# A Project Report on

**Data Confidentiality using both Steganography and Cryptography Techniques**

Submitted in partial fulfillment for award of

# Bachelor of Technology

Degree in

**Computer Science & Engineering**

By

# Sk. Kashif (Y15ACS531) D. H. Venkata Sai (L16ACS583) Sk. Sarah Ahmed (Y15ACS536) Sk. Ashhad (Y15ACS529)



Under the guidance of

**Mr. T. Nagarjuna, Asst. Prof**

Department of Computer Science and Engineering

**Bapatla Engineering College**

(Autonomous)

(Affiliated to Acharya Nagarjuna University)

# BAPATLA – 522 102, Andhra Pradesh, INDIA 2018-201i9

**Department of Computer Science & Engineering**



**CERTIFICATE**

This is to certify that the project report entitled **Data Confidentiality**

**using both Steganography and Cryptography Techniques** that is

being submitted by Sk.Kashif (Y15ACS531), D. H. Venkata Sai (L16ACS583), Sk. Sarah Ahmed (Y15ACS536), Sk.Ashhad (Y15ACS529) in partial fulfillment for the award of the Degree of Bachelor of Technology in Computer Science & Engineering to the Acharya Nagarjuna University is a record of bonafide work carried out by them under our guidance and supervision.

Date:

# Signature of the Guide Signature of the HOD

**Mr. T. Nagarjuna Dr. SK. NAZEER**

**Asst. Professor Prof & Head**

**DECLARATION**

We declare that this project work is composed by ourselves, that the work contained herein is our own except where explicitly stated otherwise in the text, and that this work has not been submitted for any other degree or professional qualification except as specified.

Sk. Kashif (Y15ACS531)

D. H. Venkata Sai (L16ACS583) Sk. Sarah Ahmed (Y15ACS536) Sk. Ashhad (Y15ACS529)

**Acknowledgement**

We sincerely thank the following distinguished personalities who have given their advice and support for successful completion of the work.

We are deeply indebted to our most respected guide **T. Nagarjuna, Asst.Professor**, designation of guide, Department of CSE, for his/her valuable and inspiring guidance, comments, suggestions and encouragement.

We extend our sincere thanks to **Dr. SK. Nazeer**, Prof. & Head of the Dept. for extending his cooperation and providing the required resources.

We would like to thank our beloved Principal **Dr. S. Rajasekaran** for providing the online resources and other facilities to carry out this work.

We would like to express our sincere thanks to our project coordinator

**Dr. N. Sudhakar,** Professor Dept. of CSE for his helpful suggestions in presenting this document.

We extend our sincere thanks to all other teaching faculty and non-teaching staff of the department, who helped directly or indirectly for their cooperation and encouragement.

Sk. Kashif (Y15ACS531)

D. H. Venkata Sai (L16ACS583) Sk. Sarah Ahmed (Y15ACS536) Sk. Ashhad (Y15ACS529)

**Abstract**

The information security has become one of the most significant problems in data communication. There are many security problems that exist in communication technology which are very critical. One such problem is related to the confidentiality of the message exchange in web. In order to address this problem, cryptography and steganography can be combined. Another major problem is to secure the data from duplication and unauthorized use. For this purpose, Digital Watermarking is used for authentication of data and protection of copyright. The joining of these techniques provide a robust and strong communication system that able to withstand against attackers. Matlab is used as a simulator to implement the techniques of cryptography, steganography and digital watermarking.

TABLE OF CONTENTS

CHAPTER NO. TITLE PAGE NO. ABSTRACT v

[LIST OF FIGURES vii](#_TOC_250017)

LIST OF ABBREVATIONS ix

1. [INTRODUCTION 1](#_TOC_250016)
   1. [CRYPTOGRAPHY 1](#_TOC_250015)
      1. SYMETRIC KEY 2
      2. ASYMETRIC KEY 2
   2. [STEGANOGRAPHY 2](#_TOC_250014)
      1. [TEXT FILES 3](#_TOC_250013)
      2. [IMAGE FILES 3](#_TOC_250012)
      3. [AUDIO FILES 3](#_TOC_250011)
   3. BENIFITS OF COMBINING THE STEGANOGRAPHY

AND CRYPTOGRAPHY 3

* 1. [DIGITAL WATERMARKING 3](#_TOC_250010)
     1. [DIFFERENT TYPES OF WATERMARKING TECHNIQUES 4](#_TOC_250009)
        1. SPATIAL DOMAIN 4
        2. TRANSFORMATION DOMAIN WATERMARKING 4
  2. BENIFITS OF COMBINING THE CRYPTO,STEGAN

AND DIGITAL WATERMARKING 5

1. [EXISTING SYSTEM 6](#_TOC_250008)
   1. APPROACHES IN CRYPTOGRAPHY 6
   2. [VIGENER CIPHER 7](#_TOC_250007)
   3. [RESULTS 8](#_TOC_250006)
2. PROPOSED SYSTEM 11
   1. [ALGORITHMS 12](#_TOC_250005)
      1. DATA EMBEDDING PROCESS 12
      2. DATA EXTRACTION PROCESS 14
3. [IMPLEMENTATION 15](#_TOC_250004)
   1. [SOURCE CODE 16](#_TOC_250003)
      1. ENCRYPTION AT SENDER SIDE ALONG

WITH STEGANOGRAPHY 16

* + 1. DECRYPTION AT RECEIVER SIDE ALONG

WITH STEGANOGRAPHY 17

* + 1. DIGITAL-WATERMARKING AT SENDER SIDE 18
    2. DIGITAL-WATERMARKING AT RECEIVER SIDE 20

1. [OUTPUTS AND RESULTS 22](#_TOC_250002)
2. [CONCLUSION 30](#_TOC_250001)
3. [REFERENCES 31](#_TOC_250000)

## List of Figures

|  |  |  |
| --- | --- | --- |
| **Figure No.** | **Figure Name** | **Page No.** |
| 1.1 | Cryptography System | 1 |
| 1.2 | Steganography System | 3 |
| 1.3 | Digital Watermarking | 3 |
| 2.1 | Vigener Cipher | 7 |
| 2.2 | Image Upload | 8 |
| 2.3 | Text Upload | 9 |
| 2.4 | Encryption and Hiding | 9 |
| 2.5 | Decryption and Extraction | 9 |
| 3.1 | Data Embedding Process | 12 |
| 3.2 | Data Extraction Process | 14 |
| 4.1 | Overview | 16 |
| 5.1 | Design | 22 |
| 5.2 | Image Uploading | 22 |
| 5.3 | Text File Uploading | 23 |
| 5.4 | Encryption along with steganography | 23 |
| 5.5 | Watermark Generation | 24 |
| 5.6 | Watermark Upload | 24 |
| 5.7 | Cover Image Upload | 25 |
| 5.8 | 3 level DWT transformation of  watermark image | 25 |
| 5.9 | 3 level DWT tranformation of  cover image | 26 |
| 5.10 | Generated watermark | 26 |
| 5.11 | Generated MSE value | 27 |
| 5.12 | Generated PSNR value | 27 |
| 5.13 | Extraction and Decryption | 28 |
| 5.14 | Extraction of watermarked image | 28 |
| 5.15 | Generated MSE value | 29 |
| 5.16 | Generated PSNR value | 29 |

|  |  |  |
| --- | --- | --- |
|  | **List of Abbrevations** |  |
| **DWT** |  | Discrete Walvet Transform |
| **PSNR** |  | Peak signal to noise ratio |
| **MSB** |  | Mean square error |
| **LSB** |  | Least Significant Bit |
| **DCT** |  | Discrete Cosine Transform |
| **DWT** |  | Discrete Wavelet Transform |
| **DFT** |  | Discrete Fourier Transform |

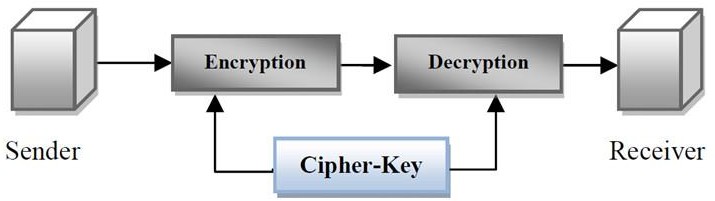
## INTRODUCTION

Information security has grown as a significant issue in our digital life. The development of new transmission technologies forces a specific strategy of security mechanisms especially in state of the data communication . The significance of network security is increased day by day as the size of data being transferred across the Internet . Cryptography and steganography provide most significant techniques for information security .The most important motive for the attacker to benefit from intrusion is the value of the confidential data he or she can obtain by attacking the system . Hackers may expose the data, alter it, distort it, or employ it for more difficult attacks . A solution for this issue is using the advantage of cryptography and steganography combined in one system.

