DSP Laboratory Project Report on

Image Steganography

M NAVEEN KUMAR (16EE230)

G MANOBHIRAMA SUMANTH (16EE216)

P UDAY KUMAR REDDY (16EE155)

Under the Guidance of,

Dr. Krishnan CMC

Department of Electrical and Electronics Engineering, NITK Surathkal

Date of Submission: 17-03-2019

in partial fulfillment for the award of the degree

of

Bachelor of Technology

In

Electrical and Electronics Engineering

At

Department of Electrical and Electronics Engineering

National Institute of Technology Karnataka, Surathkal

ABSTRACT

Keywords: Cryptography , Steganography , Cipher Text, Discrete Cosine Transforms, LSB

Cryptography is study of mathematical techniques related to information security such as confidentiality , Data integrity , data origination and authentication . Cryptographers call an original communication the clear text or plain text . Once the original communication has been enciphered or scrambled , the result is known as the cipher text or cryptogram . The enciphering process usually involves an algorithm and a key . An encryption algorithm is a particular method of scrambling a computer program or a written set of instructions . The key specifies the actual scrambling process . In this paper we'll discuss the various cryptography techniques in use today.

Cryptography was developed to fulfill at the minimum level of the following clauses :

1. **Privacy / confidentiality**
2. **Authentication**
3. **Non repudiation**
4. **Integrity**

Steganography which is art of sending coded messages in picture format is explained with an example for clarity . Cryptography plays a key role in the defense of any country, where even the radio conversation needs to be encrypted .

Contents

1 INTRODUCTION

Cryptography in greek means : kryptos is "secret" and graphos is " writing" . It is an art and science of preparing protected or coded communications . The enciphering process usually involves an algorithm and a key . An encryption algorithm is a particular method of scrambling a written set of instructions or computer program. The key specifies the actual scrambling process . The original communication may be a written or a set of digital data or broadcast message . One essential aspect for secure communications is that of cryptography , which is the focus of this presentation . But it is important to note that while cryptography is necessary for secure communications , it is not by itself sufficient.

Various aspects in information security such as data confidentiality, authentication ,data integrity and non- repudiation are central to modern cryptography. Modern cryptography exists at the intersection of the disciplines of mathematics, computer science,on communication science and electrical engineering .

The main purpose of this paper is to define some of the terms and concepts behind basic crypto graphic methods , and to offer a way to compare the myriad crypto graphic schemes in use today . Today , cryptography is a way of life , right from operating systems to SMART cards , the entire DIGITAL SECURITY is based on cryptography .

Applications of cryptography include chip-based payment cards, digital

currencies,electronic commerce , military communications and computer passwords . Cryptography also plays a major role in copyright infringement of digital media and digital rights management .

2 CRYPTOLOGY

It is the study of codes or art of writing and solving them . Cryptology can be subdivided into two branches : Cryptography and Cryptanalysis. We know what is cryptography , so before going deep into cryptography we will look into cryptanalysis and how it differs from cryptography.

3 CRYPTANALYSIS

Cryptanalysis is the study of analyzing information systems in order to study the hidden aspects of the systems . Cryptanalysis is used to breach cryptographic security systems and gain access to the contents of encrypted messages , even if the cryptographic key is unknown . In addition to mathematical analysis of cryptographic algorithms, cryptanalysis includes the study of side-channel attacks that do not target weaknesses in the cryptographic algorithms themselves, but instead exploit weaknesses in their implementation. Even though goal has been the same , the methods and techniques of crypt analysis have changed drastically through the history of cryptography , adapting to increasing cryptographic complexity , ranging from the pen-and-paper methods of the past , through machines like the Colossus computers at Bletchley Park in World War II, to the mathematically advanced computerized schemes of the present . Methods for breaking modern crypto systems often involve solving carefully constructed

problems in pure mathematics, the best-known is integer factorization.

Total Break : Finding the secret key .

Information Deduction : Gaining some information about plain texts or ciphertexts that was not previously known.

Global Deduction : Finding a functional equivalent algorithm for encryption and decryption that does not require knowledge of the secret key.

Distinguishing Algorithm : The attacker has the ability to distinguish output of the encryption (ciphertext) from a random permutation of bits.

The goal of the attacker performing crypt analysis will depend on the specific needs of the attacker in a given attack context . In most cases , if crypt analysis is successful at all , an attacker will not be able to go past being able to deduce some information about the plain text .

4 CRYPTOSYSTEM

In cryptography , a crypto system is a suite of crypto graphic algorithms needed to implement a particular security service , most commonly for achieving confidentiality (encryption) . Typically , a crypto system consists of three algorithms : one for key generation , one for encryption , and one for decryption .

It is an implementation of crypto graphic techniques and their accompanying infrastructure to provide information security services. A cryptosystem is also referred to as a cipher system.

