Algorithm for Secure Online Message Transmission

Project report submitted to Indian Institute of Information Technology, Nagpur, in partial fulfilment of the requirements for the Award of Degree of

Bachelor of Technology
in
Computer Science and Engineering

by

Divyesh Saglani
BT16CSE004

Under the guidance of

Dr. Nishat A. Ansari
Assistant Professor
Computer Science and Engineering
Indian Institute of Information Technology, Nagpur

Department of Computer Science and Engineering
INDIAN INSTITUTE OF INFORMATION TECHNOLOGY, NAGPUR
2020

Algorithm for Secure Online Message Transmission

Project report submitted to Indian Institute of Information Technology, Nagpur, in partial fulfilment of the requirements for the Award of Degree of

Bachelor of Technology
in
Computer Science and Engineering

by

Divyesh Saglani
BT16CSE004

Under the guidance of

Dr. Nishat A. Ansari
Assistant Professor
Computer Science and Engineering
Indian Institute of Information Technology, Nagpur

Department of Computer Science and Engineering
INDIAN INSTITUTE OF INFORMATION TECHNOLOGY NAGPUR
2020

Department of Computer Science and Engineering

Indian Institute of Information Technology Nagpur

Declaration

I, **Divyesh Saglani**, hereby declare that this project work titled ***"Algorithm for secure online media transmission (SOMeT)"*** is carried out by me in the **Department of Computer Science and Engineering** of **Indian Institute of Information Technology, Nagpur**. This work is original and has not been submitted earlier whole or in part for the award of any degree/diploma at this or any other Institution/University.

Date:

22nd June, 2020

Name:

Divyesh Saglani

BT16CSE004

Declaration

I, **Divyesh Saglani**, with Enrolment Number (**BT16CSE004**) understand that plagiarism is defined as any one or the combination of the following:

1. Uncredited verbatim copying of individual sentences, paragraphs or illustrations(such as graphs, diagrams, etc.) from any source, published or unpublished, including the internet.
2. Uncredited improper paraphrasing of pages or paragraphs (changing a few words or phrases, or rearranging the original sentence order)
3. Credited verbatim copying of a major portion of a paper(or thesis chapter) without clear delineation of who did or wrote what(Source: IEEE, the institute, Dec. 2004).

I have made sure that all the ideas, expressions, graphs, diagrams, etc. that are not a result of my own work, are properly credited. Long phrases or sentences that had to be used verbatim from published literature have been clearly identified using quotation marks.

I affirm that no portion of my work can be considered as plagiarism and I take full responsibility if such compliant occurs. I understand fully well the guide of the thesis may not be in a position to check for possibility of such incidences of plagiarism in this body of work.

Date:

22nd June, 2020

Name:

Divyesh Saglani

BT16CSE004

Computer Science and Engineering

IIIT Nagpur

भारतीय सूचना प्रौद्योगिकी संस्थान, नागपुर
INDIAN INSTITUTE OF INFORMATION TECHNOLOGY, NAGPUR
"An Institution of National Importance by an Act of Parliament"
RTTC, BSNL Near TV Tower, Beside Balaji Temple, Seminary Hills, Nagpur - 440 006
Website: www.iiitn.ac.in, Email: director@iiitn.ac.in, registrar@iiitn.ac.in Phone: 0712 - 2985010

Thesis Approval Certificate

This is to certify that the project titled **"Algorithm for Secure Online Message Transmission(SOMeT)"** is submitted by ***Divyesh Saglani*** with enrollment number **BT16CSE004** in partial fulfillment of the requirements for the award of the degree of **Bachelor of Technology in Computer Science and Engineering, IIIT Nagpur**. The work is comprehensive, complete and fit for final evaluation.

Date:

22nd June, 2020

Name:

Dr. Nishat Ansari
Assistant Professor
Computer Science and Engineering
IIIT Nagpur

Name:

Dr. Pooja Jain
Head of Department
Computer Science and Engineering
IIIT Nagpur

Acknowledgements

This thesis is the result of six months of rigorous work during which several people have played a crucial work in its completion. Its a great pleasure that now I have the opportunity to express my gratitude to all of them.

First and Foremost, I would like to thank ***Indian institute of Information Technology Nagpur (IIITN)*** for giving us chance of doing this **Final Year B.Tech Project** in such a friendly and learning environment.

I take this opportunity to express my heartfelt gratitude and indebtedness to my respected guide ***Dr. Nishat Ansari***, Assistant Professor, Department of Computer Science and Engineering, IIIT Nagpur who constantly motivated, supported, encouraged and guided me throughout the project. Her invaluable guidance and continuous help in every aspect enabled me to complete my thesis.

I take my deep sense of gratitude and reverence to ***Dr. Pooja Jain***, Head of Department, Computer Science and Engineering, IIIT Nagpur, for providing me requisite opportunities for this project.

I am highly thankful to ***Dr. O.G. Kakde***, Director, IIIT Nagpur and ***Dr. Ashwin Kothari***, Associate Dean, IIIT Nagpur for providing all facilities and infrastructure and supporting me morally and technically during my B.Tech academic program.

Above all, I bow my head in front of the Great Almighty, the author of knowledge and wisdom, for his countless love and for giving me strength to make my project successful.

I further avail this profound privilege to optimize my deepest sense of gratitude to all faculty members of IIIT Nagpur, friends, colleagues and relatives for their immense guidance and help during my B.Tech Course.

Thank you all for your esteemed support.

Divyesh Saglani

Abstract

The increase use of technologies and computers have benefited human race in many ways, but have also raised several security concerns. Some of these concerns are related to the data transferred over Internet. Sending normal messages over Internet is no longer secure method for data sharing as it may result in messages being breached and even compromised.

To ensure security, messages are now-a-days often hidden in digital content, like images, videos, gifs, etc using Steganography techniques and then transferred over net so it does not seem nondescript from outside.

To ensure more security, the messages are first encrypted using some Cryptographic algorithm and to ensure more security.

In this thesis on Secure Online Message Transmission(**SOMeT**), implementation of above idea done. Four different cryptographic algorithms (DES, AES, RSA and OTP) were combine with two different steganographic algorithms (LSB and OTP) for RGB and RGBA images. To compare the images after applying the algorithm, the Mean Square Error(MSE) and Peak Signal to Noise Ratio(PSNR) techniques were used. MSE is used to find error between the original image and the image obtained after applying the algorithm. Similarly, PSNR is used to measure quality of Stego image.

A comparative analysis was done between all combinations of above mentioned steganographic techniques with cryptographic techniques and some good observations were made through graph plotting.

Contents

List of Tables

List of Figures

List of Abbreviations and Symbols

OTP	One Time Pad
DES	Data Encryption Standard
AES	Advance Encryption Standard
DCT	Discrete Cosine Transformation
LSB	Least Significant Bit
MSE	Mean Square Error
PSNR	Peak Signal to Noise Ratio
IP	Initial Permutation
FP	Final Permutation
Stego-Tech	Steganography Technique
Enc-Tech	Encryption Technique
SOMeT	Secure Online Message Transmission
GUI	Graphical User Interface

cos	Cosine function
π	Pi in Maths, i.e. 180 degree

1 | Introduction

Internet usage is increasing rapidly these days, and sending data over internet requires privacy, which can be achieved by normal cryptographic algorithms, but due to the availability of high performance computers, parallel computing and resources available on the cloud, decoding some cryptographic algorithm by breaking into a system, although is a difficult task, but still possible.

The messages become more vulnerable if they are of the highest priority and the encrypted message makes it more susceptible to attacks. Thus, information security and confidentiality are very important and become more and more necessary. This issue has been worked upon, and it has been found that Steganography, Cryptography and Watermarking are some techniques to overcome these issues[1].

Steganography is a technique of concealing a digital content, like a file, message, image or video, within another digital content. The advantage of steganography is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how unbreakable they are, arouse interest and may in themselves be incriminating in countries in which encryption is illegal[2]. Steganography is concerned both with concealing the fact that a secret message is being sent and its contents.

Steganography in digital domain can be done in mainly two domains, spatial and frequency. In spatial domain, the message is directly inserted into pixels of the cover image, like using method of Least Significant Bit(LSB). The frequency domain consists of transformations like Fast Fourier Transform (FFT), Discrete Cosine Transform(DCT), Discrete Wavelet Transform(DWT) etc.

Cryptography technique of message encoding involves the message being encrypted and decrypted using a secret key. This encoded message is not understandable to one who intercepts the message unless he/she has the secret key. This keeps message secure from external attacks.

The cryptographic technique for message encoding consists are of two types, symmetric key cryptogrpahy, like Data Encryption Standard(DES), Advanced Encryption Standard(AES), One Time Pad(OTP), etc. and asymmetric key cryptography, like RSA, ElGamal Encryption, etc.