Cryptography and steganography are two approaches used to secure information, either by encoding the information with a key or by hiding it . Combining these two approaches in one system gives more security . It is useful to explain these approaches and discuss the benefits combining them.

## Cryptography

Cryptography is one of the traditional methods used to guarantee the privacy of communication between parties. This method is the art of secret writing, which is used to encrypt the plaintext with a key into ciphertext to be transferred between parties on an insecure channel. Using a valid key, the ciphertext can be decrypted to the original plaintext. Without the knowledge of the key, nobody can retrieve the plaintext. Cryptography plays an essential role in many factors required for secure communication across an insecure channel, like: confidentiality, privacy, non-repudiation, key exchange, and authentication.Figure 1.1 shows the cryptography system.There are two types of cryptographic schemes for securing the data. These schemes are often used to reach the objective: public-key cryptography, secret key cryptography, and hash functions. The length and type of the keys used depend on the type of encryption algorithm .



## Fig1.1 CRYPTOGRAPHY SYSTEM

* + 1. **Symmetric / Secret Key Cryptography**

The technique of Secret key encryption can also be known as the symmetric-key, shared key, single-key, and eventually private-key encryption. The technique of private key uses for all sides encryption and decryption secret data. The original information or plaintext is encrypted with a key by the sender side also the similarly key is used by the receiver to decrypt a message to obtain the plaintext. the key will be known only by a people who are authorized to the encryption/decryption.

However, the technique affords the good security for transmission but there is a difficulty with the distribution of the key. if one stole or explore the key he can get whole data without any difficulty. An example of Symmetric-Key is DES Algorithm.

## Asymmetric / Public Key Cryptography

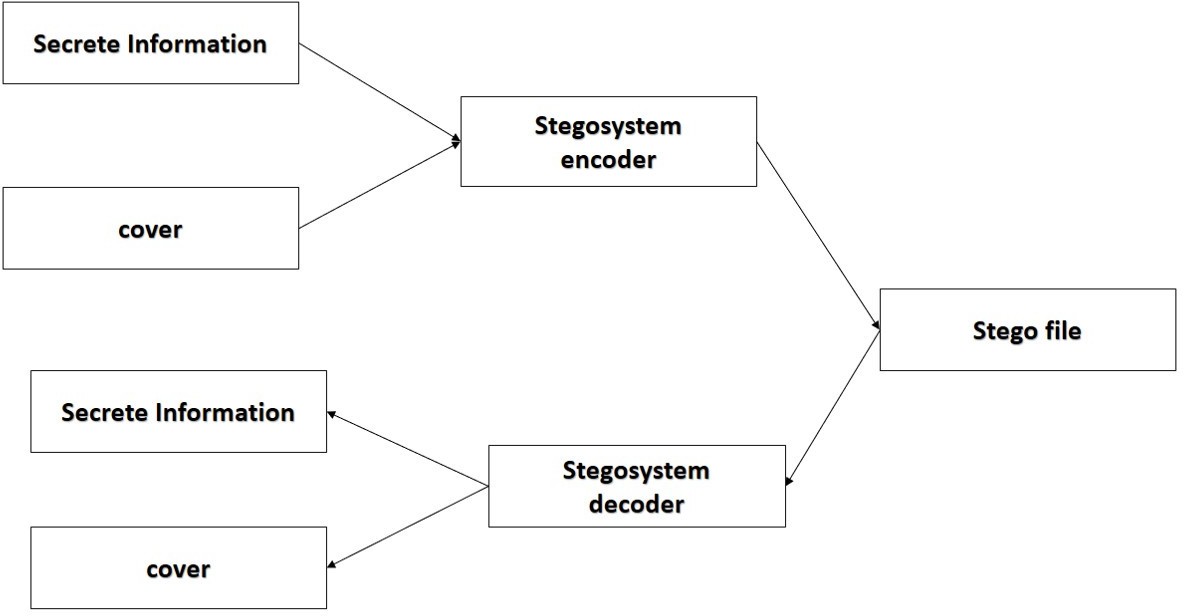
We can call this technique as asymmetric cryptosystem or public key cryptosystem, this technique use two keys which are mathematically associated, use separately for encrypting and decrypting the information.

In this technique, when we use the private key, there are no possibilities to obtain the data or simply discover the other key. all keys are needed for the technique to run. The key used for encryption is stored public therefore it’s called public key, and the decryption key is stored secret and called private key. An example of Asymmetric-Key Algorithms is RSA RSA.

## Steganography

Can be defined as the science of hiding and communicating data through apparently reliable carriers in attempt to hide the existence of the data. So, there is no knowledge of the existence of the message in the first place. If a person views the cover which the information is hidden inside of he or she will have no clue that there is any covering data, in this way the individual won’t endeavour to decode the data. Figure1.2 shows the steganography system overview.

The secret information can be inserted into the cover media by the stego system encoder with using certain algorithm. A secret message can be plaintext, an image, ciphertext , or anything which can be represented in form of a bitstream. after the secret date is embedded in the cover object, the cover object will be called as a stego object also the stego object sends to the receiver by selecting the suitable channel, where decoder system is used with the same stego method for obtaining original information as the sender would like to transfer.There are various types of steganography.



**Fig.1.2 Steganography System**

## Text Files

The technique of embedding secret data inside a text is identified as text stego. Text steganography needs a low memory because this type of file can only store text files. It affords fast transfer or communication of files from a sender to receiver.

## Image Files

It is the procedure in which we embed the information inside the pixels of image. So, that the attackers cannot observe any change in the cover image. LSB approach is a common image steganography algorithm.

## Audio Files

It is the process in which we hide the information inside an audio. There are many approaches to hide secret information in an audio files for examples Phase Coding, LSB.

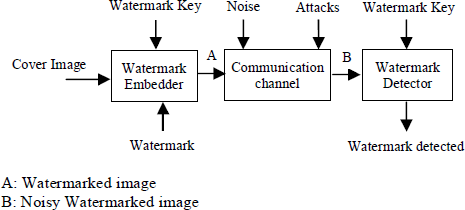
## Benefits of combine the Steganography and Cryptography

It is noted that steganography and cryptography alone is insufficient for the security of information,therefore If we combine these systems, we can generate more reliable and strong approach.The combination these two strategies will improve the security of the information secret. This combined will fulfill the prerequisites, for example, memory space, security, and strength for important information transmission across an open channel. Also, it will be a powerful mechanism which enables people to communicate without interferes of eavesdroppers even knowing there is a style of communication in the first place.

## Digital Watermarking

Digital watermarking is that technology which is used for protection of digital media such as video, audio and image . In this technique, watermark i.e. secret information is embedded in digital media using some algorithms and the watermarked media is processed. After that, watermark i.e. secret information is extracted using the particular algorithm. This technique,

i.e. digital watermarking is used for authentication of data and protection of copyright . Here two phases are used which are embedding of the watermark and detection and extraction of watermark.



## Fig1.3 Digital Watermarking

## Different types of watermarking techniques

Digital watermarking is very much popular now a days because it is easily available and it protects our data from illegal use. It has two major areas i.e. spatial domain watermarking and frequency domain watermarking. In the spatial domain techniques, we embed the watermark by modifying the pixel values. On the other hand, in transform domain watermarking, the watermark is embedded into the coefficients of transform domain.Various types of transform domain techniques are DCT, DWT and DFT. From robustness and imperceptibility point of view, transform domain techniques are better than spatial domain techniques.

## Spatial Domain Watermarking

We know that the image is made up of pixels. In this method of watermarking, we embed the watermark in some specific pixels of image . In the extraction phase, we extract the watermark from these specific pixels. This technique is very much easy to use, less complex and also takes less time. But on the other hand, it is not robust for various types of attacks.

## Transform Domain Watermarking

The transform domain watermarking is better as compared to the spatial domain watermarking. The image is represented in the form of frequency in the transform

domain watermarking. In the transform domain watermarking techniques, firstly conversion of the original image is done by a predefined transformation. Then we embed the watermark in the transform image or in the transformation coefficients. Finally, we take the inverse transform to get the watermarked image . Commonly used transform domain methods are Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Discrete Fourier Transform (DFT).

