IMAGE STEGANOGRAPHY USING LSB AND DCT

A PROJECT REPORT

Submitted by

BL.EN.U4AIE19007	Apoorva Mani
BL.EN.U4AIE19041	Maturi Tanuj
BL.EN.U4AIE19068	Aishwarya V

in partial fulfillment for the award of the degree of

BACHELOR OF TECHNOLOGY

IN

ARTIFICIAL INTELLIGENCE AND ENGINEERING

AMRITA SCHOOL OF ENGINEERING, BANGALORE

AMRITA VISHWA VIDYAPEETHAM

BANGALORE 560 035

June – 2022

BONAFIDE CERTIFICATE

This is to certify that the project report entitled **Image Steganography Using LSB and DCT** submitted by

BL.EN.U4AIE19007	Apoorva Mani
BL.EN.U4AIE19041	Maturi Tanuj
BL.EN.U4AIE19068	Aishwarya V

in partial fulfillment of the requirements in the **Degree Bachelor of Technology** “Artificial Intelligence and Engineering” as part of 21AIE435 CYBERCRIME INVESTIGATION AND DIGITAL FORENSICS Project is a bonafide record of the work carried out undermy guidance and supervision at Amrita School of Engineering, Bangalore.

<signature>	<signature>	
<Guide name>	<Guide name>	Dr. Sriram Devanathan
<Designation>	<Designation>	Professor and Chairperson,
Dept. of CSE	Dept. of CSE	Dept. of CSE

This project report was evaluated by us on ………

ACKNOWLEDGEMENT

The satisfaction that accompanies successful completion of any task would be incomplete without mention of people who made it possible, and whose constant encouragement and guidance have been source of inspiration throughout the course of this project work.

We offer our sincere pranams at the lotus feet of **”AMMA”, MATA AMRITANANDAMAYI DEVI** who showered her blessing upon us throughout the course of this project work.

We owe our gratitude to **Dr. Manoj P.**, Director, Amrita School of Engineering, Bangalore.

We thank **Dr. Sriram Devanathan,** Principal and Chairperson-CSE, Amrita School of Engineering, Bangalore for his support and inspiration.

It is a great pleasure to express our gratitude and indebtedness to our project guide “**GUIDE NAME AND DESIGNATION”**, Department of Computer Science and Engineering, Amrita School of Engineering, Bangalore for her valuable guidance, encouragement, moral support, and affection throughout the project work.

We would like to thank express our gratitude to project panel members for their suggestions, encouragement, and moral support during the process of project work and all faculty members for their academic support. Finally, we are forever grateful to our parents, who have loved, supported, and encouraged us in all our endeavors.

ABSTRACT

In this project we introduce an algorithm of digital image steganography based on Least Significant Bit (LSB) and Discrete Cosine Transform (DCT). According to the characters of human vision, in this algorithm, the information of digital watermarking which has been discrete Cosine transformed, is put into the high frequency band of the image which has been wavelet transformed. Then distills the digital watermarking with the help of the original image and the watermarking image. The simulation results show that this algorithm is invisible and has good robustness for some common image processing operations.

Keywords — digital watermarking; least significant bit (LSB), discrete cosine transform (DCT); peak signal to noise ratio (PSNR), high frequency band, mean square error.

TABLE OF CONTENTS

Page no.

CHAPTER - 1

INTRODUCTION

The Steganography is derived from the Greek word steganographic which means covert writing. It is the science of embedding information into cover objects such as images that will escape detection and retrieved with minimum distortion at the destination. The rapid growth of internet coupled with high bandwidth and low-cost computer hardware have propelled the explosive growth of steganography. The objective of modem steganography is to keep the payload(embedded information) undetected, but the steganographic systems, because of their invasive nature, leave behind the traces in the cover image. Steganography and cryptography are closely related. Cryptography provides confidentiality. Steganography on the other hand hides the message and there is no knowledge of the existence of the message. Steganography finds applications in watermarking, finger printing, and the modem multimedia message service; to name a few. The resultant image object obtained after embedding information into the cover image is called as stego object.