1.1 Problem Statement

Although some cryptographic algorithms are enough to provide message security, but they cannot guarantee the perfect message sharing as the messages may be tampered to avoid correct message revival at other end. Also, Steganography alone is also not found sufficient to send high confidential messages. Thus an idea of using Cryptography along with Steganography has been proposed by researchers and a lot of work is currently being done in this topic.

This thesis also tries to implement the above idea along with adding a comparison feature which compares different algorithms used. This thesis takes idea from an already existing paper on Secure Image Steganography[3] and LSB Steganography using DES [4]. Main Contribution in this thesis is that it takes two different steganographic algorithms, combines with four different cryptographic algorithms and compares the performance of the combination of technique used, makes useful algorithms on technique used and plots graph for the measuring parameters.

This thesis uses two Steganographic algorithms, namely Least Significant Bit(LSB), in spatial domain and Discrete Cosine Transform(DCT), in frequency domain, and four different Cryptographic Algorithms, namely, One Time Pad (OTP), Data Encryption Standard (DES) , Advance Encryption Standard (AES), symmetric key cryptography, and RSA, asymmetric key cryptography.

Measuring parameters for performance evaluation of the steganographic technique used is Mean Square Error(MSE) and Peak Signal to Noise Ratio(PSNR) and the message obtained is compared with original message. The message to be embedded is taken in text format.

1.2 Aim and Scope

In this world of high competition, everyone in the race wants to come first by either using fair or unfair means. The unfair means that one uses can be extremely harmful to people dedicatedly working towards something. To ensure safe transfer of messages over internet without anyone intercepting the message and tampering it, these methods have been proposed. Different methods have been proposed by different researches, which were found to be effective, it is important that these methods be compared to find which is the best one available for use (although each method has it own advantages and disadvantages).

1.3 Organization of Thesis

The thesis is organised in following order. Chapter 1 contains a brief introduction to the topic and gives idea on the problem statement. Chapter 2 describes in brief the previous work done on the topic. Chapter 3 is divided into two section, Steganography and Cryptography. It gives an insight on Basics of Main Concepts used for SOMeT. It gives basic definitions of concepts as well as gives some mathematical equations and tables used while implementing SOMeT.

Chapter 4 is the gives idea of how SOMeT was used for implementation. This chapter has flowcharts that were used for implementing SOMeT. Chapter 5 describes about Implementation of SOMeT. It has details about platform used, process of implementation and results obtained by applying implementation strategies.

Chapter 6 draws conclusion from results obtained. It also has some observations made while implementing the project and tells about the future of project, what can be added or changed for improvement of project. Last chapter has some of the References used while implementing the project.

2 | Literature Review

Some works have recently been published on using Steganography and Cryptography together for message transfer over internet. The previous research work of [3], [5], [6], [7], [4] have all combined Steganography with Cryptography. Each paper uses a different combination and of the steganography and cryptography algorithm, with each having its own advantages.

The research works done in [3], [5],[6] and [7] uses Discrete Cosine Transformation(DCT) Technique for Image Steganography but each uses different Cryptographic Algorithm. Research Paper [5] uses Arnold Transformation to scramble the message, whereas [6] uses Blowfish Algorithm to do the same and [7] uses RSA Algorithm for message encryption. Paper [3] uses OTP Encryption Technique for encoding the message.

2.1 Discrete Cosine Transform Domain

Research Paper [3] has proposed a combination of steganography with DCT and OTP encryption. This system encrypts a secret message before embedding in digital imagery. Based on the evaluation of the proposed algorithm produces an image that is identical to the cover image, this is evidenced by the value of PSNR and MSE are relatively excellent, as well as a perfect extraction. They get their average PSNR value as 51.1225 and average MSE value as 0.50232 and Normalized Cross Correlation (NCC) value as 1 using .bmp extension images. The message encrypted used was in image form. They also applied JPEG compression and mid filter on Images and found out NCC for correspoding images. Average NCC value obtained was 0.8159.

In another research work done[5], a frequency domain approach of Image Steganography has been proposed. Here first the message image is preprocessed by Arnold Transform to scramble it then Discrete Cosine Transform is used to get frequency domain components and data has been embedded with value comparison of Quantization Matrix. This proposed algorithm has shown very goood result in visual analysis as well as numerical analysis i.e. calculation of PSNR and Structural Similarity(SSIM). The average PSNR obtained was 47.27 and average SSIM obtained

was 0.876

In another research paper[7], a DCT-steganography based on encryption is proposed. To provide high security steganography and cryptography are combined together. This system encrypts secret information before embedding in the image. Steganography uses RSA algorithm for encryption and decryption. According to the simulation results, the stego images of our proposed algorithm are almost identical to the cover images and it is very difficult to differentiate between them. Better PSNR values will get when compared with LSB steganography with Huffman coding. Experimental results shows high PSNR values obtained when the size of secret image is less compared to the size of cover image. This paper has used different images of different sizes. The average PSNR value obtained was 55.7385.

2.2 Discrete Wavelet Transform Domain

Ketan Shah et al [8] in their research, the most important thing is the confidentiality and privacy of the information itself. Use of Data Encryption Standard (DES) as a process to handle the confidentiality and use of steganography using Discrete Wavelet Transform (DWT) as a process to handle the privacy of information. Messages that have been encrypted using Data Encryption Standard (DES) are then inserted into the cover (24- bit digital image format * .jpeg) as cover using Discrete Wavelet Transform (DWT) steganography method to generate stego image. From the performance test results shown that the value of Peak Signal to Noise Ratio (PSNR) from image-stego image produces a high value even after the image experienced some type of attack.

2.3 Least Significant Bit Domain

While the above-mentioned papers have used Discrete Cosine Transformation Technique, paper[4] uses Least Significant Bit Technique for Image Steganography. Moreover for message encoding, this paper uses Data Encryption Standard(DES) technique. The method that they have proposed, which combines DES encryption and LSB based canny algorithm generated a good quality of stego images. This method embedded a secret image, which has been encrypted using DES algorithm. After that, the encrypted image was inserted into edges area of the object in a cover image using LSB algorithm. Experiment result was tested using PSNR and MSE, which generated best PSNR value 72.2698 dB; it also generated average PSNR value, which is equal to 72.21584 dB. All stego images have PSNR value above 40 dB that indicated imperceptible stego images and good quality of stego images.

In another research [9], the combination of steganography and cryptography in the research is to be used for data security. Grayscale image or color image can be used as cover. The used of bit matching techniques makes the process of matching the color bits will take a short time when using a cover image that has a lot of color variations. Adding noise to the stego image makes some messages changes. Damage occurs due to the addition of salt and paper noise from MSE 0.0067 and damage when the addition of Gaussian noise occurs starting from MSE 0.00234.

2.4 Other related Researches

Furthermore, research conducted by Sachin Mungmode et al. [10] used Edge Adaptive Steganography method based on Threshold Value and Least Significant Bit Matching Revisited (LSBMR) method. From these studies, the high Peak Signal to Noise Ratio (PSNR) value is about 90 dB (Canny = 94 dB, Sobel = 94 dB, Threshold = 94.1 dB) with message length inserted along 400 bits.

Other research [11] used Canny Edge Detection to determine the location of message insertion. The location has been previously randomized using the Hash function, and then the message is inserted. From the results of this study concluded that the use of cover with high edge areas has high Peak Signal to Noise Ratio (PSNR) value (41.5895 dB) and it had the ability to store large messages when compared with another cover which has low edge areas (PSNR 39.3610 dB and PSNR 38.6527 dB). The constant use of the Hash function also makes it more difficult for an attacker to extract messages from the stegoimage.

Moreover, the experiment [12] compared some edge detection techniques combined with Least Significant Bit (LSB) in the ability to store messages (payload). Edge detection techniques have been compared are Robert, Laplace, Prewitt, Sobel, and Canny. From the results of this study, it was found that Canny edge detection technique has the ability to store large messages (high payload) compared to the other techniques, and this technique is very suitable in image steganography.

Each algorithm has its own advantages and disadvantages. Continuous research work is still going on for improving this technique to provide more stability and higher security.