1. **Discrete cosine transform** It is generally used for the signal processing. In this

we transform the image into the frequency domain. It is applied in many areas like pattern recognition, data compression, and image processing. This technique is more robust than spatial domain watermarking techniques. The main steps used in DCT are:

* Firstly, take the image and divide it into non-overlapping 8\*8 blocks.
* Calculate forward DCT of each of the non-overlapping blocks.
* Use HVS blocks selection criteria.
* Now use highest coefficient selection criteria.
* Then embed watermark in the selected coefficient.
* Now take inverse DCT transform of each block.

## Discrete wavelet transform

Discrete Wavelet Transform (DWT) gives a multi resolution representation of the image. This representation provides a simple framework for interpreting the image formation. The DWT analyses the signal at multiple resolution. When we apply the DWT to an image, it divides the image into two quadrants, i.e. high frequency quadrant and low frequency quadrant. This process repeats until the signal has been entirely decomposed. If we apply 1- level DWT on two dimensional image, it divides it into four parts, i.e. *LL*: It consists the low frequency details of the original image. We can say that approximation of the image lies in this part.

*LH*: It consists vertical details of the original image.

*HL*: It consists the horizontal details of the original image.

*HH*: It consists high frequency details of the original image.

Since we know that the detail of original image lies in low frequency coefficients, so we embed the watermark into low frequency coefficients . If we apply IDWT, we

can reconstruct the original image from the decomposed image.

## Discrete fourier transform

Discrete Fourier Transform (DFT) offers more robustness against geometric attacks like scaling, cropping, translation, rotation, etc. It decomposes an image in sine and cosine form. In this, embedding may be done in two ways: direct embedding and the template based embedding. In the direct embedding technique we modifying DFT magnitude and phase coefficients and then the watermark is embedded. The template based embedding technique introduces the concept of templates. In DFT domain, during embedding process, we embed the template, which is used to find the transformation factor. When the image is transformed, firstly this template is searched and it is then used to resynchronize the image. After this, detector is used to extract the embedded spread spectrum watermark.

## Benefits of combine the Cryptography , Steganography and Digital Watermarking.

Steganography and Digital Watermarking are both forms of information hiding where the context can be viewed as keeping the information a secret or making the information subtle respectively.Steganoraphy provides protection against detection and digital watermarking provides protection against removal.

## EXISTING SYSTEM

Steganography literally means Covered Writing. It is the process of hiding the secret data inside a cover image such that only the intended receiver knows its existence. Internet plays an important role for data transmission and data sharing.It is a worldwide and publicized medium, some confidentiality data might be stolen, copied modified or destroyed. Here security is a main problem so we use Steganography as a solution. Cryptography involves converting a message text into an unreadable cipher. A large number of cryptography algorithms have been created till date with the primary objective of converting information into unreadable ciphers. Cryptography systems can be broadly classified into symmetric-key systems and public key systems. The symmetric key systems uses a common key for encryption and decryption of the message. This key is shared privately by the sender and the receiver. The sender encrypts the data using the joint key and then sends it to the receiver who decrypts the data using the same key to retrieve the original message

.

## Approches in Cryptography

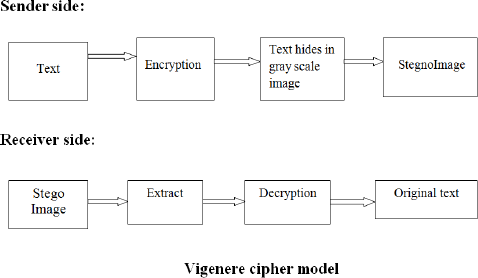
A. Matrix for substitution mapping A matrix M with 16 rows and 95 columns initialized with ASCII codes of characters using secret key is used for mapping the plaintext characters into level-one cipher text characters. During encryption, a block of 16 plaintext characters in the message is taken into a buffer. The ASCII code of the character P(i) is obtained. From this ASCII code, 32 aresubtracted. The resulting integer is used as column number j of ith row of the matrix M. The element contained in this cell which is an ASCII code of a character, is taken as the level-one cipher text character CL1 (i) corresponding to the plaintext character P (i).In this way all the characters in a block are mapped into level-one cipher text characters and all plaintext character blocks are mapped into level-one cipher text character blocks. 0 through column 15 in row n of matrix M concatenated. These keys are used in translation rounds. Another set of sub-keys Ktp\_n0, Kps\_n1, Ktp\_n2 and Ktp\_n3 are generated such that Ktp\_n0 = character of matrix M with row number n and column number 0. Here, each key is a character represented by the corresponding element in the matrix M. These keys are used in transposition rounds. B.Substitution mapping procedure A given message is broken into blocks of sixteen plaintext characters P (0) through P (15). Plaintext character P (i) is taken and a number j is calculated such that j = (ASCII code of plaintext character P (i) – 32). This number, j, is used as column number of the matrix M. Using j as column number we proceed to find the element in the ith row of the matrix M. This element (ASCII code of a character) is used as level-one cipher text character CL1 (i) for a given plaintext character P (i). For example, for the plain text character P (0) in a block, i = 0, j = (ASCII code of plaintext character P (0) – 32) is used as column number of row 0 of the matrix M to obtain level one cipher text character corresponding to P (0). Similarly for character P(1) in the plaintext character block, i = 1 and j = ( ASCII code of plaintext character P(1) – 32) where j is used as column number of the row 1 of the matrix to obtain level-one cipher text character corresponding to P(1). In this way, all the 16 plaintext characters in a block are mapped into 16 level one cipher text characters denoted by CL1(i), i =0 to 15. The characters of level 1 cipher text character block (CL1 (0) through CL1 (15)) are transferred to a16 element array A1.*C.Translation and Transposing* Eight rounds of translation and transposition operations are performed on the level 1 cipher text character block. The translation operations are done using X-OR operation performed on the cipher text character block using sub key, Kts\_n in the nth round. The translated cipher text character block is transposed using four arrays whose elements are circular shifted using sub-keys Ktp\_n0, Ktp\_n1, Ktp\_n2, Ktp\_n3 used

in that round. These operations make the resulting output cipher text characters extremely difficult to decrypt by any adversary without having the secret key. The translation and transposition produce the effect of diffusion. *D.LSB* In this method researcher embedded one bit or more from secret message in cover directly. This is way simplicity and easy to detect and extract secret message. To enhancement the security of LSB standard, some researcher using Intermediate Significant Bit and Most Significant Bit (ISB and MSBA). In developed LSB method to increase security by using intermediate significant bit (ISB) to hide secret message in smooth area in image. He using 2, 3, 4 bit in cover to hide secret message. On other hands proposed techniques to embed to conceal the secret data .This however makes the hiding capacity of the carrier image very low. *E.Transform domain* Discrete Wavelet Transform is used for digital images. Many DWTs are available. Depending on the application most appropriate one should be used. To hide text message integer wavelet transform can be used. When DWT is applied to an image it is decomposed into four sub bands: LL, HL, LH and HH. The LL part contains the most significant features. So if the information is hidden in LL part the stego image can withstand compression or other manipulations. Sometimes distortion may be produced in the stego image and then other sub bands can be used. DWT is becoming more popular and is replacing DCT and DFT in many applications such as compression. DWT has excellent properties, mainly suitable for compression and embedding, as listed below: Decomposition of the signal into different frequency bands by DWT closely matches with the HVS characteristics and this makes it possible to processes the different frequency bands independently The high frequency sub bands in DWT locate the image features such as edges and texture regions, which are

less sensitive to HVS characteristics and hence can be used for embedding. In compression, multi resolution representation property of DWT is suitable for transmission of image and video data.