Let us discuss a simple model of a cryptosystem that provides confidentiality to the information being transmitted. This basic model is depicted in the illustration below :

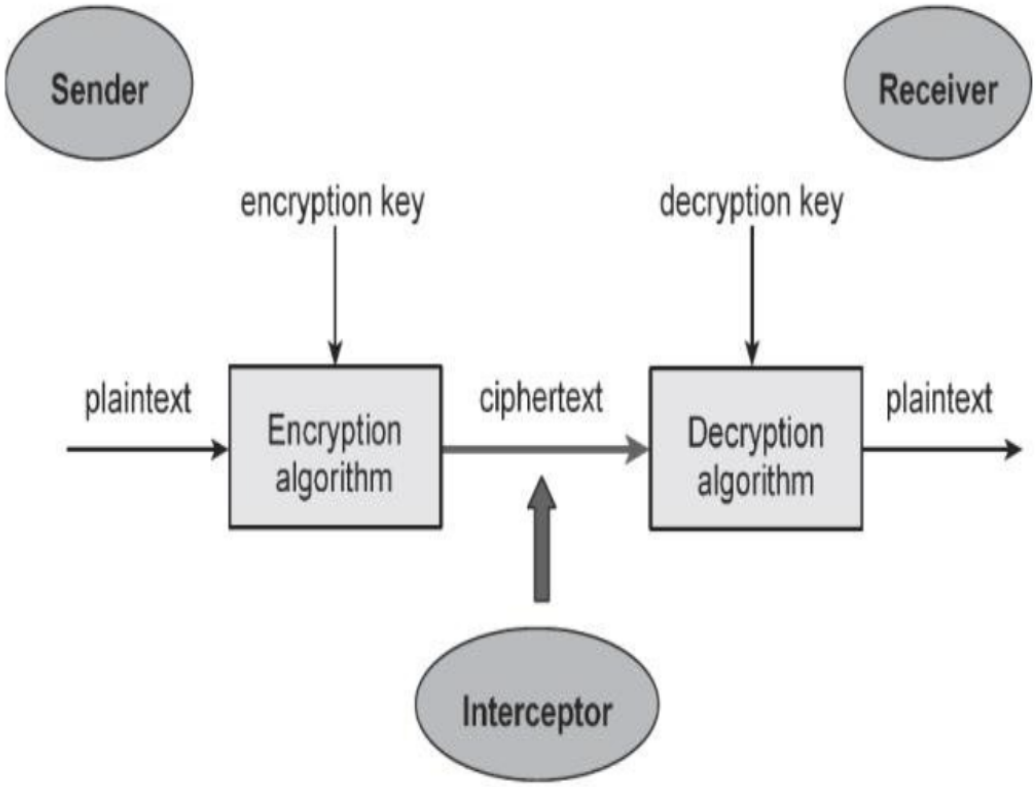

fig 1.1 CRYPTOSYSTEM MODEL

The illustration shows a sender who wants to transfer some sensitive data to a receiver in such a way that any party intercepting or eavesdropping on the communication channel cannot extract the data. The objective of this simple cryptosystem is that at the end of the process, only the sender and the receiver will know the plaintext .

Components of a Cryptosystem :

Various components of basic crypto system are as follows :

1. **Encryption Algorithm**: It is a mathematical process that produces a ciphertext for any given plaintext and encryption key. It is a cryptographic algorithm that takes plaintext and an encryption key as input and produces a ciphertext .

2. **Encryption Key** : It is a value that is known to the sender . The sender inputs the encryption key into the encryption algorithm along with the plain text in order to compute the cipher text .

3. **Decryption Algorithm** : It is a mathematical process , that produces a unique plain text for any given cipher text and decryption key . It is a crypto graphic algorithm that takes a cipher text and a decryption key as input , and outputs a plain text. The decryption algorithm essentially reverses the encryption algorithm and is thus closely related to it .

4. **Decryption Key** : It is a value that is known to the receiver. The decryption key is related to the encryption key, but is not always identical to it. The receiver inputs the decryption key into the decryption algorithm along with the ciphertext in order to compute the plaintext. For a given cryptosystem , a collection of all possible decryption keys is called a key space .

5. **An interceptor** (an attacker) is an unauthorized entity who attempts to determine the plaintext . He can see the cipher text and may know the decryption algorithm. He , however, must never know the decryption key.

5 HISTORY OF CRYPTOGRAPHY

The first documented use of cryptography in writing dates back to circa

1900 B.C . when an Egyptian scribe used non-standard hieroglyphs in an inscription . Some experts argue that cryptography appeared spontaneously sometime after writing was invented , with applications ranging from diplomatic missives to war-time battle plans .

A more recent example can be seen during WORLD WAR - 1 :

Before the United States entered World War I, the German government tried to provoke a war between the United States and Mexico. On January 19, 1917, the German foreign secretary, Arthur Zimmermann, sent an encoded telegram to his diplomatic representatives in Mexico, asking them to propose a secret alliance with the Mexican government. But British intelligence officers intercepted and quickly decoded the message, sending it on to President Woodrow Wilson. A huge public outcry ultimately resulted in an American declaration of war against Germany .
It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications .

Hieroglyph : The Oldest Cryptographic Technique

The first known evidence of cryptography can be traced to the use of ' hieroglyph . Some 4000 years ago, the Egyptians used to communicate by messages written in hieroglyph . This code was the secret known only to the scribes who used to transmit messages on behalf of the kings. One such hieroglyph is shown below. Later , the scholars moved on to using simple mono-alphabetic substitution ciphers during 500 to 600 BC . This

involved replacing alphabets of message with other alphabets with some secret rule. This rule became a key to retrieve the message back from the garbled message .

fig 1.2 HIEROGLYPH USED BY EGYPTIANS

The Spartans used a system which consisted of a thin sheet of papyrus wrapped around a staff (now called a "staff cipher"). Messages were written down the length of the staff, and the papyrus was unwrapped. In order to read the message, the papyrus had to be wrapped around a staff of equal diameter. Called the 'scytale' cipher, this was used in the 5th century B.C. to send secret messages between greek warriors. Without the right staff, it would be difficult to decode the message using the techniques available at that time. The following version of the alphabet demonstrates the technique. First we see the wrapped version of the alphabet, then the unwrapped version.

eg : ADGJMPSVY

BEHKNQTWZ

CFILORUX

ADGJMPSVYBEHKNQTWZCFILORUX

(unwrapped version)

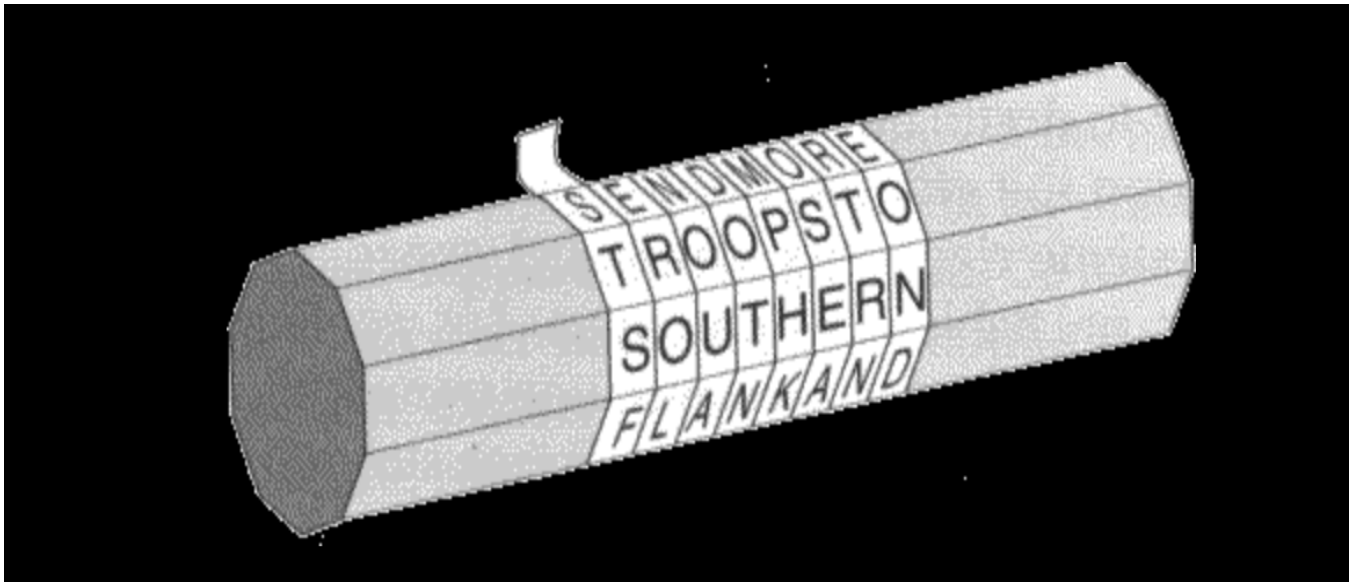

fig 1.3 SCYTALE CIPHER

Types of Classical Ciphers :

1 . Simple substitution cipher :

The simple substitution cipher is a cipher that has been in use for many hundreds of years . It basically consists of substituting every plain text character for a different cipher text character.

It is an improvement to the Caesar Cipher. Instead of shifting the alphabets by some number, this scheme uses some permutation of the letters in alphabet. For example, A.B.....Y.Z and Z.Y.....B.A are two obvious permutation of all the letters in alphabet. so, the total set of permutations with 26 letters is 26!

Example

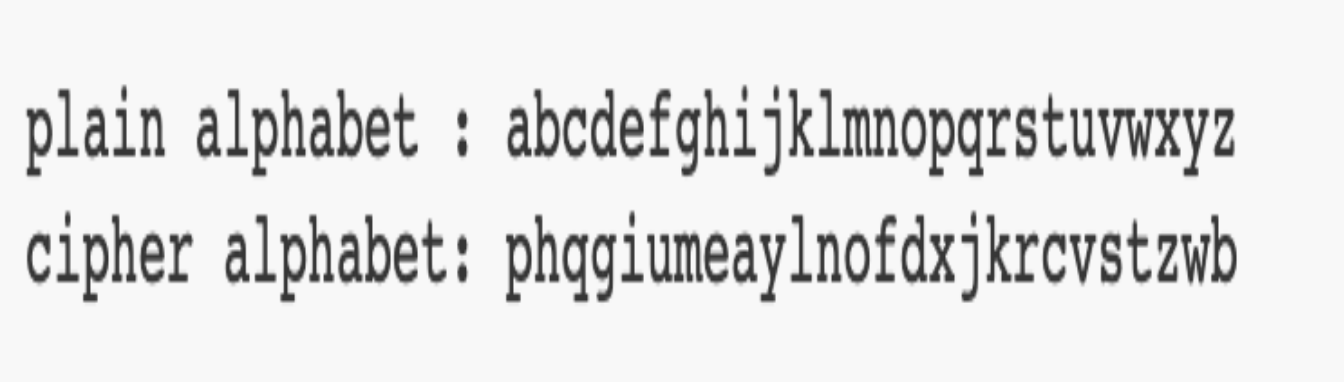

fig 1.4 substitution cipher

In this example, the chosen permutation is K,D, G, ..., O. The plaintext point is encrypted to MJBXZ. On receiving the ciphertext, the receiver, who also knows the randomly chosen permutation, replaces each ciphertext letter on the bottom row with the corresponding plaintext letter in the top row. The ciphertext MJBXZ is decrypted to point.