Steganographic Techniques

i. Physical Steganography: Physical Steganography has been widely used. In ancient time people wrote message on wood and then covered it with wax. Message was written on the back of postage stamps. Message was written on paper by secret inks.

ii. Digital Steganography: Digital Steganography is the art of invisibly hiding data within data. It conceals the fact that message exists by hiding the actual message. In this, secret data can be hidden inside the image, text, sound clip which can be represented in binary.

iii. Printed Steganography: Digital Steganography output can be in the form of printed documents. The letter size, spacing and other characteristics of a cover text can be manipulated to carry the hidden message. A recipient who knows the technique used can recover the message and then decrypt it

CHAPTER - 2

SYSTEM SPECIFICATIONS

2.1 SOFTWARE REQUIREMENTS

Languages used to develop this project: PYTHON

- LEX
- YACC

2.2 DIFFERENT MODULES OF PROJECT

Different Folders:

1. **Comparison_images**: This folder contains the images that outputs of different algorithms .
2. **Dct_encoded**: This folder contains the image that displays result of dct algorithm.
3. **Lsb_encoded**: This folder contains the image that displays result of LSB algorithm

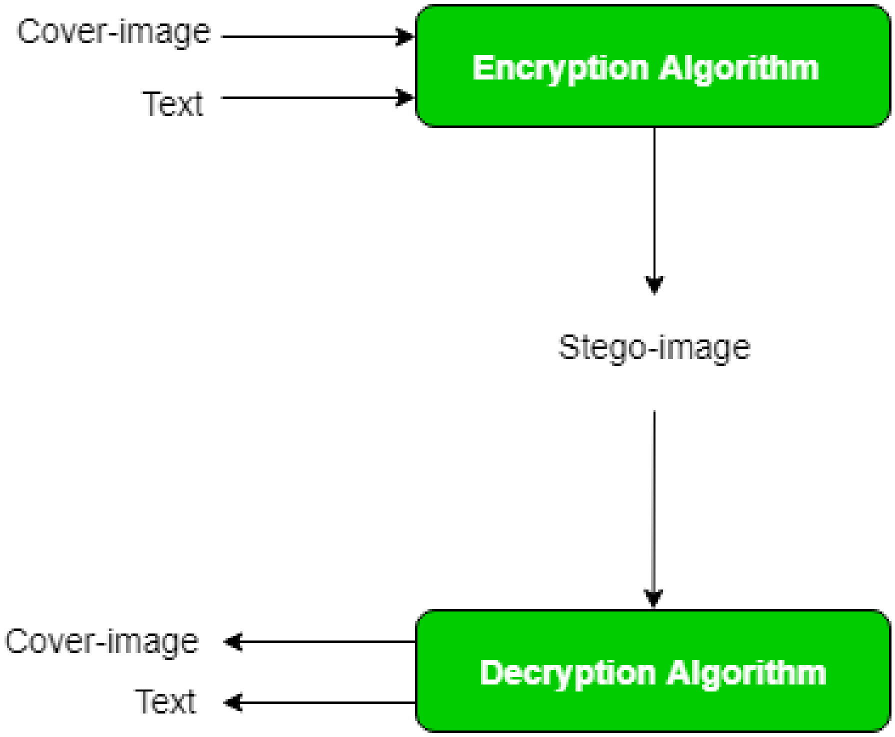
Different Files:

1. **final.ipynb:** The final python code which will is ran in colab by giving various images as inputs .

CHAPTER – 3

SYSTEM ARCHITECTURE

We take a sample image and data (text) that need to hidden inside image and send them into the encryption algorithm then we get n stereo image giving that as input to the decryption algorithm we get the decrypted text and image.



CHAPTER – 4
SYSTEM IMPLEMENTATION

4.1 DCT IMPLEMENTATION

DCT Based Steganography Algorithm to embed text message:

```
    Step 1: Read cover image.
    Step 2: Read secret message and convert it in binary.
    Step 3: The cover image is broken into 8×8 block of pixels.
    Step 4: Working from left to right, top to bottom subtract128 in each block of pixels.
    Step 5: DCT is applied to each block.
    Step 6: Each block is compressed through quantization table.
    Step 7: Calculate LSB of each DC coefficient and replace with each bit of secret message.
    Step 8: Write stego image.
```

Algorithm to retrieve text message:

```
    Step 1: Read stego image.
    Step 2: Stego image is broken into 8×8 block of pixels.
    Step 3: Working from left to right, top to bottom subtract128 in each block of pixels.
    Step 4: DCT is applied to each block.
    Step 5: Each block is compressed through quantization table.
    Step 6: Calculate LSB of each DC coefficient.
    Step 7: Retrieve and convert each 8 bit into character
```