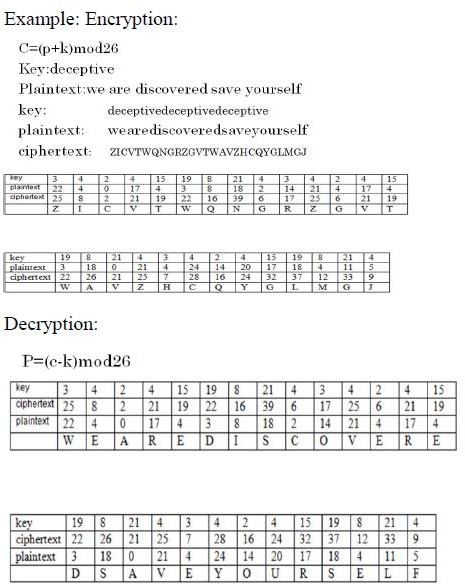
## Vigener Cipher

Vigenere encryption algorithm was developed by Blaise De Vigenere in 1583.It uses the defined square matrix termed as tabula recta, Vigenere square, or Vigenere Table and custom key to encrypt the plain text message .It is a poly alphabetic cipher in which a given letter or symbol in a plain will not always enciphered by the same cipher letter or symbol. By far, the best known poly-alphabetic substitution cipher is the Vigenere Cipher. In this previous cipher is added to current iteration such that confidentiality increases. For Vigenere Cipher:



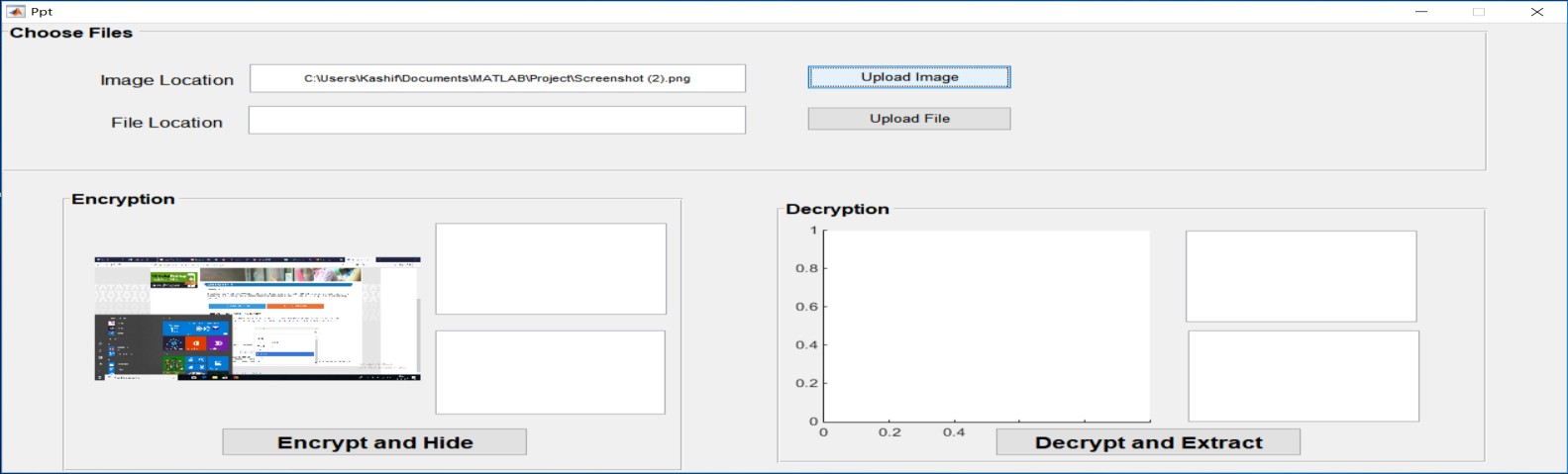
In the above model, In sender side the text can be encrypted using Vigenere Cipher algorithm((c[i] = p[i] + k[j] ) mod 127) and then the text is hiding in an image using LSB stenographic technique. In receiver side the text can be extracted from an stegno image and then decrypted using ((p[i] = c[i] - k[j] ) mod 127). So, that we can get the original text.

Example :

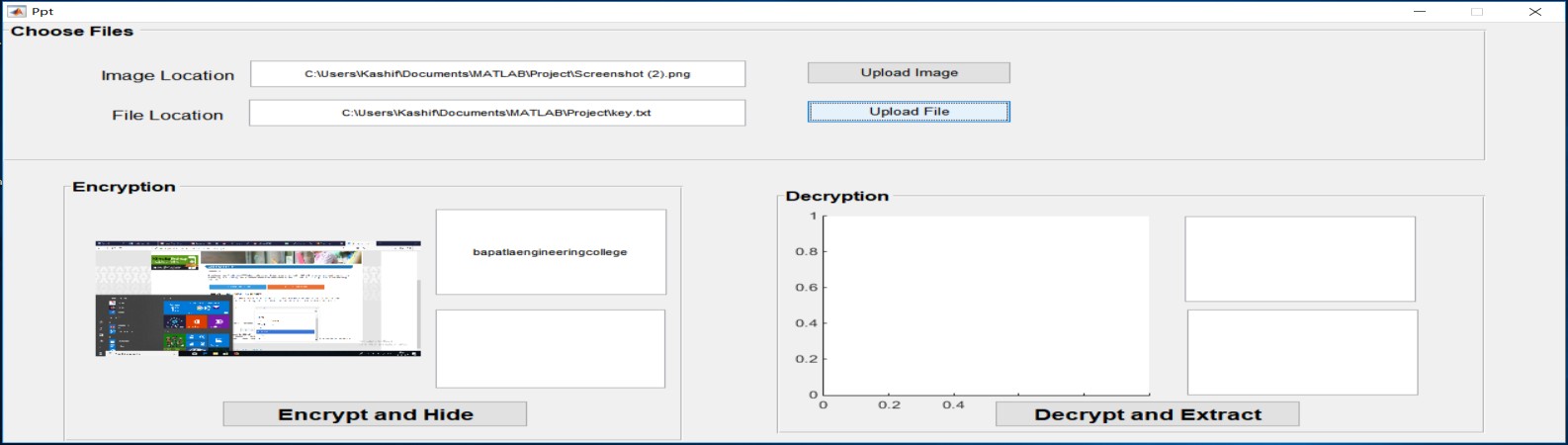


## RESULTS

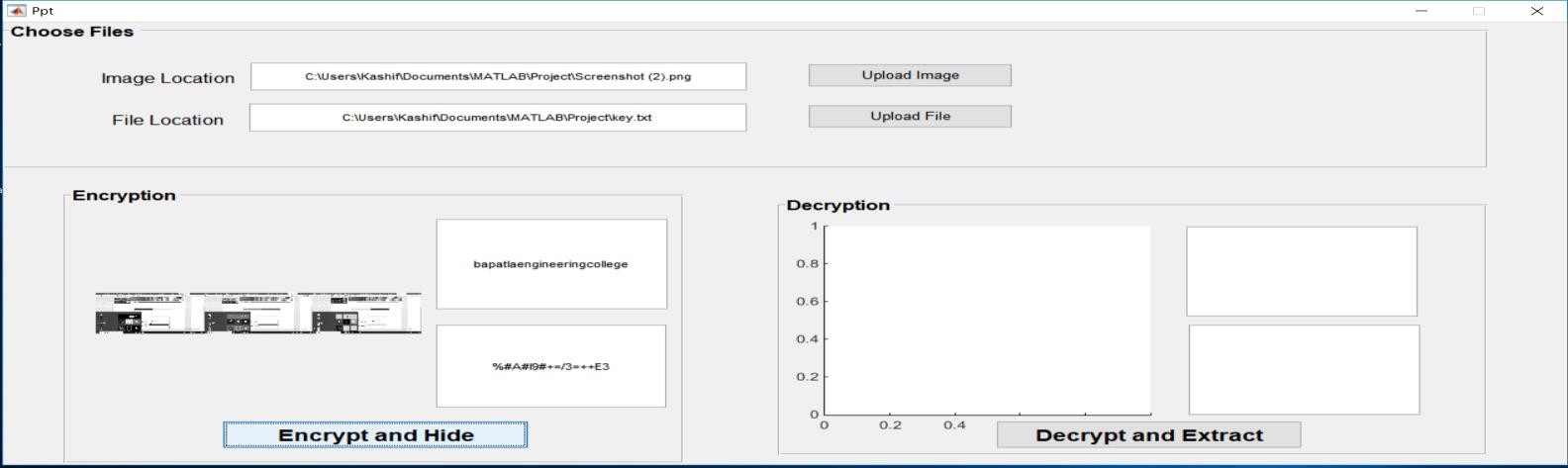
Vigenere Cipher:



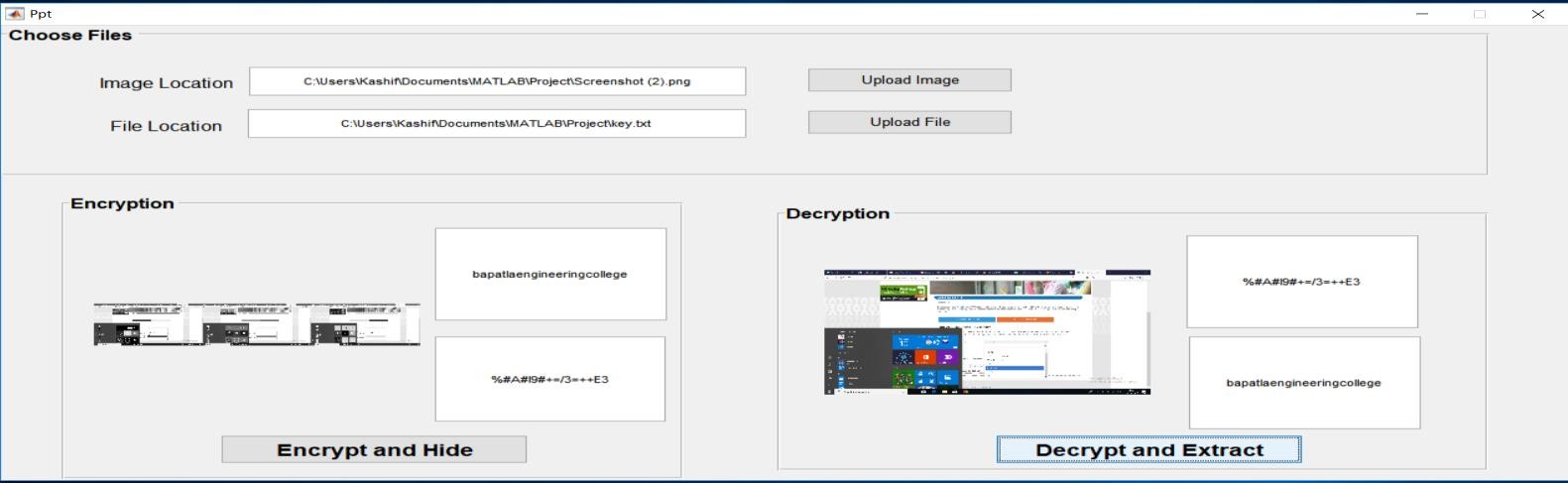
## Fig2.2ImageUpload



**Fig2.3 Text Upload**



**Fig2.4 Encryption and Hiding**



**Fig2.5 Decryption and Extraction**

To provide security we use either cryptography or steganography but in this we are including both cryptography and steganography to provide better security.In the proposed system, steganographic method uses the special domain technique that is the LSB Steganography technique which uses the formats like bmp,jpg etc. This paper can be extended to a level such that it can be used for different types of image formats like jpeg,bmp etc. in the future**.**

## PROPOSED APPROACH

There has been an increasing demand for information security and secure communication with continuous growth of internet users. Out of various available security mechanisms the most widely used security mechanism is Steganography with Digital Watermarking.

Steganography and Digital Watermarking combines three security mechanisms steganography and cryptography as one and Digital watermarking both together. This mechanism has advantages of providing high security, low time complexity but this mechanism does not enhance capacity, robustness, and image quality. In this paper we have used a new version of Steganography with Digital Watermarking using status Least Significant Bit (LSB) algorithm and 2-D Haar-Discrete Wavelet Transform (DWT) algorithm both together. This new mechanism has advantages of both algorithms status Least Significant Bit (LSB) and 2-D Haar-Discrete Wavelet Transform (DWT).

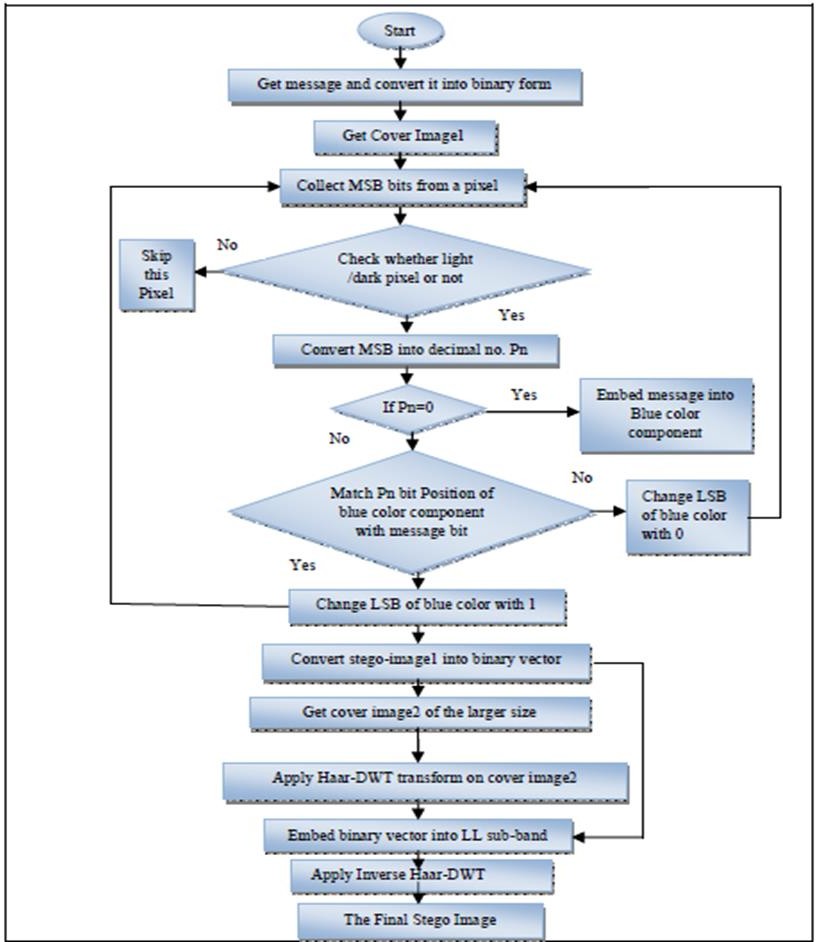
The main objective of this new security mechanism is to achieve high security,payload capacity, high Peak Signal to Noise Ratio (PSNR) value, low Mean Square Error (MSE) value, good imperceptibility and robustness. Today, in this new era of internet Information Security is becoming a big problem for the world due to the fast growth of internet users day by day. If an internet user wanted to share his personal information with other internet user by using the social applications, then hackers can attacked on these social applications and they can hack all the personal information about the internet user. Therefore to protect all the personal information from an unauthorized person we need security mechanisms. “Steganography” is a Greek word which means “hiding writing”. Steganography word is the combination of two parts: Steganos which means “secret” and Graphic which means “writing. Steganography is a security mechanism of hiding sensitive information among the bits of a cover file such as an image, text, an audio file and video file in such a way that only sender and receiver know about the hidden message inside the cover file. Cryptography comes from a Greek word meaning hidden or secret writing for secure Communication in the presence of an unauthorized person. Cryptography includes encryption and decryption process of a message. Cryptography is the art of protecting sensitive information by encrypting it into an unreadable format called cipher text .

The person who has a secret key can decrypt the message in to Plain text. In cryptography the message is converted into encrypted form with the help of encryption key which is known to sender and receiver only. However, the transmission of encrypted message is not safe because the encrypted message may easily arouse attacker‘s suspicion and may be intercepted or attacked easily.Stegano-Digital Watermarking is the security mechanism in which steganography and cryptography are used together. In Stegano-Digital Watermarking secret message to be transmitted is first encrypted using encryption algorithm. Then the encrypted message (cipher text) is hidden into a cover file using steganographic technique. The cover file is then sent to the receiver. Even if a hacker suspects the presence of data into the cover file and recovers the cipher text he will still need decryption algorithm to understand the message. So using the dual steganography is much more secure than using cryptography or steganography alone. A new version of steganography is the security mechanism which uses steganography within steganography. In this secret data is embedded in a cover image using the status Least Significant Bit embedding algorithm to generate a stego-image. Then stego- image is considered as secret data and it is again embedded in other cover image using the 2- D Haar-Discrete Wavelet Transform embedding algorithm which creates a final stego–

image. Stegano-Digital watermarking is the process of transmitting two or more images simultaneously in a single channel which is achieved by merging the images. In order to achieve enhanced security, two images can be merged so that when an intruder tries to intercept the secret data, it is not knowledgeable to him. In this technique at the sender side, sender uses a secret message and two cover mediums 1 and 2. Out of which secret message and cover medium 1 are private and cover medium 2 is public.

## ALGORITHMS

In the proposed scheme steganography and Digital Watermarking are used. The main reason behind this if steganography is used only once then an unauthorized person can hack secret data from any multimedia cover medium over the internet. But if steganography and Digital watermarking is used, then even if an unauthorized person can hack the secret data from any cover medium at the first time then second time secret data will be secured inside any cover medium. Thus this proposed work is used to protect the secret data at two times. To achieve the goal of high security, embedding capacity, good imperceptibility and robustness use the new version of dual steganography using the two status Least Significant Bit (LSB) algorithm and 2-D Haar-Discrete Wavelet Transform(DWT) algorithm together. It presents the data hiding and data extraction process for the proposed scheme.