3 | Techniques used in SOMeT

3.1 Steganography

Steganography in digital domain can be done in mainly two domains, spatial and frequency. In spatial domain, the message is directly inserted into pixels of the cover image, like using method of Least Significant Bit(LSB). The frequency domain consists of transformations like Fast Fourier Transform (FFT), Discrete Cosine Transform(DCT), Discrete Wavelet Transform(DWT) etc. The two steganographic techniques that were used in this thesis were:

3.1.1 Discrete Cosine Transform (DCT)

DCT in digital Image processing is done by dividing the images into small pieces or sub-block with standard size 8x8 pixels[13]. The results of transformation of 8x8 pixel sub-blocks will generate 64 coefficients which consist of a DC coefficient and 63 AC coefficients[3]. Say input image A is NxM. C(i,j) is the intensity of of pixel in row i and column j of image A. F(u,v) is the DCT coefficient in row k1 and column k2 of the DCT matrix. For most images, much of the signal energy lies at low frequencies appearing in upper left corner of DCT. Compression is achieved since the lower right values represent higher frequencies, and are often small - small enough to be neglected with little visible distortion. The DCT input is an 8 by 8 array of integers. This array contains each pixel's gray scale level[14]. The equation for DCT encoding is given as follows:

$$F_{u,v} = \alpha_u.\alpha_v.\sum_{i=0}^{N-1}\sum_{j=0}^{M-1} \cos\frac{u.\pi(2.i+1)}{2.N}.\cos\frac{v.\pi(2.j+1)}{2.M}.C_{i,j} \tag{3.1}$$

where,

$0 \leq u \leq N - 1$
$0 \leq v \leq M - 1$

$$\alpha_u = \begin{cases} \frac{1}{\sqrt{N}} & u = 0 \\ \sqrt{\frac{2}{N}} & 1 \leq u \leq \text{N-1} \end{cases} \tag{3.2}$$

$$\alpha_v = \begin{cases} \frac{1}{\sqrt{M}} & v = 0 \\ \sqrt{\frac{2}{M}} & 1 \leq v \leq \text{M-1} \end{cases} \tag{3.3}$$

3.1.2 Least Significant Bit(LSB)

LSB is a simple approach to embed information in an image. It is a steganography technique of spatial domain where messages are directly inserted into pixel of cover image[9]. This method has good imperceptible value and hence image changes cannot be detected by naked eye. The insertion is done by changing the LSB bit plane of each pixel according to the message bits. An example is shown below.

Say a Cover Image has 8 pixels and is represented in 8-bit binary form[4] as shown in table 3.1

01100100	01111101	00011101	10000100
11110011	00101010	10101010	11000111

Table 3.1: Pixels of Image in Binary Form

Say the message is 1 byte long and is represented in 8-bit binary form as shown in table 3.2.

10100101

Table 3.2: Message in Binary Form

The stego image formed after embedding Message in table 3.2 inside the Cover Image in 3.1 is shown in table 3.3

The underlined and bold bits in table 3.3 is an LSB that changes based on the message bits. Since only the least significant bit changes in the original pixel column, this change is not visible to naked eye.

01100101	01111100	00011101	10000100
11110010	00101011	10101010	11000111

Table 3.3: Stego Image for LSB

3.2 Cryptography

Cryptography technique of message encoding involves the message being encrypted and decrypted using a secret key. This encoded message is not understandable to one who intercepts the message unless he/she has the secret key. This keeps message secure from external attacks. The cryptographic technique for message encoding consists are of two types, symmetric key cryptography, like Data Encryption Standard(DES), Advanced Encryption Standard(AES), One Time Pad(OTP), etc. and asymmetric key cryptography, like RSA, ElGamal Encryption, etc. Cryptographic techniques used in this thesis were:

3.2.1 One Time Pad (OTP)

One Time Pad or OTP is a symmetric key stream cipher. It is quite popular and often used in many organizations as their encryption technique. OTP is thought of an encryption technique that cannot be cracked. But, for this, it requires a one-time pre-shared key (key should not be used again), the same size as or longer than the message being sent. The plain text is paired with random key resulting in the encrypted text. The plain text and the key are paired together using modular addition operation (XOR operation). OTP can be considered as a perfect cipher if it follows the given condition:

1. Key is truly random
2. Key as long as plain text
3. Key never used in whole or in part before
4. Key is completely secret (even while key sharing)

Say M(i) denotes i^{th} bit value In original message text and K(i) denotes i^{th} bit in key string and C(i) denotes i^{th} bit in the corresponding cipher text. Then, the encryption done using OTP Algorithm is given by Equation 3.4 and decryption is is given by Equation 3.5

$$C_i = M_i \oplus K_i \tag{3.4}$$

$$M_i = C_i \oplus K_i \tag{3.5}$$

3.2.2 Data Encryption Standard(DES)

Data Encryption Standard is a symmetric key block cipher. It encrypts 64 bit block of message at a time with 56 bit encryption key to get a 64 bit block of cipher text. The structure for DES is shown in figure[15] 3.1. The DES Encryption Process in

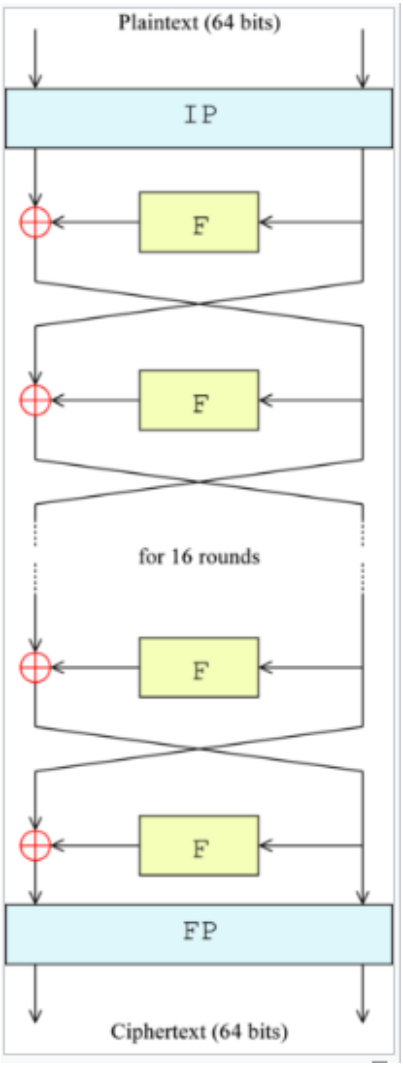

Figure 3.1: DES Structure

total has 16 rounds. In each round a Feistel Cipher is used. In a Feistel network, the block is divided into 2 halves, each of length 32 bits, left one being called L_i and Right one being called R_i where i denotes the i^{th} round. Let f be the feistel or the transformation function and K be the internal key(48 bit key derived from the original key). The algorithm used in each Feistel block is given by equations 3.6 and 3.7. Detail of a round function is shown in figure 3.2[16].

$$L_i = R_{i-1} \tag{3.6}$$

$$R_i = L_{i-1} \oplus f(R_{i-1}) \tag{3.7}$$

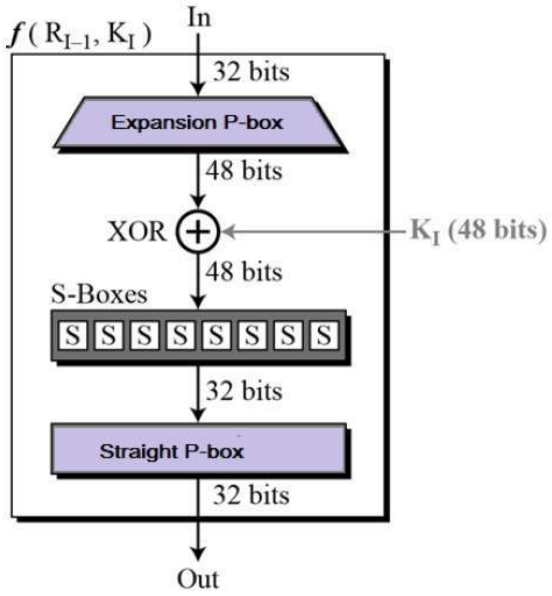

Figure 3.2: DES Round Function

3.2.3 Advance Encryption Standard(AES)

Advance Encryption Standard (AES) is replacement for DES as the key size of DES was small. It is much faster and stronger than DES (as DES was found vulnerable to exhaustive key search). AES is a symmetric key block cipher. It has three variants where each variant has different key size, i.e. 128 bits or 192 bits or 256 bits. AES is based on substitution and permutation network rather than feistel network. AES performs all computations at bytes level and hence 128-bit key is treated as 16 byte key and is divided in four columns and four rows for processing as a matrix. Number of rounds are based upon size of key. They are 10 for 128-bit key, 12 for 192-bit key and 14 for 256-bit key.

Each round uses 128-bit key which is calculated from original AES key[16]. The AES Algorithm is described in figure 3.3. The encryption algorithm for each round process is defined in figure 3.4. Each round has four sub processes. The four processes in order are:

- Byte Substitution
- Shift Rows
- Mix Columns
- Add Round Key

Mix Columns is not performed in last round. Xor Operation is used for round key operation.