2 . Transposition cipher :

Instead of replacing the characters with other characters, this cipher changes

the order of the characters .

The key determines the position that the characters are moved .

The key for this cipher is not standard .

Instead of list of alphabatic substitution it is a mapping order .

Such as (1,2,3,4,5)=(3,4,5,2,1). This means that the third element is put in the place of first thus followed by fourth then the fifth ,second and finally followed by the original first element .

eg : "WORLD" – "RLDWO"

3 . Concealment cipher :

It hides a message in a longer message i.e "a message within a message" .

Example :

The agreed secret key is to use every sixth word .

Selecting every sixth word will decrypt the message.

" I have been trying to buy you a nice gift like gold or an antique but prices now are really high" to "buy gold now".

6 MODERN CRYPTOGRAPHY

Modern Cryptography operates on binary bit sequences whereas classic

cryptography manipulates traditional characters, i.e., letters and digits directly .

Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, electrical engineering, and communication science .

Secrecy is obtained through a secrete key which is used as the seed for the algorithms .

7 STEGANOGRAPHY

Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video. The word steganography combines the Greek words steganos meaning "covered, concealed, or protected", and graphein meaning "writing"

Comparision of Cryptography and Steganography :

Cryptography and Steganography are well known and widely used techniques that manipulate information in order to cipher or hide their existence respectively.

Steganography is the art and science of communicating in a way which hides the existence of the communication. Cryptography is the practice of protecting the contents of a message alone .

Steganography is concerned with concealing the fact that a secret message is being sent as well as concealing the contents of the message. Cryptography prevents unauthorized party from discovering the content of communication but Steganography prevents discovery of the existence of communication .

The advantage of steganography over cryptography alone 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 . In other words, steganography is more discreet than cryptography when we want to send a secret information. On the other hand, the hidden message is easier to extract.

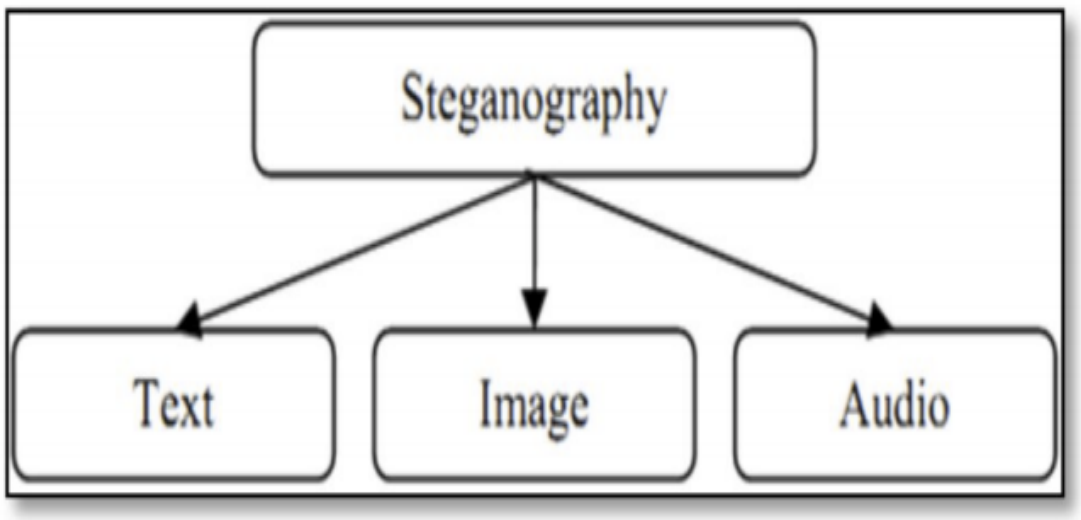

fig 1.6 Classification of steganography

8 IMAGE STEGANOGRAPHY

Now that we know the basics of steganography, lets learn some simple image processing concepts . Before understanding how can we hide an image inside another, we need to understand what a digital image is.

We can describe a digital image as a finite set of digital values, called pixels. Pixels are the smallest individual element of an image, holding values that represent the brightness of a given color at any specific point. So we can think of an image as a matrix (or a two-dimensional array) of pixels which contains a fixed number of rows and columns .

Procedure for Hiding an image inside another :

1. To hide an image inside another, the image which will be hidden needs to have at most the same size of the image which will hide it.
2. We must create two loops to go through all rows and columns (actually each pixel) from the images.
3. So, we get the RGB from the image 1 and image 2 as binary values .
4. We merge the most significant bits from the image 1 with the most significant bits from the image 2
5. Finally, we convert the new binary value to a decimal value .

hence , And set it to a new pixel position from the resulted image . Now we have an image hidden inside another image.

fig 1.7 steganographic image processing

As you can see in the image above, we lost some image quality in the process, but this does not interfere with image comprehension .

9 LSB based Steganography

9.0.1 What is a digital image?

AS seen in the previous section we can describe a digital image as a finite set of digital values, called pixels. So the image is essentially a matrix of pixel densities.