* + 1. Data Embedding Process:

In data embedding process two cover images are used i.e. cover image1 and cover image2(watermark image). The secret data is embedded inside the cover image1 with the help of status Least Significant Bit (LSB) embedding algorithm to generatea stego-image1. Next this stego-image1 is considered as the secret data and it is embedded inside other cover image2 by using the 2-D Haar Discrete Wavelet Transform (DWT) embedding algorithm which generates a final stego-image.

The Proposed algorithm works as follows at the sender side:

Step1: Get the original message. Step2: Convert it into binary form. Step3: Get the cover image1.

Step4: Collect the MSB bits from a pixel (Red, Green, Blue color component). Step5: Check the pixel whether it is a lighter or darker pixel.

Step6: From the MSBs, for lighter image1 if it contains two bits 1 and for the darker image1 if it contains two bits 0,

select this pixel for hiding message bit. Otherwise, skip this pixel. Step7: Convert MSB into decimal number Pn.

Step8: If Pn=0 for the darker image1 only embed the message bit into the Blue color component of the pixel.

Step9: For lighter image1 or other value of Pn:

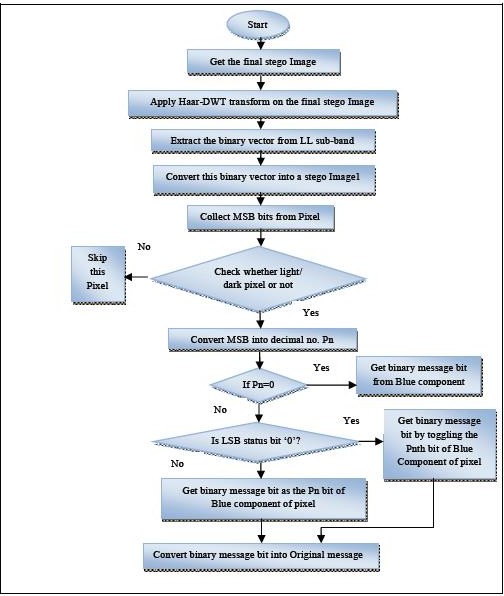
1. Check Pn bit position of the Blue color component with message bit.
2. If it matches then change the LSB of Blue color component with 1.
3. If it does not match then change the LSB of Blue color component with 0. Step10: Get the cover image2 of the larger size.

Step11: Apply Haar-DWT transform on the cover image2 which creates four sub bands LL, LH, HL and HH.

Step12: Convert the stego-image1 obtained from the step 9 into a binary vector.

Step13: Embed this vector into the LL sub band pixels of transformed image2 by adding random values to that pixel value.

Step14: Apply inverse Haar-DWT transform to regenerate the final stego-image. Step15: Transmit the final stego-image.



**Fig.3.2** Flowchart for Data Extraction Process

* + 1. Data Extraction Process:

In data extraction process stego-image1 is extracted from the final stego-image by using the Discrete Wavelet Transform (DWT) extraction algorithm. Next, secret data is extracted from stego-image1 by using the Least Significant Bit (LSB) extraction algorithm.

The Proposed algorithm works as follows at the receiver side:

Step1: Get the final stego-image.

Step2: Apply Haar-DWT transform on the final stego-image.

Step3: Extract the binary vector from LL sub band by comparing the pixel values i.e. if there is no match, then it contains vector bit else not.

Step4: Convert this binary vector into pixel values to form a stego-image1.

Step5: Collect the MSB bits from a pixel (Red, Green, Blue color component) from stego- image1 obtained from previous step.

Step6: Check the pixel whether it is a lighter or darker pixel.

Step7: From the MSBs, for lighter image1 if it contains two bits 1 and for the darker image1 if it contains two bits 0, select this pixel for extracting message bit. Otherwise, skip this pixel.

Step8: Convert MSB into decimal number Pn.

Step9: If Pn=0 only get the binary message bit from Blue component of the pixel. Step10: If Pn>0, check the LSB (Status bit) whether it is 0 or 1.

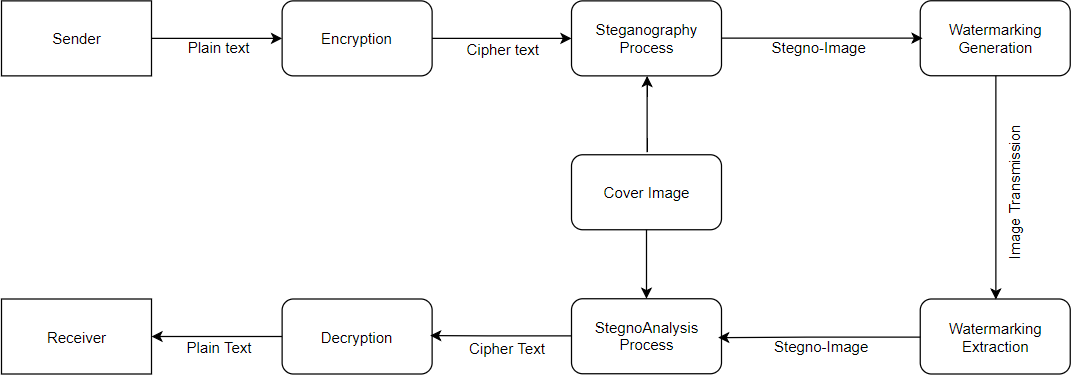
* + - 1. If the LSB equals to 0, then collect the binary message bit by toggling the Pn bit of the Blue component of the pixel.
      2. If the LSB equals to 1, then collect the binary message bit as the Pn bit of the Blue component of the pixel.

Step11: Convert the binary message bits into its original form.

During data transmission if data is intercepted then it can be used successfully by an unauthorized person over the internet. Therefore to provide more security to the information at the time of communication over unsecured channel a

Stegano-Digital Watermarking advance technique for data security is needed. In this paper, proposed highly secured data hiding Stegano-DigitalWatermarking scheme which is based on status LSB and 2-D Haar-DWT algorithms. A new Stegano-DigitalWatermarking is a technique which combines steganography within steganography that offers an ideal system for secret data transmission with respect to stand-alone cryptographic and steganographic techniques. This technique hides the secret message in binary form in two cover images due to which double protection has been provided to confidential data. The Final Stego-image is looking perfectly intact and has high PSNR value and low MSE value. Hence, an unintended observer will not be aware of existence of the secret message inside the cover image. The extracted secret data is perceptually similar to the original secret data. This method is one of the safest forms of the digital data transmission and communication with the internet and other communication system in this digital world.

## Implementation



**Fig.4.1 Overview**

## Source Code:

* + 1. **Encryption at sender side along with Steganography**

It takes a text file and peforms encryption using vigener cipher and also takes an image to insert the encrypted text into the image to perform steganography.

global fullpathname2 %image global fullpathname4 %text FID = fileread(fullpathname4); str=uint16(FID);

global key key=[1:95;1:95;1:95;1:95;1:95;1:95;1:95;1:95;1:95;1:95;1:95;1:95;1:95;1:95;1:95;1:95;];

char(key); global keey2

for i=1:length(str) if i>17

index=i; i=mod(index,16); j=str(index)-32; keey2(index)=j;

enc(index)=mod((str(index)+key(i,j)),127); elseif i<=16

index=i; j=str(i)-32;

keey2(index)=j; enc(index)=mod((str(index)+key(i,j)),127);

end

end

global encstr encstr=char(enc);

set(handles.text10,'String',encstr);

set(handles.text9,'String',encstr); x=imread(fullpathname2) x=uint16(x); [x\_row,x\_col]=size(x)

c=numel(encstr) Str=encstr;

a=1;

%loop part is repeated for the size of image and goes on until it get to

%our character number for i=1:x\_row

for j=1:x\_col if(a<=c)

if(x(i,j)+Str(a)>255)

temp=x(i,j)+Str(a)-256; else

temp=x(i,j)+Str(a); end z(i,j)=uint8(temp);

else

z(i,j)=uint8(x(i,j)); end

a=a+1; end

end disp(z)

imwrite(z,'stegano\_coverr.png'); axes(handles.axes5); img=imread('watermark\_generated.png'); imshow(img);