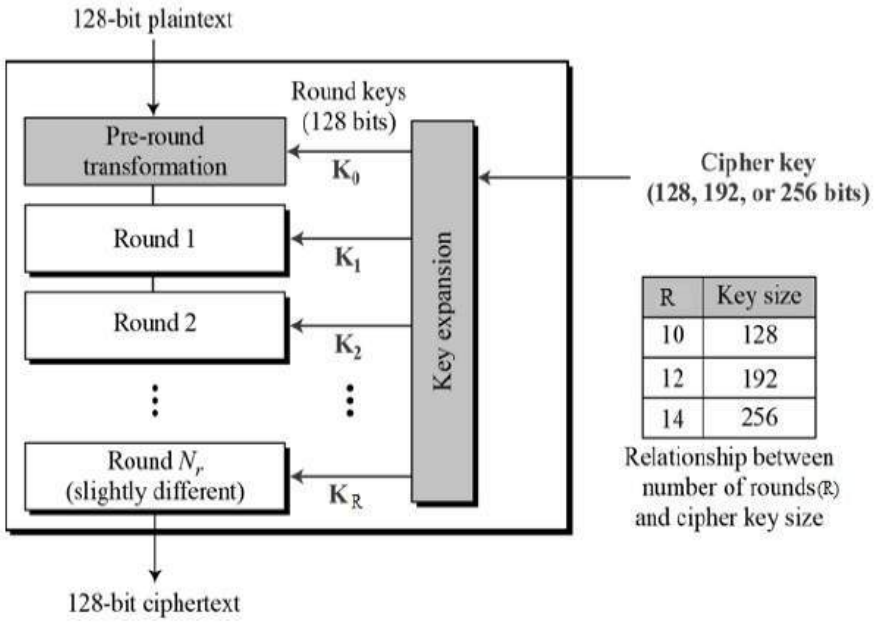

Figure 3.3: AES Structure

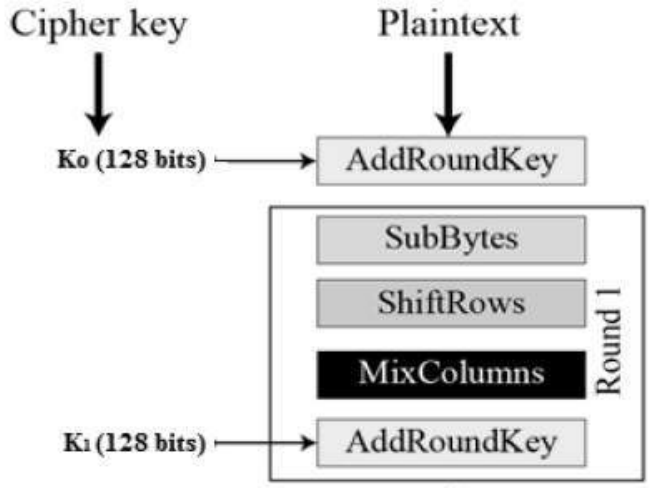

Figure 3.4: AES Round Function

3.2.4 RSA Encryption

RSA(Rivest-Shamir-Adleman) is public key cryptographic technique of encryption and is most common and one of the most secure way of encrypting the data. RSA uses two exponents, e and d, where e is public key and d is private key. Encryption

and decryption uses modular exponentiation. Modular exponentiation is of polynomial speed where as modular logarithm is very hard as no faster algorithm is available yet.

The encryption for a plain text $\boldsymbol{P}$ happens using public key of receiver using equation 3.8 and decryption happens using private key of receiver as shown in equation 3.9. Let $\boldsymbol{C}$ be corresponding cipher text. Since everyone knows the public key, hence the encryption is of polynomial time. Where as only receiver knows the private key and hence for him, the decryption is of polynomial time but for some third party, it is very difficult to decrypt. The reason is shown in figure 3.5 and overall RSA structure is shown in figure 3.6. The key generation for RSA algorithm is shown in Algorithm 1

$$C = P^e \mod n \tag{3.8}$$

$$P = C^d \mod n \tag{3.9}$$

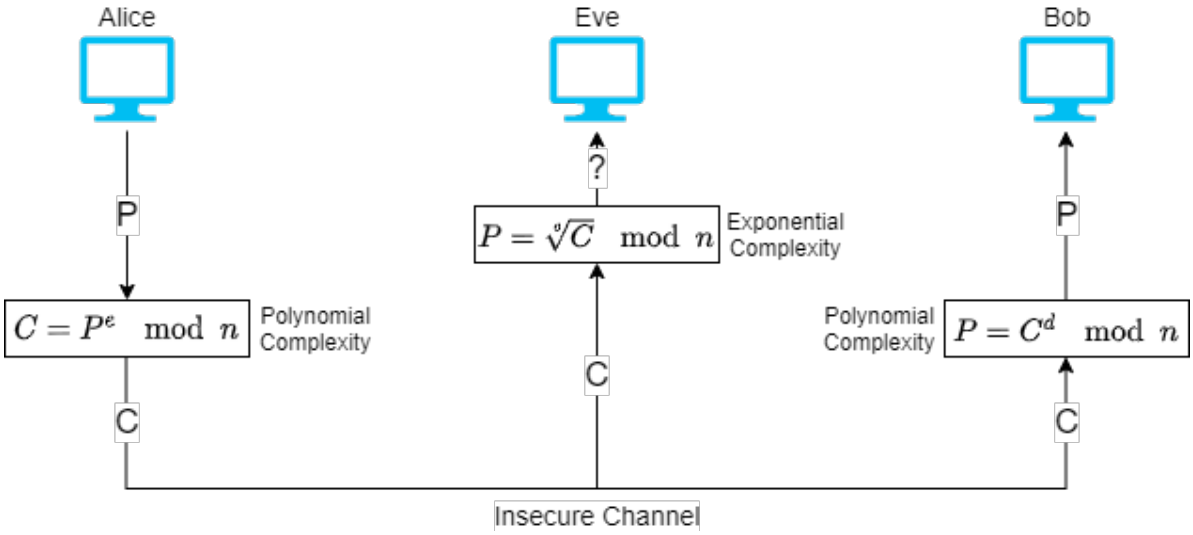

Figure 3.5: Complexity Operations in RSA

Algorithm 1 RSA Algorithm

procedure RSA KEY GENERATION
  select two large primes $\boldsymbol{p}$ and $\boldsymbol{q}$ such that $p \neq q$
  $n \leftarrow p \times q$
  $\Phi(n) \leftarrow (p-1) \times (q-1)$
  select $\boldsymbol{e}$ such that $1 < e < \Phi(n)$ and $\boldsymbol{e}$ is coprime to $\Phi(n)$
  $d \leftarrow e^{-1} \mod \Phi(n)$
  $PublicKey \leftarrow (e, n)$
  $PrivateKey \leftarrow d$
  $Keys = list(PrivateKey, PublicKey)$
  return Keys
end procedure

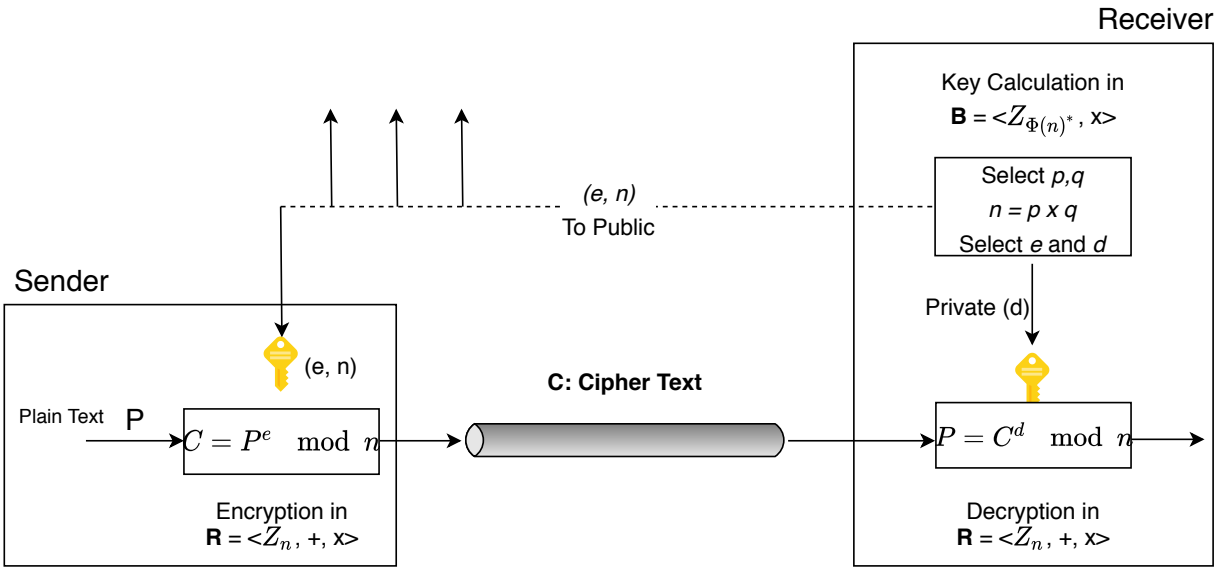

Figure 3.6: RSA Structure

4 | SOMeT Design

Given Below are 2 sub-sections that describes the work done in project. First section gives an overview of Algorithm used using flowchart and second section describes the implementation of project and the measurements used to evaluate the performance of algorithm.

