication	<1 %
26	De Rosal Ignatius Moses Setiadi, Supriadi Rustad, Pulung Nurtantio Andono, Guruh Fajar Shidik. "Digital Image Steganography Survey and Investigation (Goal, Assessment, Method, Development, and Dataset)", Signal Processing, 2023 Publication	<1 %
27	Raviraja Holla, D. Suma. "Enhancing Laryngeal Spinocellular Carcinoma Image Security with	<1 %

	DCT", Indian Journal of Otolaryngology and Head & Neck Surgery, 2023 Publication	
28	dspace.daffodilvarsity.edu.bd:8080 Internet Source	<1 %
29	Reis, Joana. "Artificial Intelligent Doctors vs. Human Doctors: Does the Type of Doctor in Cosmetic Procedures Influences Consumer Self-Esteem?", Universidade NOVA de Lisboa (Portugal), 2024 Publication	<1 %
30	ijritcc.org Internet Source	<1 %
31	link.springer.com Internet Source	<1 %
32	nijocet.fud.edu.ng Internet Source	<1 %
33	opus.lib.uts.edu.au Internet Source	<1 %
34	uat.manipal.edu Internet Source	<1 %
35	vdocuments.net Internet Source	<1 %
36	www.ijcaonline.org Internet Source	<1 %

37	www.koreascience.or.kr Internet Source	<1 %
38	An, Le, and Bir Bhanu. "Improved image super-resolution by Support Vector Regression", The 2011 International Joint Conference on Neural Networks, 2011. Publication	<1 %
39	Tamer Rabie, Ibrahim Kamel. "On the embedding limits of the discrete cosine transform", Multimedia Tools and Applications, 2015 Publication	<1 %
40	Ganavi M, Prabhudeva S, Hemanth Kumar N P. "An Efficient Image Steganography Scheme Using Bit-plane Slicing with Elliptic Curve Cryptography and Wavelet Transform", International Journal of Computer Network and Information Security, 2022 Publication	<1 %

Exclude quotes	On	Exclude matches	< 3 words
Exclude bibliography	On		

How much of this submission has been generated by AI?

*3%

of qualifying text in this submission has been determined to be generated by AI.

* Low scores have a higher likelihood of false positives.

Caution: Percentage may not indicate academic misconduct. Review required.

It is essential to understand the limitations of AI detection before making decisions about a student's work. We encourage you to learn more about Turnitin's AI detection capabilities before using the tool.

Frequently Asked Questions

What does the percentage mean?
The percentage shown in the AI writing detection indicator and in the AI writing report is the amount of qualifying text within the submission that Turnitin's AI writing detection model determines was generated by AI.

Our testing has found that there is a higher incidence of false positives when the percentage is less than 20. In order to reduce the likelihood of misinterpretation, the AI indicator will display an asterisk for percentages less than 20 to call attention to the fact that the score is less reliable.

However, the final decision on whether any misconduct has occurred rests with the reviewer/instructor. They should use the percentage as a means to start a formative conversation with their student and/or use it to examine the submitted assignment in greater detail according to their school's policies.

How does Turnitin's indicator address false positives?
Our model only processes qualifying text in the form of long-form writing. Long-form writing means individual sentences contained in paragraphs that make up a longer piece of written work, such as an essay, a dissertation, or an article, etc. Qualifying text that has been determined to be AI-generated will be highlighted blue on the submission text.

Non-qualifying text, such as bullet points, annotated bibliographies, etc., will not be processed and can create disparity between the submission highlights and the percentage shown.

What does 'qualifying text' mean?
Sometimes false positives (incorrectly flagging human-written text as AI-generated), can include lists without a lot of structural variation, text that literally repeats itself, or text that has been paraphrased without developing new ideas. If our indicator shows a higher amount of AI writing in such text, we advise you to take that into consideration when looking at the percentage indicated.

In a longer document with a mix of authentic writing and AI generated text, it can be difficult to exactly determine where the AI writing begins and original writing ends, but our model should give you a reliable guide to start conversations with the submitting student.

Disclaimer
Our AI writing assessment is designed to help educators identify text that might be prepared by a generative AI tool. Our AI writing assessment may not always be accurate (it may misidentify both human and AI-generated text) so it should not be used as the sole basis for adverse actions against a student. It takes further scrutiny and human judgment in conjunction with an organization's application of its specific academic policies to determine whether any academic misconduct has occurred.

CO and PO Mapping

CLOs		PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
ICT 4299.1	Assess the work available in the literature related to the project to identify the limitations and risks.	2	3	2	3	2	2	2	2	2	3	2	2
ICT 4299.2	Practice planning and time management in solving the problem.	1	1	1	1	1	1	1	3	3	3	2	2
ICT 4299.3	Demonstrate professional skills to work effectively in a team or individually.	3	3	3	3	3	3	3	3	3	3	3	3
ICT 4299.4	Develop the ability to adopt a methodological approach to solve societal problems..	2	3	3	2	2	3	3	3	2	2	2	3
ICT 4299.5	Conduct experimentation and testing to achieve the defined objectives through computing/coding/statistical analysis	3	3	3	3	3	2	2	3	2	2	2	3
ICT 4299.6	Compose the technical report with effective communication on incorporating ethical practices.	3	3	3	3	3	3	3	3	3	3	3	3
ICT 4299 (Avg. correlation level)		**2.33**	**2.67**	**2.5**	**2.5**	**2.33**	**2.33**	**2.33**	**2.5**	**2.5**	**2.67**	**2.33**	**2.67**

PROGRAM OUTCOMES (PO)

Engineering Graduates will be able to:

1. Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.