## Decryption at receiver side along with Steganography

It takes a stegano image file and peforms extraction and decryption operation to get the human readable text.

x=imread('stegano\_coverr.png' y=imread('grayimage.jpg');

x=uint16(x); %Convert them to unit 16 format y=uint16(y); %Convert them to unit 16 format

[x\_row, x\_col]=size(x); %for processing total image i need toknow no of rows and cols. retrieve them.

b=0;k=1;

for i=1:x\_row-1 for j=1:x\_col-1

if(x(i,j)>=y(i,j))

a=x(i,j)-y(i,j); else

a=256+x(i,j)-y(i,j); end

if(a~=0)

z(k)=uint8(a k=k+1;

else

b=1 break;

end end if(b==1)

break; end

end

fid=fopen('decrypted.txt','w'); for i=1:k-1

fprintf(fid,'%c',z(i)); end

text = fileread('decrypted.txt') set(handles.text9,'String',text) axes(handles.axes5) img=imread('stegano\_coverr.png') imshow(img)

## Digital Watermarking generation at Sender Side

It takes a watermark image and a stegano image and generates a watermarked image finally to provide authentication.It can also calculates PSNR and MSE value.

clc; clear all;

warning off; chos=0; possibility=8;

while chos~=possibility,

chos=menu('Digital 3-level image watermarking','select the watermark image[1]','select the Cover image[2]','show 3-level coverimage[3]','show 3-level watermarkimage[4]','show watermarked image[5]','Calculate MSE for embedding[6]','Calculate PSNR for embedding[7]','exit');

if chos==1

[fname pname]=uigetfile('\*.\*','select the watermark Image'); imageinput=imread(fname);

imshow(imageinput); A=rgb2gray(imageinput); P1=im2double(A); P=imresize(P1,[2048 2048]);

[F1,F2]= wfilters('haar', 'd');

[LL,LH,HL,HH] = dwt2(P,'haar','d');

[LL1,LH1,HL1,HH1] = dwt2(LL,'haar','d');

[LL2,LH2,HL2,HH2] = dwt2(LL1,'haar','d');

end

if chos==2

[fname pname]=uigetfile('\*.\*','select the Watermark'); imw2=imread(fname);

watermark=im2double(imw2); watermark=imresize(watermark,[2048 2048]); [WF1,WF2]= wfilters('haar', 'd');

[L\_L,L\_H,H\_L,H\_H] = dwt2(watermark,'haar','d');

[L\_L1,L\_H1,H\_L1,H\_H1] = dwt2(L\_L,'haar','d');

[L\_L2,L\_H2,H\_L2,H\_H2] = dwt2(L\_L1,'haar','d');

save('test.mat','LL2','L\_L2') end

if chos==3

imshow(LL2,'DisplayRange',[]), title('3leveldwt of watermark image')

end

if chos==4

imshow(L\_L2,'DisplayRange',[]), title('3 level dwt of cover image') end

if chos==5 Watermarkedimage=LL2+0.0001\*L\_L2;

%computing level-1 idwt2 Watermarkedimage\_level1=idwt2(Watermarkedimage,LH2,HL2,HH2,'haar');

%computing level-2 idwt2 Watermarkedimage\_level2=idwt2(Watermarkedimage\_level1,LH1,HL1,HH1,

'haar');

%computing level-3 idwt2 Watermarkedimage\_final=idwt2(Watermarkedimage\_level2,LH,HL,HH,

'haar'); imshow(Watermarkedimage\_final,'DisplayRange',[]);

imwrite(Watermarkedimage\_final,'watermark\_generated.png'); setappdata(0,'watermark',Watermarkedimage\_final);

end

if chos==6 pic1= P;

pic2= Watermarkedimage\_final; mse=MSE(pic1,pic2)

end

if chos==7 pic1= P;

pic2= Watermarkedimage\_final; psnr=PSNR(pic1,pic2)

end

end

## Digital Watermarking extraction at Receiver Side

It takes a watermark image generates a stegano image and this image is sent to the decryption process and extracts the watermarked image separately. It can also calculates PSNR and MSE value.

clc; clear all;

warning off; chos=0; possibility=4;

while chos~=possibility,

chos=menu('Digital 3-level image watermarking',

'show extracted image[1]','Calculate MSE for extraction[2]', 'Calculate PSNR for extraction[3]','exit');

if chos==1 wimage\_final=getappdata(0,'watermark'); load('test.mat','LL2','L\_L2')

[F11,F22]= wfilters('haar', 'd');

[a b c d]=dwt2(wimage\_final,'haar','d'); [aa bb cc dd]=dwt2(a,'haar','d');

[aaa bbb ccc ddd]=dwt2(aa,'haar','d'); recovered\_image=aaa-LL2;

imshow(recovered\_image,[]); imwrite(recovered\_image,'watermark\_recovered.png'); title('extracted watermark')

end

if chos==2

end

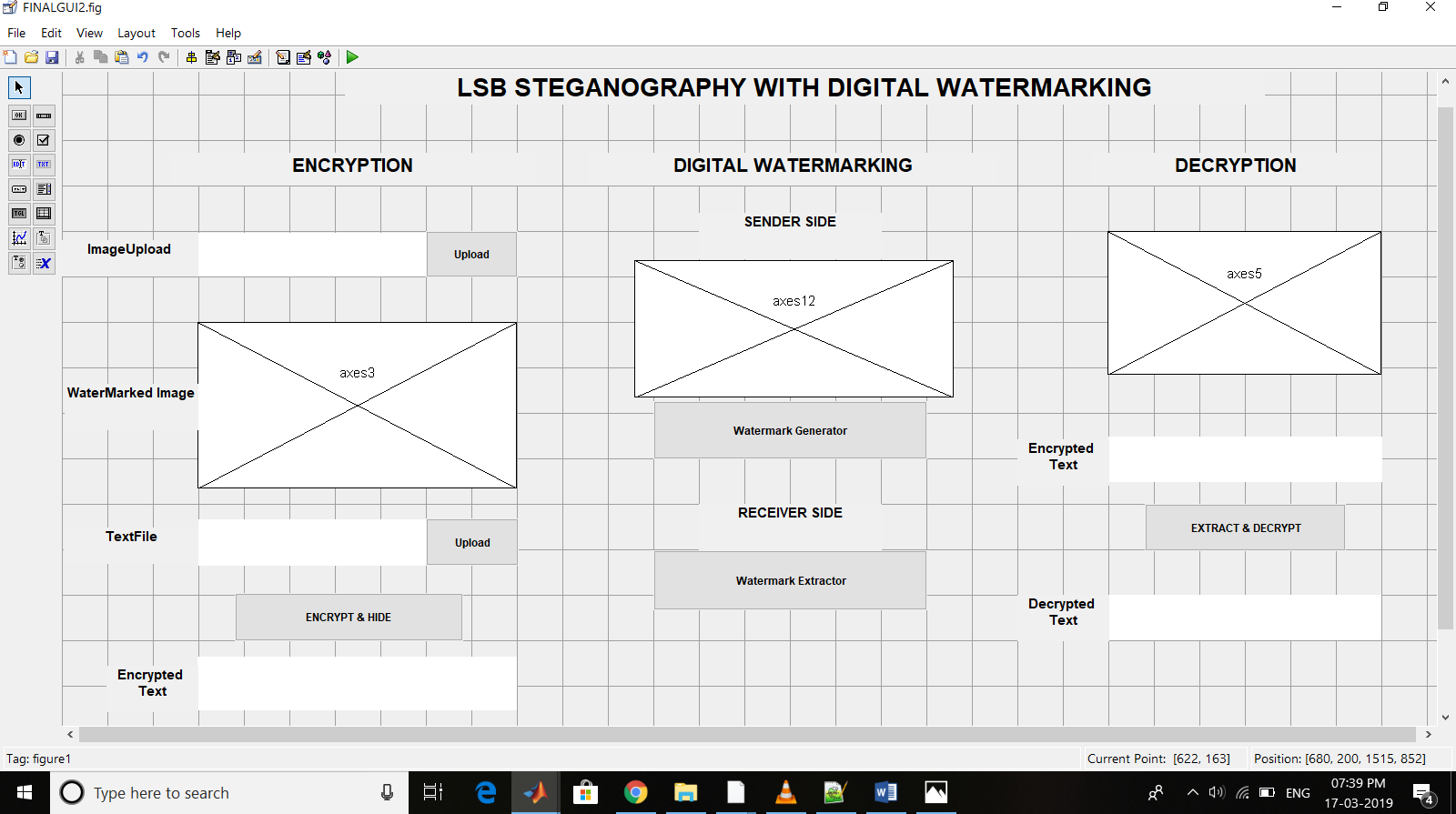
clear pic1; clear pic2; pic1=L\_L2;

pic2=recovered\_image; mse\_extraction=MSE(pic1,pic2)