4.1 Algorithm Design

Flowchart of Simple Steganography with Cryptography algorithm is explained using flowchart as shown in figure 4.1. This flowchart involves both encoding and decoding technique[9].

The flowchart shown in figure 4.1 helped in deriving extension models for implementation. Two different algorithms were designed[3], [4]. One used Discrete Cosine Transform Technique for image Steganography and other used Least Significant bit. For different encryption Algorithms were used namely AES, DES, RSA and OTP. Flowchart for DCT encoding with any one of the above-mentioned Encryption Technique is mentioned in figure 4.2 and the flow chart for corresponding decoding is given in figure 4.3.

Edge Detection: A pixel, which has intensity value changes sharply in a digital image, is an edge pixel. Edge detection is used to recognize connected edge pixels. Edge detection is one of the digital image processing that is used to determine the edge of the object contained in the image. The utilized for edge detection in steganography is to improve the imperceptibility value, wherein message insertion is performed on the edge area of the cover image. Changes in pixel values occur only on the edge of the image; therefore, the human eye cannot distinguish it[4].

The encoding and decoding flow charts for using LSB with cryptography are shown in figure 4.4 and figure 4.5 respectively.

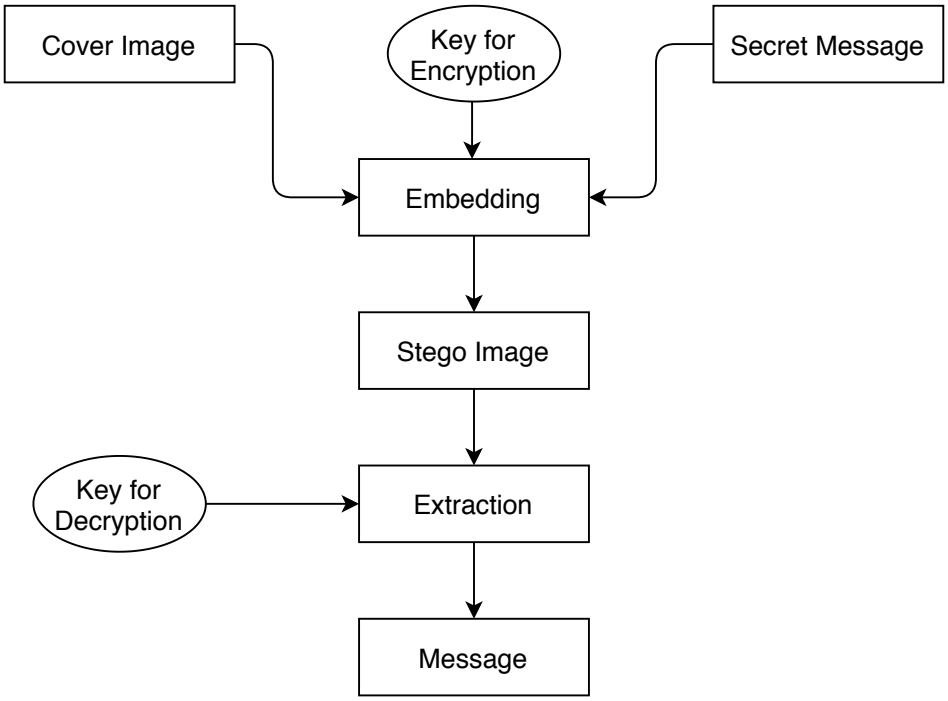

Figure 4.1: Basic Idea of use of Steganography and Cryptography

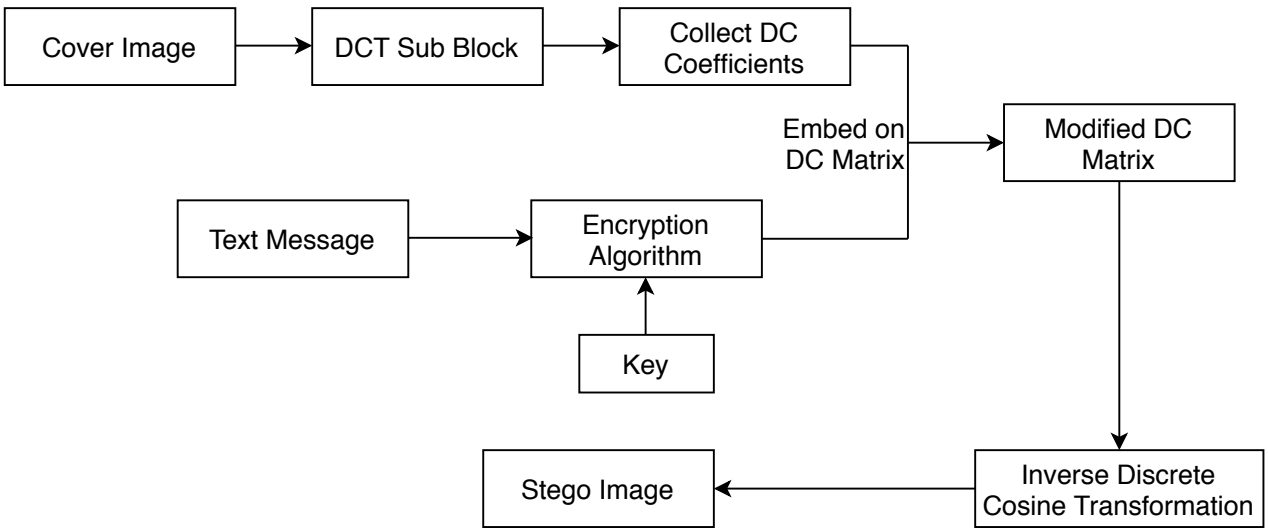

Figure 4.2: Encoding Technique for DCT

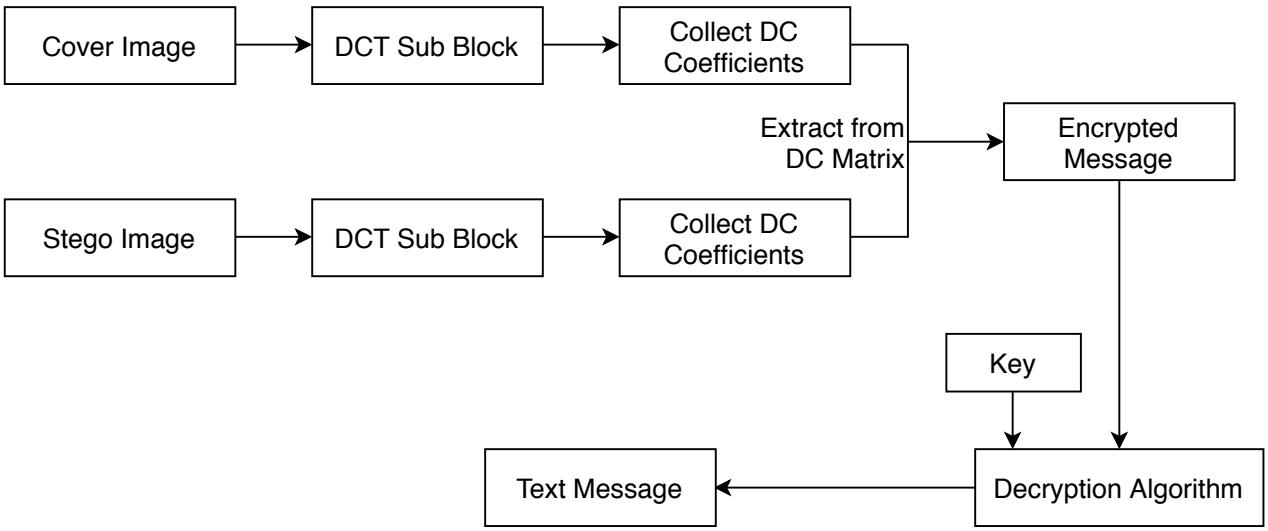