9.0.2 The hiding method

The leftmost bit is the most significant bit. If we change the leftmost bit it will have a large impact on the final value. For example, if we change the leftmost bit from 1 to 0 (11111111 to 01111111) it will change the decimal value from 255 to 127.

On the other hand, the rightmost bit is the less significant bit. If we change the rightmost bit it will have less impact on the final value. For example, if we change the leftmost bit from 1 to 0 (11111111 to 11111110) it will change the decimal value from 255 to 254. Note that the rightmost bit will change only 1 in a range of 256.

Thus, each pixel has three values (RGB), each RGB value is 8-bit (it means we can store 8 binary values) and the rightmost bits are less significant. So, if we change the rightmost bits it will have a small visual impact on the final image. This is the steganography key to hide an image inside another. Change the less significant bits from an image and include the most significant bits from the other image.

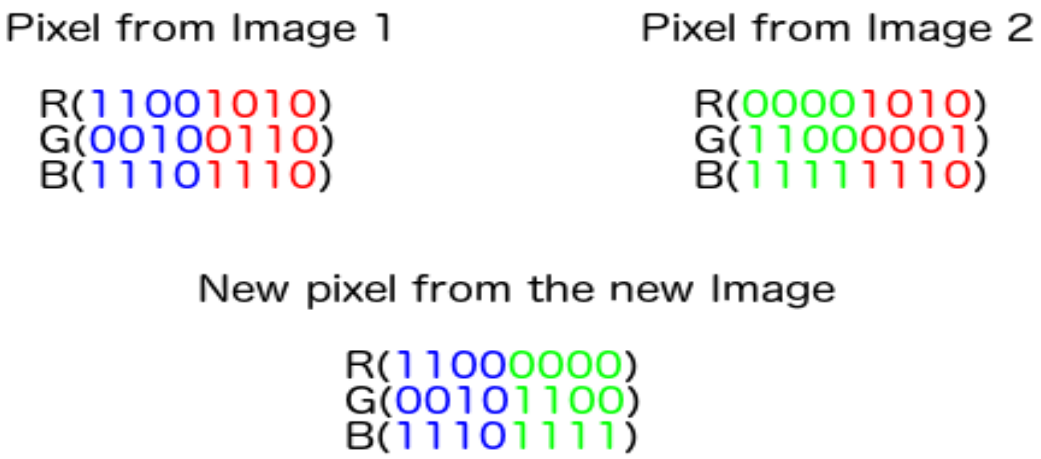

Figure 9.1: LSBs of the cover image replaced with hidden image's MSBs

10 Discrete Cosine Transformation

DCT coefficients are used for JPEG compression. It separates the image into parts of differing importance. It transforms a signal or image from the spatial domain to the frequency domain. It can separate the image into high, middle and low frequency components.

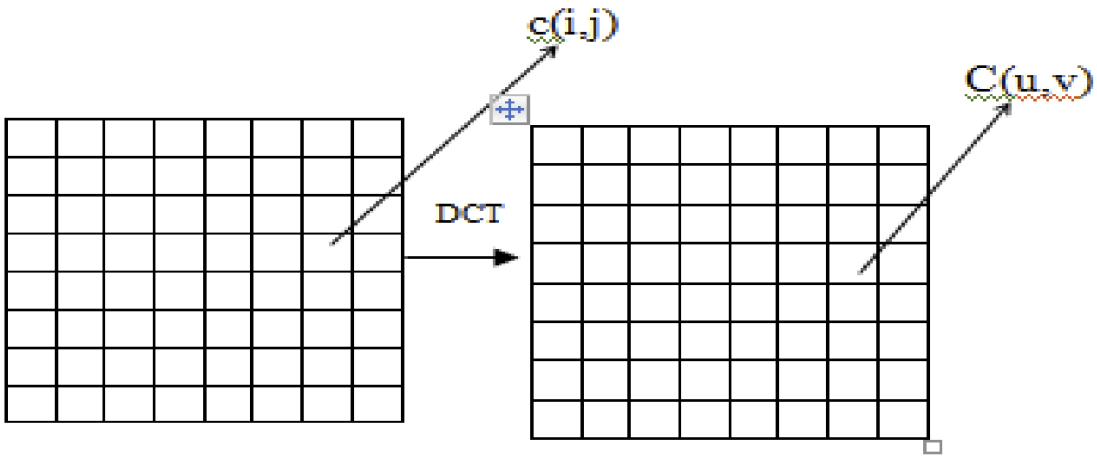

Figure 10.1: Discrete cosine transform of an image

Here, the input image is of size N X M. c(i, j) is the intensity of the pixel in row i and column j; C(u,v) is the DCT coefficient in row u and column v of the DCT matrix. Signal energy lies at low frequency in image; it appears in the upper left corner of the DCT. Compression can be achieved since the lower right values represent higher frequencies, and generally small enough to be neglected with little visible distortion. DCT is used in steganography asImage is broken into 88 blocks of pixels. Working from left to right, top to bottom, the DCT is applied to each block. Each block is compressed through quantization table to scale the DCT coefficients and message is embedded in DCT coefficients.