4.2 LSB IMPLEMENTATION

LSB Based Steganography Algorithm to embed text message:-

```
    Step 1: Read the cover image and text message which is to be hidden in the cover image.
    Step 2: Convert text message in binary.
    Step 3: Calculate LSB of each pixel of cover image.
    Step 4: Replace LSB of cover image with each bit of secret message one by one
    Step 5: Write stego image
```

Algorithm to retrieve text message:-

```
    Step 1: Read the stego image.
    Step 2: Calculate LSB of each pixel of stego image.
    Step 3: Retrieve bits and convert each 8 bits into character.
```

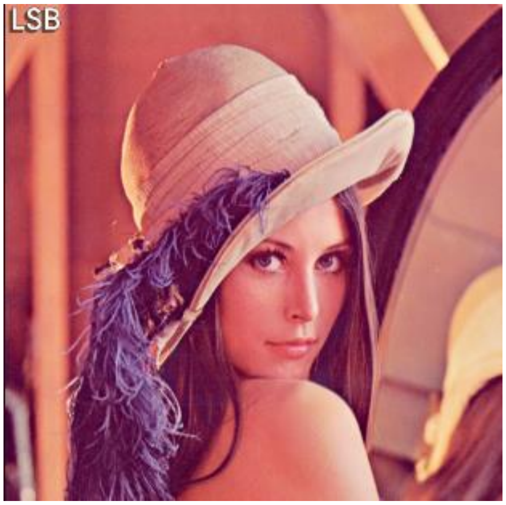
CHAPTER – 5

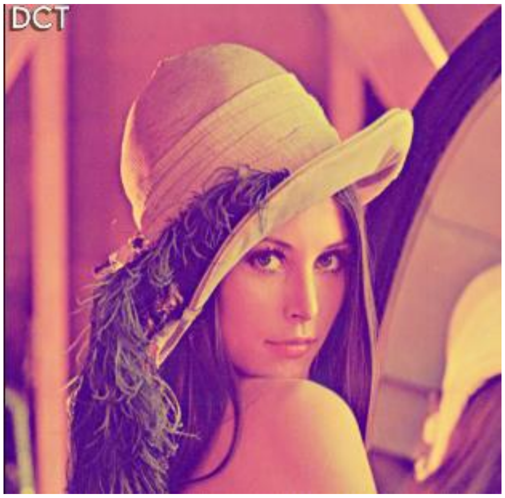
SYSTEM TESTING AND RESULTS ANALYSIS

TEST CASE 1 :

Input:

Output:

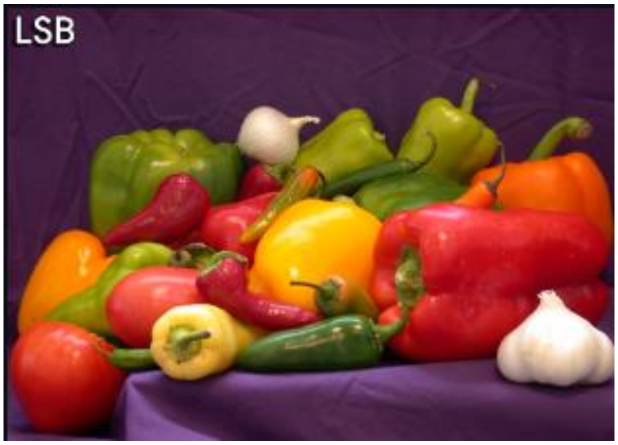


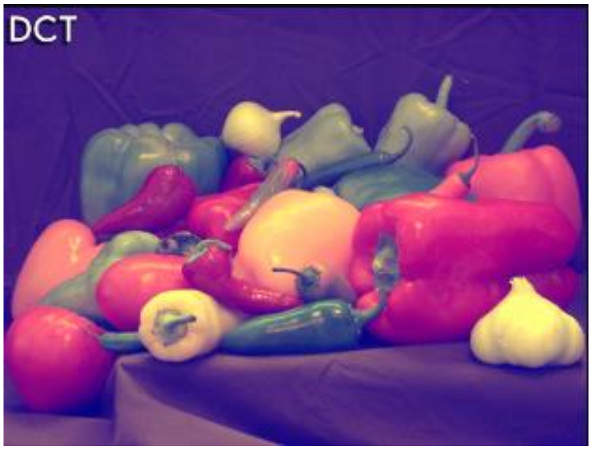


TEST CASE 2 :