Figure 4.3: Decoding Technique for DCT

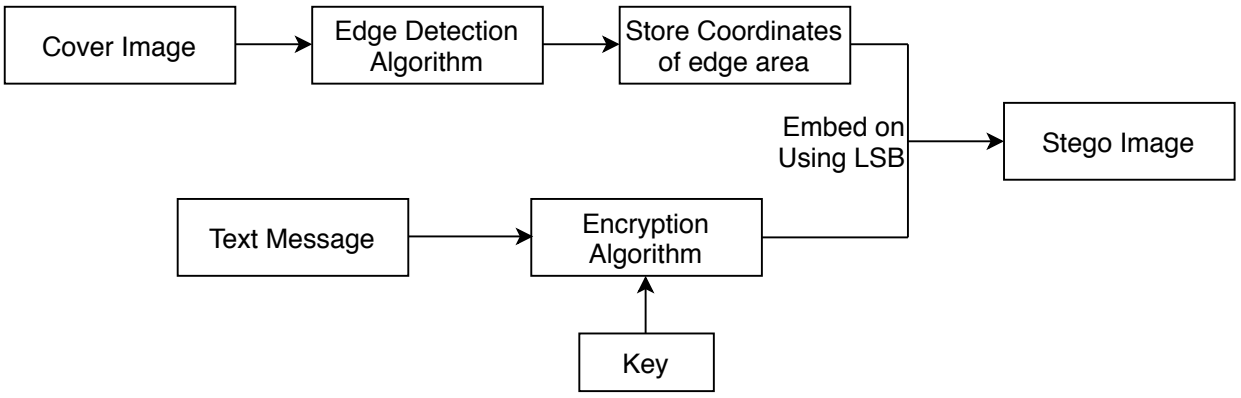

Figure 4.4: Encoding Technique for LSB

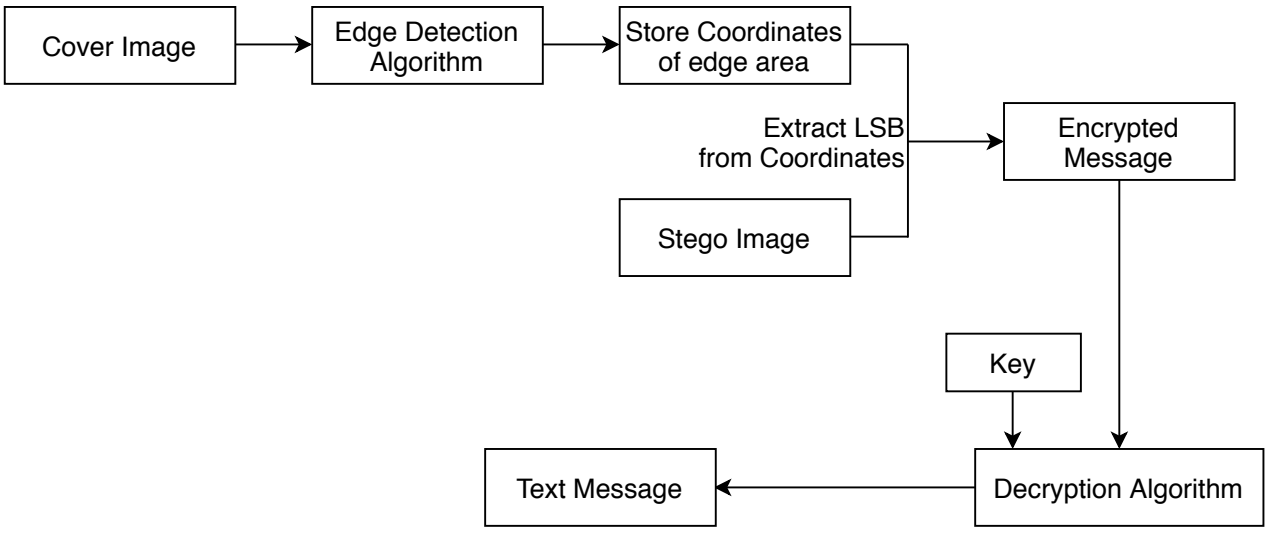

Figure 4.5: Decoding Technique for LSB

5 | Implementation and Performance Evaluation

5.1 Implementation Details

5.1.1 Platform used

To implement the algorithm, a Windows machine with Intel(R) Pentium(R) 2.16 GHz Processor and 4GB RAM was used. The algorithm was coded in Python using Python 3.6 IDLE.

5.1.2 GUI Implementation

A **GUI** was also formed for better interfacing. The GUI was made to combine any one of the 2 Steganographic Techniques(DCT and LSB) with any one of 4 Cryptographic Techniques(DES, AES, OTP and RSA). The feature of comparison of performance measures used to analyse the algorithms. A bar graph was plotted between the average MSE and the algorithm used. Another bar graph was plotted between average PSNR and the algorithm used. This graph helps in better understanding which algorithm is better. The snippets of GUI are shown from Figure 5.1 to Figure 5.5

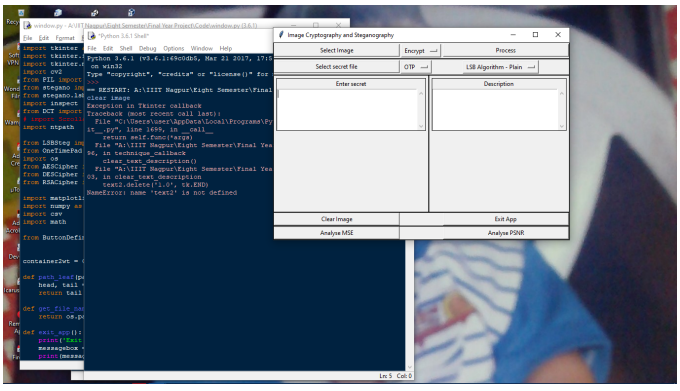

Figure 5.1: GUI for Algorithm

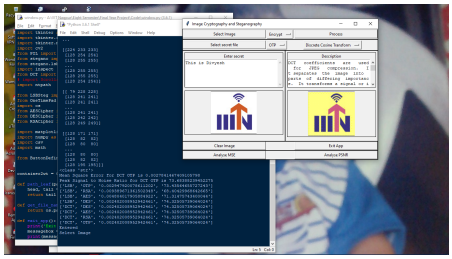

Figure 5.2: Encoding (Part 1)

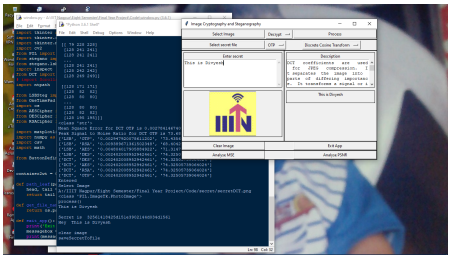

Figure 5.3: Decoding (Part 1)

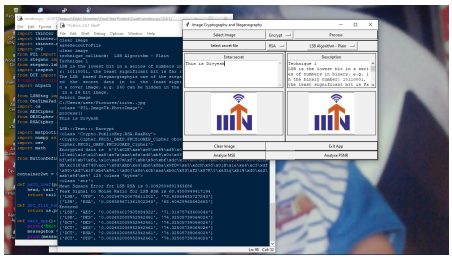

Figure 5.4: Encoding (Part 2)

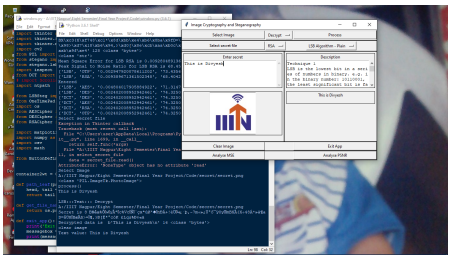

Figure 5.5: Decoding (Part 2)

5.2 Performance Evaluation Parameters

Three parameters were used for evaluation the performance of the Algorithm. These were Mean Square Error(MSE), Peak Signal to Noise Ratio(PSNR) and String Comparison Percentage.