The Following formulas are used to Compute the DCT and Inverse DCT for an 8*8 block

DCT:

$C(u,v) = a(u)a(v)\sum_{i=0}^{7}\sum_{j=0}^{7} c(u,v)Cos(\frac{(2i+1)u\pi}{16})Cos(\frac{(2j+1)v\pi}{16})$

Inverse DCT:

$c(u,v) = \sum_{i=0}^{7}\sum_{j=0}^{7} a(u)a(v)C(u,v)Cos(\frac{(2i+1)u\pi}{16})Cos(\frac{(2j+1)v\pi}{16})$

Where $a(i) = \frac{1}{\sqrt{8}}$ if $i = 0$ and $\frac{1}{2}$ otherwise

11 Results and Conclusions

For the image steganography the following 2 images were used as the cover image and the secret image. These 2 memes from Star Wars were selected due to the presence of texts in image which make the image more vulnarable to attacks due to similar pixel density in neighbouring areas of a pixel.

Figure 11.1: The Cover image and the Secret Image

11.1 4 bit LSB encoding

In this method 4 least significant bits were used from the cover image and these bits were replaced by the secret image's 4 Most significant bits(MSB's). The image is hence distorted and not like the cover image. The 16 values from 0-15 were then hashed to different values from 0-15 so that the data is more secure. The hash acts as a key to the secret image.

Code Snippet for Hiding Data:

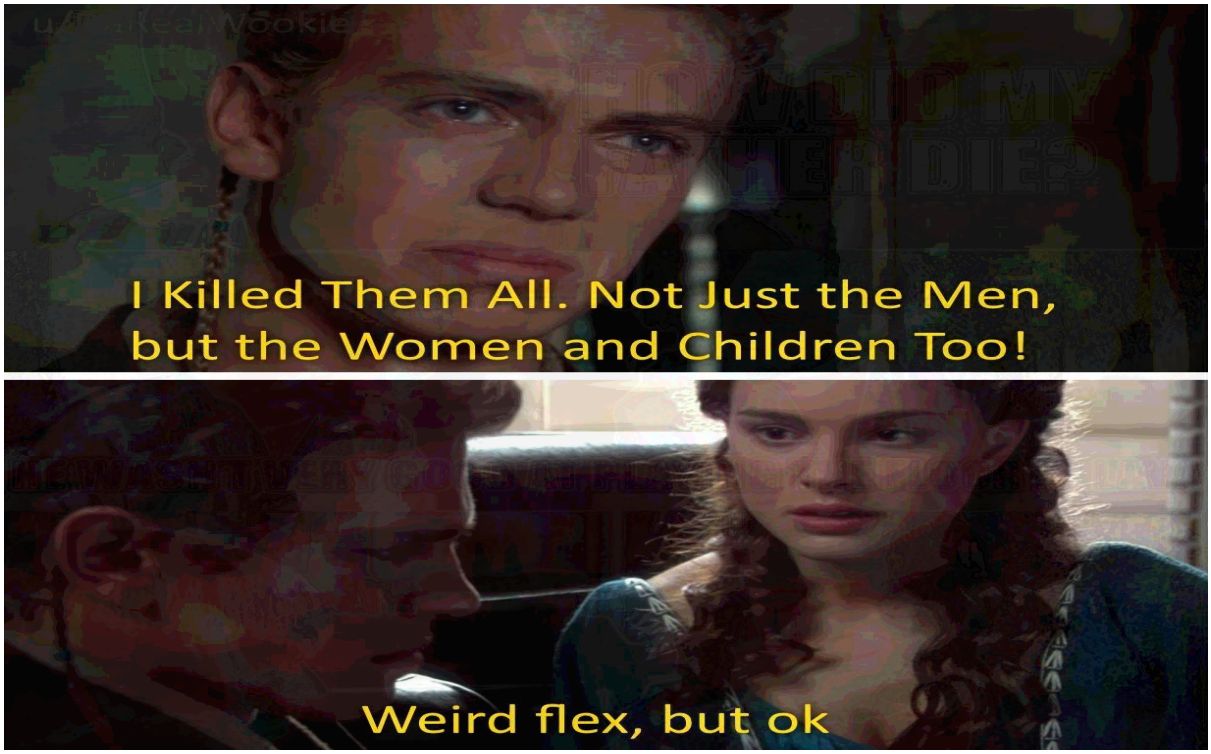

Figure 11.2: The Cover Stego Image with the hidden image

Figure 11.3: The Recovered Secret Image

As seen from the above 2 images, The recovered image seems lossless since the most significant bits are recovered but the stego image is violating the purpose of stegonagraphy. It shows how the image contains a hidden image if closely observed.

11.2 2 bit LSB encoding

In this method 2 least significant bits were used from the cover image and these bits were replaced by the secret image's bits. The image is hence more like the cover image even after modification. The cover image is resized to a bigger image to fit the entire data. The 8 bits of the image are encoded 2 bits at once in a 2*2 block of the cover image.

Figure 11.4: The Cover Stego Image with the hidden image

Figure 11.5: The Recovered Secret Image

As seen from the above 2 images, The recovered image is lossless and the cover image shows minimum signs of being a stego image. This is exactly what we need. We will further see how this can also be improved.

11.3 2 bit LSB encoding with random shuffle

This is similar to the previous method but in this method the locations of pixels are randomly shuffled by a key which is used as the seed for the rand function in C++. This key prevents from attacks that suspect stegonography in images and extracting the secret data. The following 3 images show the stego image, extracted secret image, the extracted image without the key/with the wrong key.