2. Problem analysis: Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.

3. Design/development of solutions: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.

4. Conduct investigations of complex problems: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.

5. Modern tool usage: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.

6. The engineer and society: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.

7. Environment and sustainability: Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.

8. Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.

9. Individual and team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.

10. Communication: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.

11. Project management and finance: Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.

12. Life-long learning: Recognize the need for and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

CLOs		PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9
ICT 4299.1	Assess the work available in the literature related to the project to identify the limitations and risks.	3	2	2	2	2	3	1	2	3
ICT 4299.2	Practice planning and time management in solving the problem.	1	3	3	3	2	1	2	2	2
ICT 4299.3	Demonstrate professional skills to work effectively in a team or individually.	3	3	3	2	2	3	3	1	2
ICT 4299.4	Develop the ability to adopt a methodological approach to solve societal problems..	2	3	1	3	2	2	2	1	2
ICT 4299.5	Conduct experimentation and testing to achieve the defined objectives through computing/coding/statistical analysis	2	2	3	3	3	3	2	3	2
ICT 4299.6	Compose the technical report with effective communication on incorporating ethical practices.	2	2	2	2	3	1	2	3	1
ICT 4299 (Avg. correlation level)		**2.16**	**2.5**	**2.33**	**2.5**	**2.33**	**2.16**	**2.0**	**2.0**	**2.0**

1. To identify, analyse and develop software systems using appropriate techniques and concepts related to information technology
2. To design an algorithm or process within realistic constraints to meet the desired needs through analytical, logical and problem-solving skills.
3. To apply state of the art IT tools and technologies, IT infrastructure management abilities in treading innovative career path as a prospective IT engineer
4. Apply the principles of science, maths and computer programming to solve complex problems related to information technology.
5. Apply knowledge of programming, computational intelligence, computer graphics and visualization, data analytics, software system design, cyber security to arrive at solutions to real world problems.
6. Apply IT knowledge to design and develop systems with respect to societal, user, customer needs, health and safety, diversity, inclusion, societal, environmental codes of practise and industry standard.
7. Integrate and interface industry relevant hardware and software components and technology to come up with innovative and creative solutions.
8. Use of industry standard software tools and platform to design and analyze IT systems.
9. Learn to function collaboratively as a member of leader in diverse teams in multidisciplinary settings to manage the process effectively and document, present and communicate with the engineering community.

COURSE Code	Course Title	PO 1	PO2	PO3	PO 4	PO 5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PS02	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO 9
ICT 4299	Project Work	**Avg:**	**Avg:**	**Avg:**	**Avg:**	**Avg:**																

IET (AHEP Mapping):

CLOs		C1	C2	C3	C4	C5	C6	C13	C16	C17
ICT 4299.1	Assess the work available in the literature related to the project to identify the limitations and risks.	3	2	2	3	3	3	2	3	3
ICT 4299.2	Practice planning and time management in solving the problem.	2	3	2	2	3	3	3	2	2
ICT 4299.3	Demonstrate professional skills to work effectively in a team or individually.	3	3	3	3	2	2	3	3	3
ICT 4299.4	Develop the ability to adopt a methodological approach to solve societal problems..	3	2	3	3	3	2	2	3	3
ICT 4299.5	Conduct experimentation and testing to achieve the defined objectives through computing/coding/statistical analysis	3	3	3	3	2	2	3	3	3
ICT 4299.6	Compose the technical report with effective communication on incorporating ethical practices.	3	3	2	2	3	3	3	3	2
ICT 4299 (Avg. correlation level)		**2.83**	**2.67**	**2.5**	**2.67**	**2.67**	**2.5**	**2.67**	**2.83**	**2.67**

Category	AHEP LO number	AHEP LO Statements
Science & Maths	C1	Apply knowledge of mathematics, statistics, natural science and engineering principles to the solution of complex problems. Some of the knowledge will be at the forefront of the particular subject of study
Engineering Analysis	C2	Analyse complex problems to reach substantiated conclusions using first principles of mathematics, statistics, natural science and engineering principles
	C3	Select and apply appropriate computational and analytical techniques to model complex problems, recognising the limitations of the techniques employed
	C4	Select and evaluate technical literature and other sources of information to address complex problems
Design & Innovation	C5	Design solutions for complex problems that meet a combination of societal, user, business and customer needs as appropriate. This will involve consideration of applicable health & safety, diversity, inclusion, cultural, societal, environmental and commercial matters, codes of practice and industry standards
	C6	Apply an integrated or systems approach to the solution of complex problems
The Engineer & Society	C7	Evaluate the environmental and societal impact of solutions to complex problems and minimise adverse impacts
	C8	Identify and analyse ethical concerns and make reasoned ethical choices informed by professional codes of conduct
	C9	Use a risk management process to identify, evaluate and mitigate risks (the effects of uncertainty) associated with a particular project or activity
	C10	Adopt a holistic and proportionate approach to the mitigation of security risks
	C11	Adopt an inclusive approach to engineering practice and recognise the responsibilities, benefits and importance of supporting equality, diversity and inclusion
Engineering Practice	C12	Use practical laboratory and workshop skills to investigate complex problems
	C13	Select and apply appropriate materials, equipment, engineering technologies and processes, recognising their limitations
	C14	Discuss the role of quality management systems and continuous improvement in the context of complex problems
	C15	Apply knowledge of engineering management principles, commercial context, project and change management, and relevant legal matters including intellectual property rights
	C16	Function effectively as an individual, and as a member or leader of a team
	C17	Communicate effectively on complex engineering matters with technical and non-technical audiences
	C18	Plan and record self-learning and development as the foundation for lifelong learning/CPD