Input:

Output:

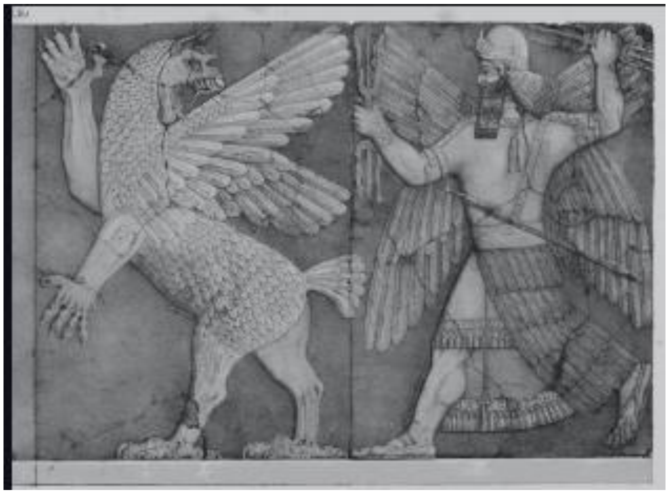


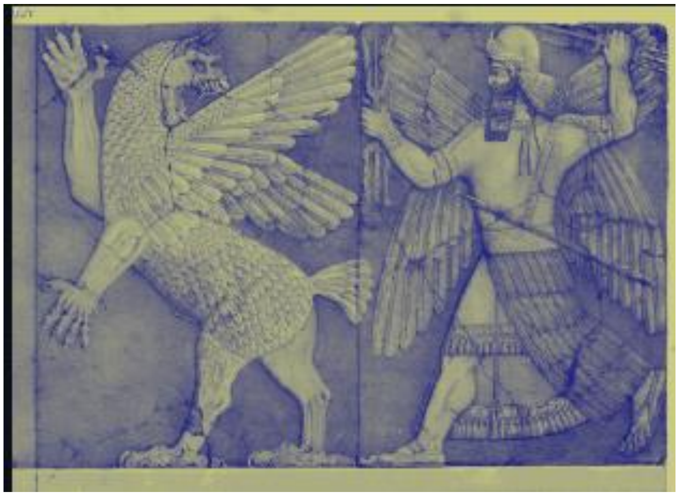


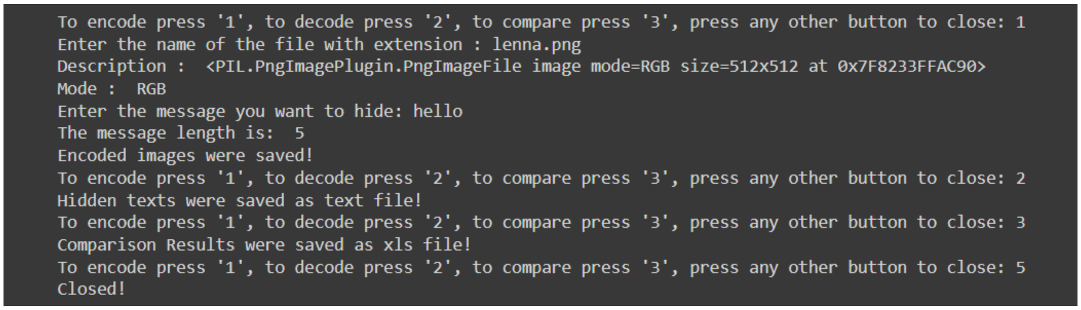
TEST CASE 3:

Input:

Output:

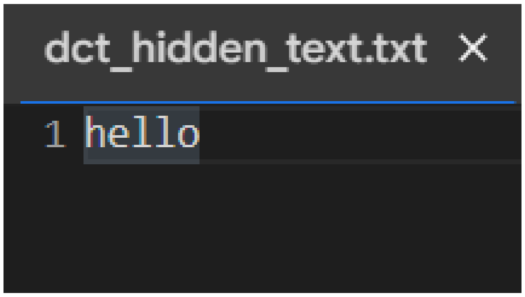




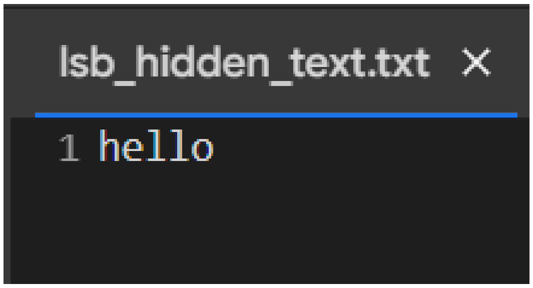


```
To encode press '1', to decode press '2', to compare press '3', press any other button to close: 1
Enter the name of the file with extension : lenna.png
Description :  <PIL.PngImagePlugin.PngImageFile image mode=RGB size=512x512 at 0x7F8233FFAC90>
Mode :  RGB
Enter the message you want to hide: hello
The message length is:  5
Encoded images were saved!
To encode press '1', to decode press '2', to compare press '3', press any other button to close: 2
Hidden texts were saved as text file!
To encode press '1', to decode press '2', to compare press '3', press any other button to close: 3
Comparison Results were saved as xls file!
To encode press '1', to decode press '2', to compare press '3', press any other button to close: 5
Closed!
```

This is the menu after running the code where we can give input text and get encrypted image and also decrypted image with text now, we can see the results after decryption from images using both the algorithms

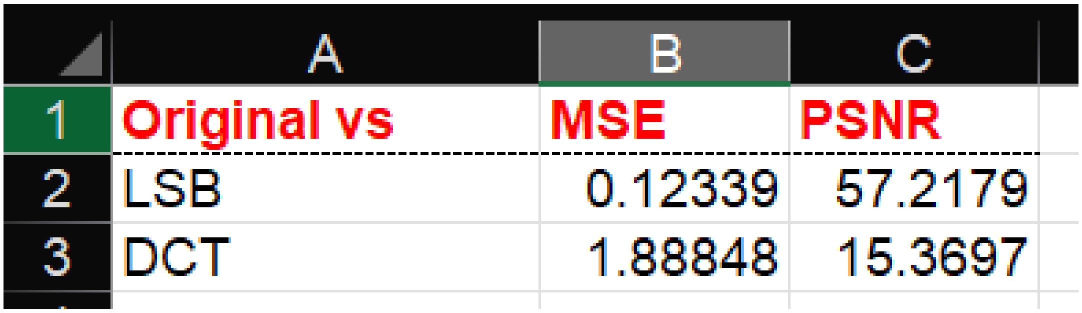


```
1 hello
```



```
1 hello
```

Comparison result of both algorithm and their MSE AND PSNR values



	A	B	C
1	Original vs	MSE	PSNR
2	LSB	0.12339	57.2179
3	DCT	1.88848	15.3697

CHAPTER – 6

CONCLUSION AND FUTURE SCOPE

- This project discusses in detail about the LSB and DCT algorithms on steganography application. The LSB and DCT algorithms are implemented for steganography application. In this experiment, performance analysis of LSB and DCT methods are successfully completed, and experimental results are discussed.
- We have kept the DWT implementation for future work.
- The MSE and PSNR values are compared for the LSB and DCT algorithms. From the experiment results it is observed that the PSNR of DCT is high as compared to the other two algorithms.
- Thus, the experiment concludes the DCT algorithm is more suitable for the steganography application compared to the LSB based algorithms.

REFERENCES

[1] Saravanan Chandran, Koushik Bhattacharyya, “Performance Analysis of LSB, DCT, and DWT for Digital Watermarking Application using Steganography” - International Conference on Electrical, Electronics, Signals, Communication and Optimization (EESCO) - 2015.

[2] Gurmeet Kaurand Aarti Kochhar, “A Steganography Implementation based on LSB & DCT”, “International Journal for Science and Emerging, Technologies with Latest Trends” 4(1), ISSN No. (Online):2250-3641, ISSN No. (Print): 2277-8136, 35-41 (2012).

[3] Zakir khan, “What is the PSNR ratio value for steganography image?”, available at the following link: https://www.researchgate.net/post/What_is_the_PSNR_ratio_value_for_steganography_image

[4] Krasimir Kordov and Borislav Stoyanov, “Least Significant Bit Steganography using Hitzl-Zele Chaotic Map”, - INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2017, VOL. 63, NO. 4, PP. 417–422

[5] Neivin Mathew, Robyn Rintjema and Steven Kalapos, “Comparison of Image Steganography Techniques (DCT vs LSB)”