Figure 11.6: The Cover Stego Image with the hidden image with randomisation

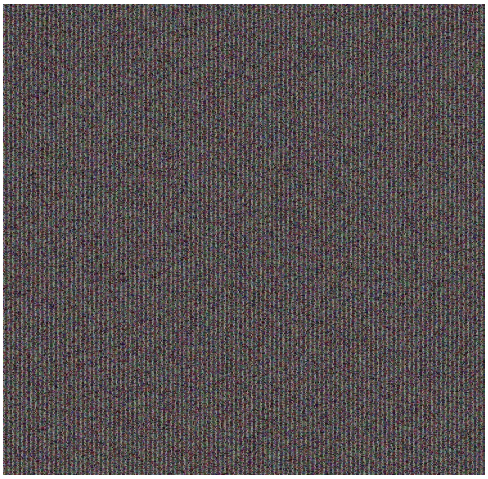

Figure 11.7: The Recovered Secret Image with the proper Key and without the Key

As seen from the above images, the secret image is safe from attacks that try to extract the hidden images.

11.4 1 bit LSB encoding

In this method only the least significant bit (1's place) was used from the cover image and these were replaced by the secret image's 4 Most significant bits(MSB's). The cover image is resized to be bigger to fit more bits. This increases the file size.

Figure 11.8: The Cover Stego Image with the hidden image

Figure 11.9: The Recovered Secret Image

As seen from the above 2 images, the stego image is very similar to the cover image now that only 1 bit is being modified. Although, to a human eye it doesn't seem much different from 2 bit encoding and just increases the size of the stego image unnecessarily.

11.5 Discrete Cosine Transform by encoding in DC value

By splitting the image in 8*8 blocks we can find the 2 Dimentional Discrete Cosine Transform of the block. The formula is seen in the previous section. The 8*8 block is converted to frequency domain with majority of the data in the DC component or F(0,0) where F(u,v) denotes the DCT coefficient of (u,v).

This method has lot of drawbacks if not implemented carefully. Let us look at the results of the DCT when the secret image is embeded in the DC component.

Figure 11.10: The Cover Stego Image with the hidden image and the Recovered image

As seen from the above 2 images there is a lot of noise and the secret image is not proper. This is due to the fact that when we take Inverse Discrete Cosine Transform, the pixel values that we get is in decimals whereas the pixel values stored are only integers from 0-255. To avoid this we need to run the loop that embeds the Secret image in DC component multiple times until we get a better result.

11.6 Discrete Cosine Transform by encoding in Non DC values

This method is similar to the previous method but over here we embed the secret image in the non DC components of the image. This improves the quality by some amount.

This method also has lot of drawbacks if not implemented carefully. Let us look at the results.

Figure 11.11: The Cover Stego Image with the hidden image and the Recovered image

As seen from the above 2 images there is a lot of noise and the secret image is not proper but the secret image is much better when compared to the last one although the stego image is distorted and clearly looks like an image that carries a secret image. This is again due to the fact that when we take Inverse Discrete Cosine Transform, the pixel values that we get is in decimals whereas the pixel values stored are only integers from 0-255. We can avoid this by running the loop that embeds the Secret image in DC component multiple times until we get a better result. The following table shows the comparison of various methods.

Comparison of various methods					
	4 Bit LSB	2 Bit LSB	1 Bit LSB	DCT (DC)	DCT (Non DC)
Hidden Image's Quality	Good Enough	Good	Good	Bad	Bad
Unhidden Image's Quality	Good	Good	Good	Bad	Bad
Naked Eye Identification	Yes	No	No	Yes	Yes
Elapsed Time to Hide	<1s	<1s	<1s	35s	50s
Elapsed Time to Unhide	<1s	<1s	<1s	14s	16s

11.7 Hiding Text in Images by LSB

The Method used to do this is the same as the 2 bit encoding where instead of hiding a pixel we are hiding the 8-bit ASCII text. The following image shows successful recovery of message

Figure 11.12: The Cover Stego Image with the hidden message

```
naveen@mine:~/Desktop/Repositories/DSP-MINI-PROJECT/LSB/text secret message$ ./hider
ENTER THE MESSAGE
naveen is in EEE
naveen@mine:~/Desktop/Repositories/DSP-MINI-PROJECT/LSB/text secret message$ ./unhider
HIDDEN MESSAGE IS
naveen is in EEE
```

Figure 11.13: The recovery of the secret message

As we can see from the above images the secret message doesn't affect the original cover image such that it is visible to the naked eye. Thus this method is safe and good to use to send secret messages.

11.8 The Distorted Images by DCT method

In the previous sections we have seen how the DCT method gets the images distorted. As mentioned earlier this is due to the pixel values being only integers from 0-255 which do not hold decimal points. Due to this, when the algorithm is finished, the saved pixels are floored to the lower integral value (example from 32.3 to 32). This creates noise and this is highly disturbing since the LSB's are affected which is what holds the secret message. Below image shows the change in the DC value after the pixels are floored to lower integral values.