5.2.1 Mean Square Error

The Mean Square Error(MSE) tells how close the output image is to the input image. The error is the difference in the number of estimator with the amount to be estimated. Differences occur due to randomness or because the estimator does not take into account information that can produce more accurate estimates. The smaller the MSE value of an image the better the quality The Mean Square Error(MSE) is calculated using the equation 5.1[3].

$$MSE = \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \sum_{k=0}^{2} \left\| g(i,j,k) - f(i,j,k) \right\|^2 \qquad (5.1)$$

where,

M,N = number of columns and rows in pixel
g(i,j,k) = input image
f(i,j,k) = output image

5.2.2 Peak Signal to Noise Ratio

PSNR are used as a measure of a quality of the reconstructed image. It is most commonly used as a measure of the quality of reconstruction of image watermarking to indicate imperceptibility. Imperceptibility means that the perceived quality of the host image should not be distorted by the watermark[3]. A higher PSNR would indicate that the reconstruction is of higher quality. PSNR is given by equation 5.2

$$PSNR_{DB} = 20.\log_{10}(\frac{255}{\sqrt{MSE}}) \tag{5.2}$$

5.2.3 String Comparison Percentage

Since the message in this project is taken to be in form of text or string, the extracted message can be compared with the original message easily using any of the string compare algorithm or even by naked eye. The formula used in this thesis for string comparison is given by Equations 5.3 and 5.4

$$\alpha_i = \begin{cases} 1 & derivedString[i] == originalString[i] \\ \\ 0 & derivedString[i] \; != originalString[i] \end{cases} \tag{5.3}$$

$$FracOdd = \sum_{i=0}^{strlen-1} \alpha_i \tag{5.4}$$

5.2.4 Images and Message used for Evaluation

The Images shown below were taken and the combination of all Steganography and Cryptography techniques were applied to all the images. And the since the message to be encrypted was in text, string compare algorithm was to used to compare the messages obtained before and after applying the algorithm. The average Mean Square Error(MSE) and Peak Signal to Noise Ratio(PSNR) was calculated know how close the original images were to the images obtained after applying the algorithm. A common secret message was used in all images. The secret message used was:

Divyesh Saglani welcomes you all!

Images used as reference for algorithm are(RGBA and RGB type images) shown from figure 5.6 to figure 5.15. **To encode these images, conventional DCT Algorithm was used in which the message in DCT was encoded in blue pixels for RGB and RGBA images.**

Figure 5.6: ariel.png

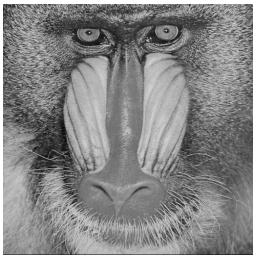

Figure 5.7: baboon.png

Figure 5.8: barbara.png

Figure 5.9: car.png

Figure 5.10: cctv.png

Figure 5.11: cottage.png

Figure 5.12: f16.png

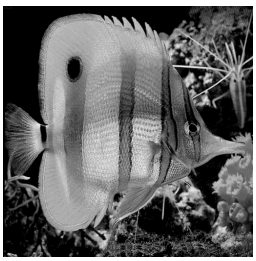

Figure 5.13: fish.png

Average MSE and PSNR was calculated for all combination of algorithm. The data obtained for MSE and PSNR is represented in table 5.2.

The data obtained in table 5.2 was visualized using graph shown in figure 5.16 for Average Mean Square Error and 5.17 for Peak Signal to Noise Ratio. The text

Figure 5.14: iiitn.jpg

Figure 5.15: lena.png

message decoded was compared with original text message and they were found to be same.