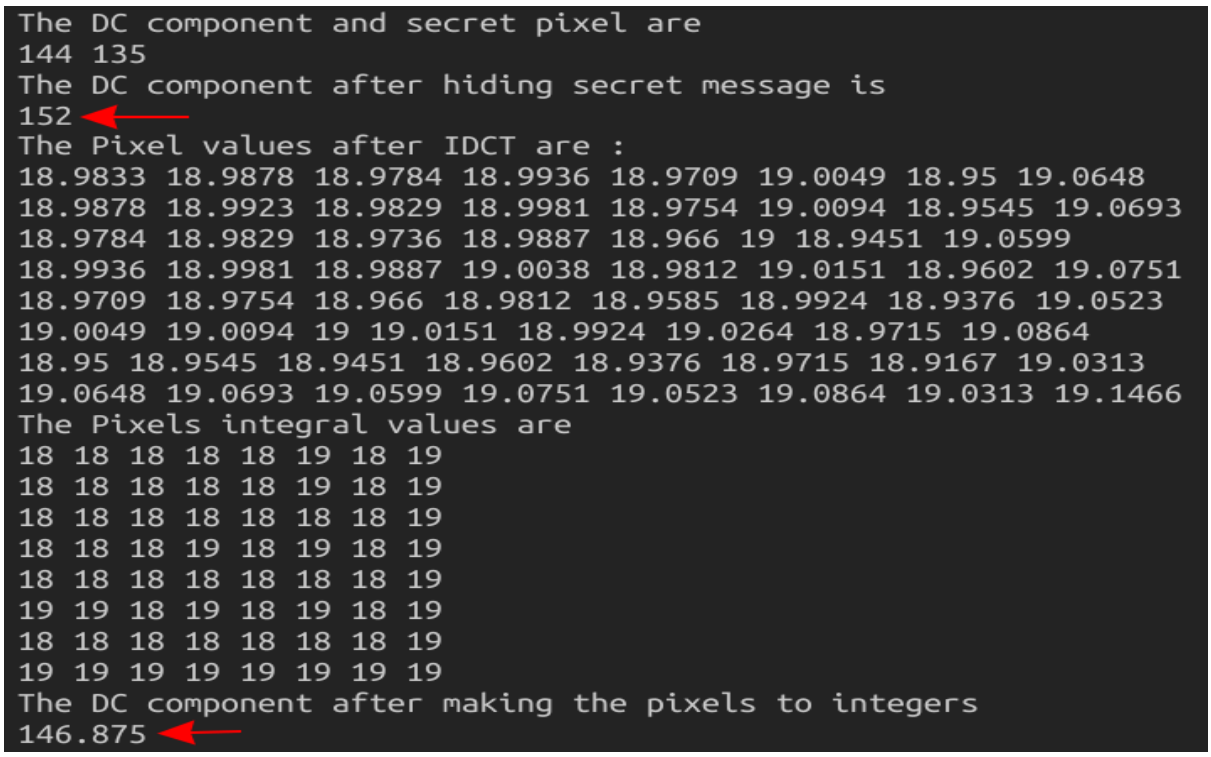

Figure 11.14: Image showing the pixel values being floored to the smaller integral value.

As we can see from the above image the secret pixel is being changed.

The MSB's of the secret pixel 135 (10000111) are 1000 or 8. The DC component 152 has 8 in it's LSBs (since 152&15 = 8). But after the modification of pixels to integers the new value of almost 147 contains 0011 in it's LSBs or 147&15 = 3. This is a totally different pixel value from 8 and this is the reason for the wrong or distorted output with noise. This can only be avoided by multiple execution of the loop so that the pixel values are almost integers. Even that doesn't guarantee a better result. Thus to encode a secret message it's better to avoid the frequency domain.

References

[1] CPSC 350 Data Structures: Image Steganography - Nick Nabavian

[2] A Secure Steganographic Algorithm Based on Frequency Domain for the Transmission of Hidden Information - A. Soria-Lorente1, and S. Berres

[3] Image Steganography Using Frequency Domain Dr. MAHESH KUMAR, MUNESH YADAV

[4] A Study of Various Steganographic Techniques Used for Information Hiding - C.P.Sumathi1 , T.Santanam and G.Umamaheswari

[5] An introduction to steganography methods - Mehdi Hariri, Ronak Karimi and Masoud Nosrati

[6] Steganography techniques - Drago Dumitrescu1 , Ioan-Mihail Stan1, Emil Simion

[7] Two Components based LSB and Adaptive LSB Steganography based on Hybrid Feature Detection for Color Images with improved PSNR and Capacity - Mamta. Juneja, and Parvinder S. Sandhu

[8] An Analysis of LSB DCT based Steganography Dr. Ekta Walia, Payal Jain

[9] DWT based Invisible Image Watermarking Algorithm for Color Images - Anumol T.J and P Karthigaikumar

[10] Application of Stochastic Diffusion for Hiding High Fidelity Encrypted Images Jonathan Blackledge and AbdulRahman Al-Rawi

[11] Comparison study between LSB and DCT Based Steganography - Alaa Abdul Hussein Daleh Al-magsoosi

[12] Steganography, Cryptography, Watermarking: A Comparative Study - Hardikkumar V. Desai

[13] Data Masking: A New Approach for Data Hiding? - Regunathan Radhakrishnan, Mehdi Kharrazi and Nasir Memon

[14] Some New Methodologies for Image Hiding using Steganographic Techniques - Rajesh Kumar Tiwari and Gadadhar Sahoo

[15] `https://users.cs.cf.ac.uk/Dave.Marshall/Multimedia/node231.html`

[16] Image Steganography Using Discrete Cosine Transform (DCT) and Blowfish Algorithm Monika Gunjal, Jasmine Jha

[17] A New Approach for Steganography? - Regunathan Radhakrishanan, Mehdi Kharrazi ans Nasir Memon

[18] DWT Based Watermarking Algorithm of Color Images - Guangmin Sun, Yao Yu