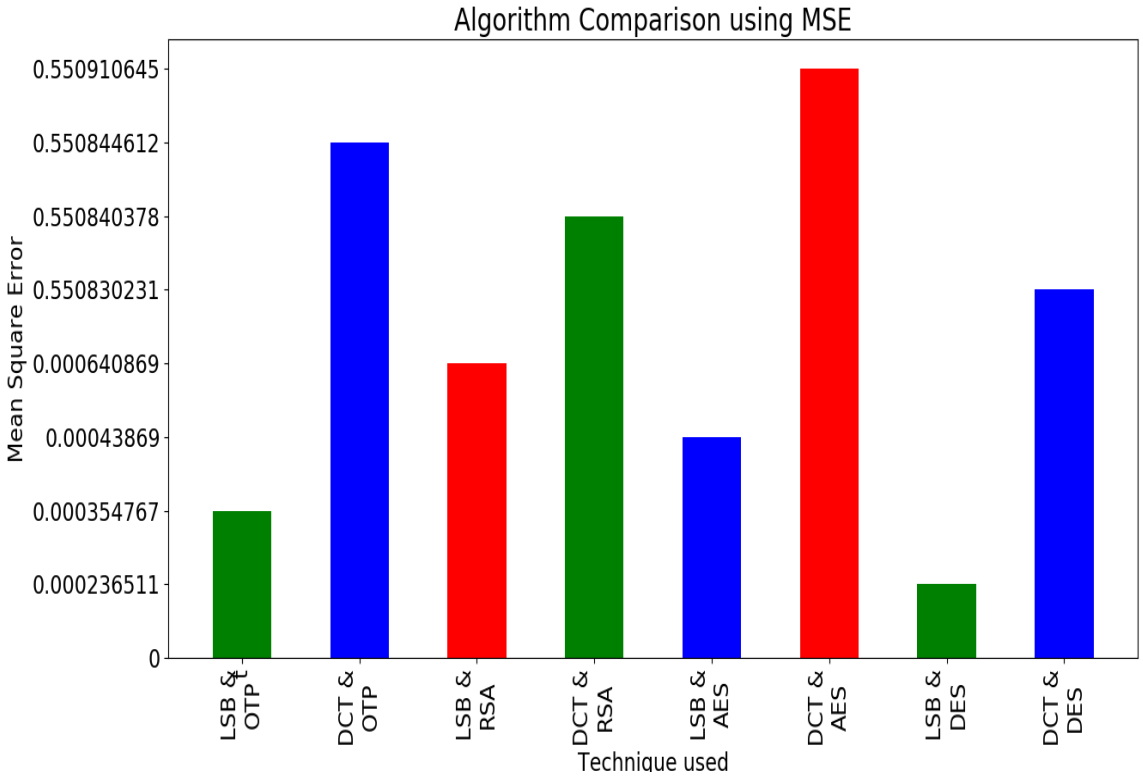

Figure 5.16: Algorithm Comparison using MSE

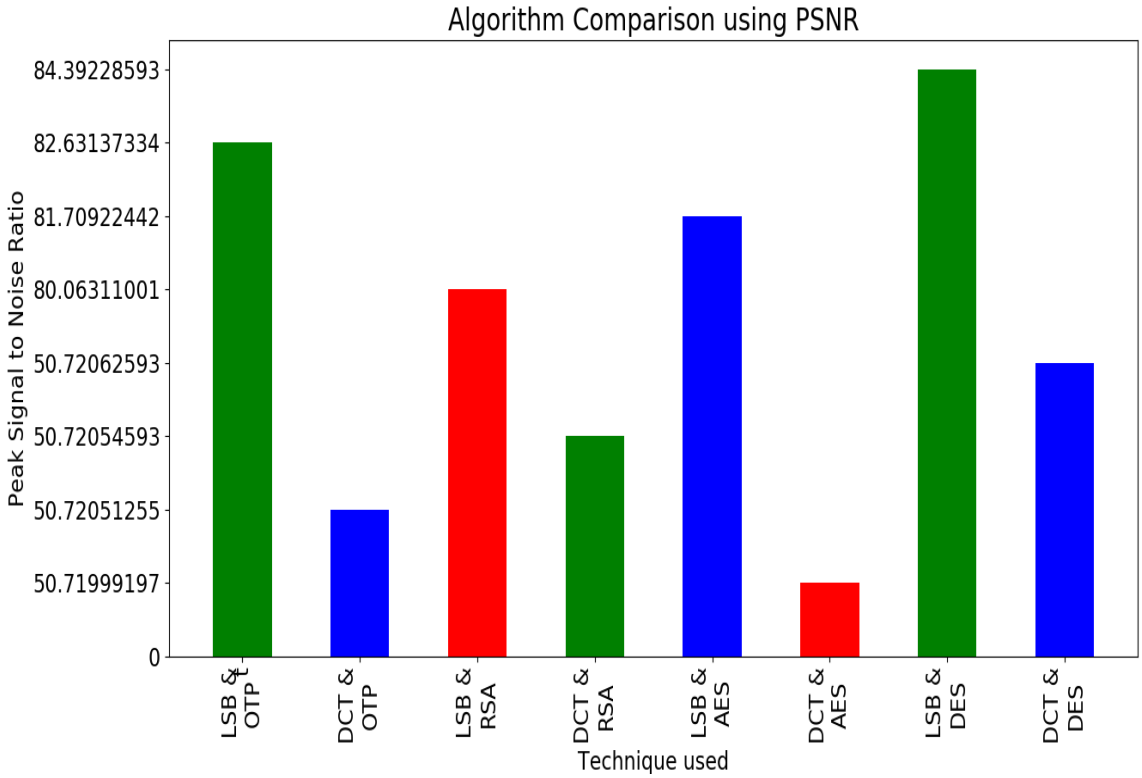

Figure 5.17: Algorithm Comparison using PSNR

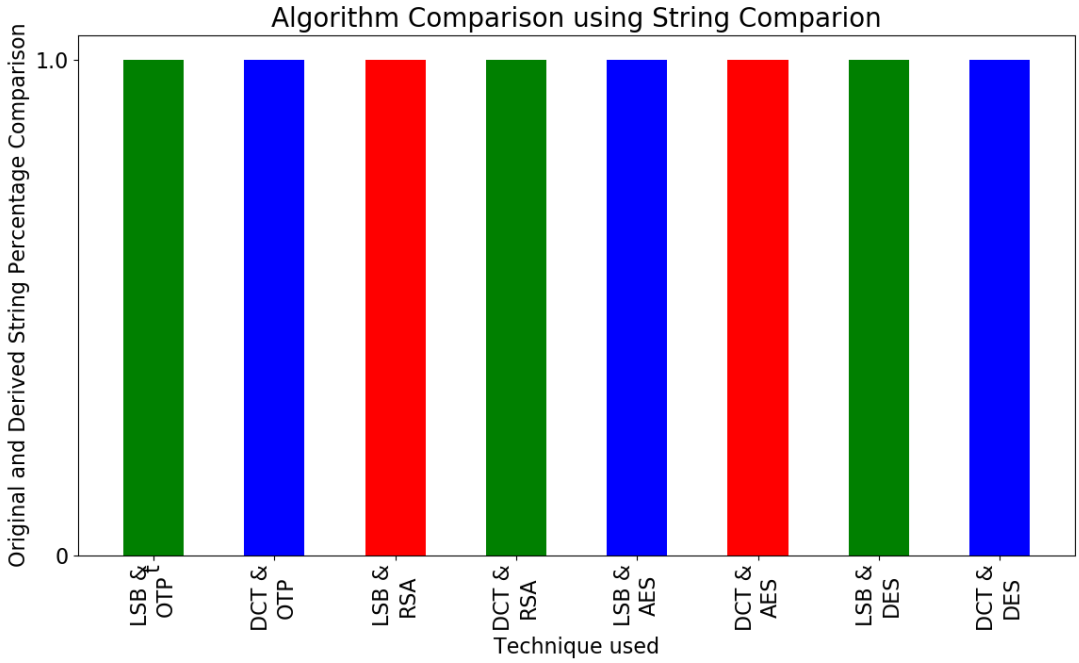

Figure 5.18: Original String and Decoded String Comparison

Stego-Tech	Enc-Tech	String Comparison Percentage(0-1)
LSB	OTP	1
DCT	OTP	1
LSB	RSA	1
DCT	RSA	1
LSB	AES	1
DCT	AES	1
LSB	DES	1
DCT	DES	1

Table 5.1: Percentage (0-1) of Original String Compared with Decoded String

Stego-Tech	Enc-Tech	MSE	PSNR
LSB	OTP	0.000354766845703125	82.6313733426562
DCT	OTP	55.0844612121582	30.720512549663226
LSB	RSA	0.000640869140625	80.063110010937
DCT	RSA	55.08403778076172	30.72054593378312
LSB	AES	0.00043869018554687 5	81.7092244246595
DCT	AES	55.091064453125	30.71999197105002
LSB	DES	0.00023651123046875	84.392285933213
DCT	DES	55.08302307128906	30.720625936412095

Table 5.2: Average MSE and PSNR values for all Algorithms

5.3 Observation during Implementation

The general DCT process uses the blue pixels for message message encoding for colored images. For grayscale images, the encoding is done directly since it does not have RGB pixels. For RBGA images, alpha pixel can be used for message encoding as alpha indicates how opaque each pixel is, and thus if the bit of alpha pixel is changed, only the Mean Square Error change in both images will be very less compared to the case where either of RGB pixels were chosen. This process may help in minimization of MSE for colored images as well. For minimization of MSE for RGB images, an RGB image can first be converted to RGBA image and then applying algorithm to the converted image thus reducing MSE error to larger extent as in RGBA the alpha pixels can be used for message encoding which will just change the intensity of original image and not the blue or red or green pixels thus keeping the colored images same with a bit different intensity still difficult to predict.

6 | Conclusion and Future Work

6.1 Conclusions

Observing the figures and the tables given in the previous chapters, following conclusions were made:

- Least Significant bit technique was found to be better off than the Discrete Cosine Transformation and the MSE value for algorithm which had steganography technique as DCT was found to be significantly greater than those having steganography technique as LSB.
- Similar was the case with the PSNR for LSB and DCT ans PSNR was found more for algorithms using LSB than those using DCT.
- All cryptographic algorithms were found to be well off as when the decoded message was compared with original message (text), all messages were found to be same.
- Some cryptographic algorithms, that theoretically provides more security than others, took a bit longer time to run than others.

6.2 Observations

These were some of the observations made. It can be concluded from the above observations that this system encrypts a secret message and then embeds it into an digital image. The image obtained after encoding was not found to be much different from the original image.

Since non-grayscale images were used, the DCT algorithm showed a bit of difference between original and the embedded image. But those difference can be reduced by choosing grayscale digital image for message encoding. The proof of getting lower MSE and higher PSNR value for grayscale images using DCT Algorithm can be found in paper Secure Image Steganography Algorithm Based on DCT with OTP Encryption[3] where they used grayscale images for image encoding.

Using LSB algorithm was found to be efficient for both grayscale as well as non-grayscale images as the MSE value was very less and PSNR was sufficiently high for non-grayscale images as well.

6.3 Future Work

Following ideas can be thought to work upon.

A new encryption Technique can be used. Suggestion are the use of Honey Encryption Strategy for encryption as this algorithm provides resilience to brute-force attacks. The research work on using and improving Honey Encryption is under progress. More encryption algorithms like Elliptical Curve Cryptography(ECC) or Quantum Cryptography can also be tried out.

Another improvement that can be done is to try using Discrete Wavelet Transform (DWT) or Discrete Fourier Transform(DFT) image transformation instead of DCT. Although DCT has advantage as it uses real values instead of imaginary values in case of DWT and complex values in case of DFT.

To keep DCT for an advantage, another research can be done on minimizing the Mean Square Error values for image transformation of non-grayscale images. If successful, it would add an advantage of using frequency domain image transformation with minimal chance of error in the encoded image as compared to original image.

References

[1] Ozdemir Cetin and A Turan Ozcerit. A new steganography algorithm based on color histograms for data embedding into raw video streams. *computers & security*, 28(7):670–682, 2009.

[2] Steganography, wikipedia, May 2020.

[3] Eko Hari Rachmawanto, Christy Atika Sari, et al. Secure image steganography algorithm based on dct with otp encryption. *Journal of Applied Intelligent System*, 2(1):1–11, 2017.

[4] Edi Jaya Kusuma, Oktaviana Rena Indriani, Christy Atika Sari, Eko Hari Rachmawanto, et al. An imperceptible lsb image hiding on edge region using des encryption. In *2017 International Conference on Innovative and Creative Information Technology (ICITech)*, pages 1–6. IEEE, 2017.

[5] Barnali Gupta Banik and Samir Kumar Bandyopadhyay. Implementation of image steganography algorithm using scrambled image and quantization coefficient modification in dct. In *2015 IEEE International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN)*, pages 400–405. IEEE, 2015.

[6] Monika Gunjal and Jasmine Jha. Image steganography using discrete cosine transform (dct) and blowfish algorithm. *International Journal of Computer Trends and Technology (IJCTT)*, 11(4):144–150, 2014.

[7] T Shahana. A secure dct image steganography based on public-key cryptography. *International Journal of Computer Trends and Technology (IJCTT)*, 4(7):2039–2043, 2013.

[8] Ketan Shah, Swati Kaul, and Manoj S Dhande. Image steganography using dwt and data encryption standard (des). *International Journal of Science and Research (IJSR)*, 3(5):372–376, 2014.

[9] Prasetiyo Budi, Rahmat Gernowo, Beta Noranita, and M Kom. The combination of bit matching-based steganography and des cryptography for data security. 2013.

[10] Sachin Mungmode, RR Sedamkar, and Niranjan Kulkarni. An enhanced edge adaptive steganography approach using threshold value for region selection. *arXiv preprint arXiv:1601.02076*, 2016.

[11] Saurabh Singh and Ashutosh Datar. Improved hash based approach for secure color image steganography using canny edge detection method. *International Journal of Computer Science and Network Security (IJCSNS)*, 15(7):92, 2015.

[12] Soumyajit Sarkar and Arijit Basu. Comparison of various edge detection techniques for maximum data hiding using lsb algorithm. *International Journal of computer Science and information Technologies*, 5(3):4722–4727, 2014.

[13] Alan C Bovik. *The essential guide to image processing*. Academic Press, 2009.

[14] Dave Marshall. The discrete cosine transform (dct).

[15] Data encryption standard, wikipedia, Jun 2020.

[16] Cryptography, tutorialspoint.

[17] Behrouz A. Forouzan and Debdeep Mukhopadhyay. *Cryptography and network security*. Mc Graw Hill Education (India) Private Limited, 2015.