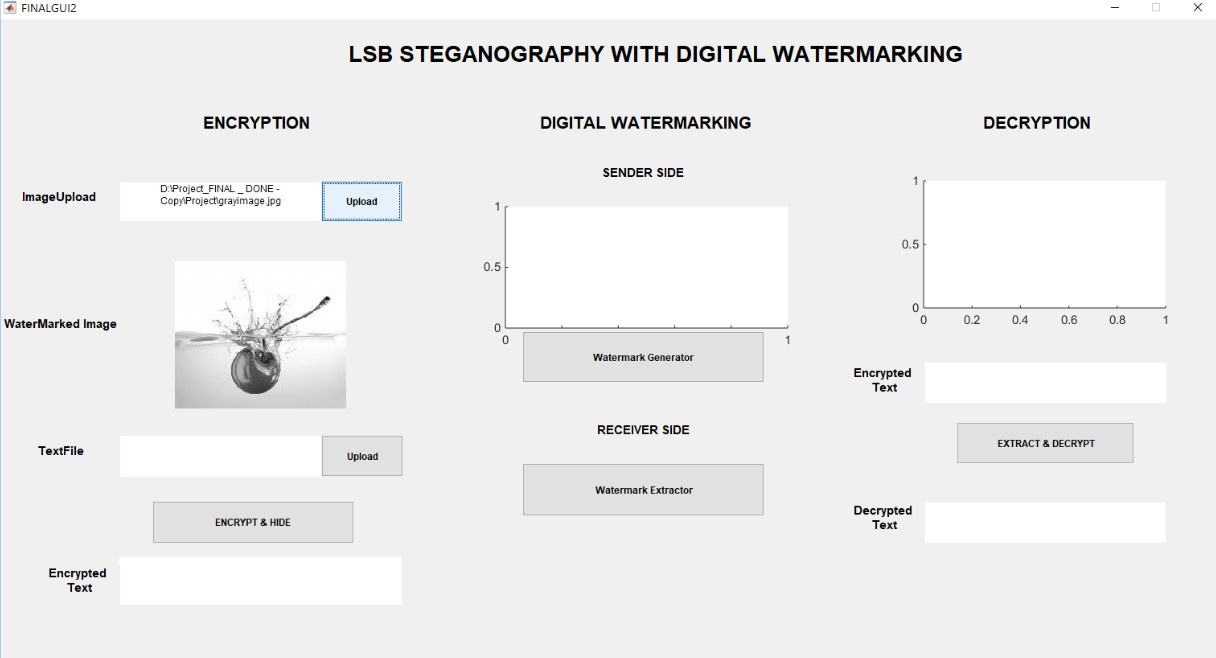
end

if chos==3 psnr\_extraction=PSNR(pic1,pic2) end

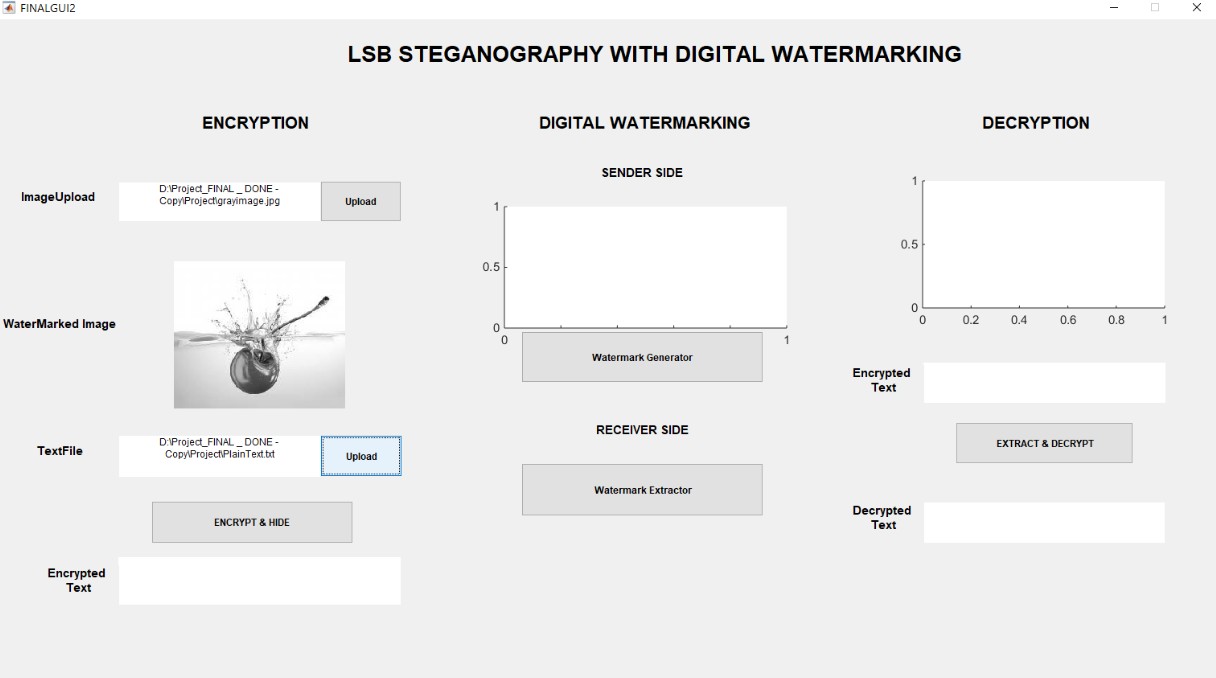
## Outputs and Results



**Fig.5.1 Design**

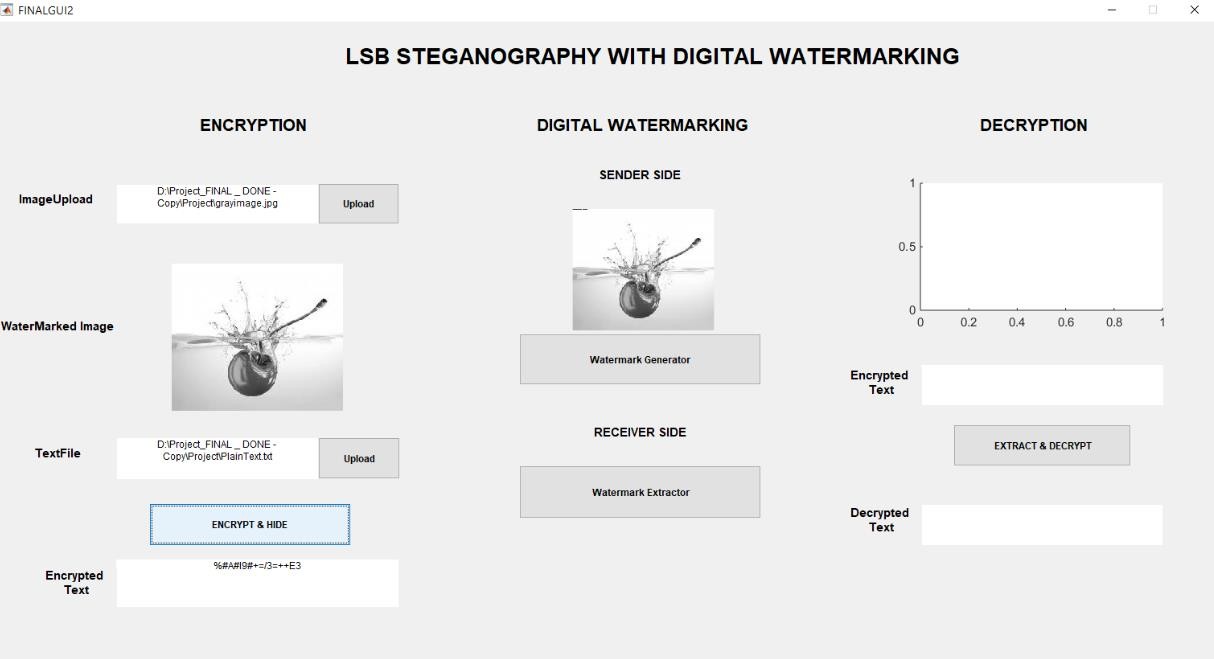


**Fig.5.2 Image Uploading**



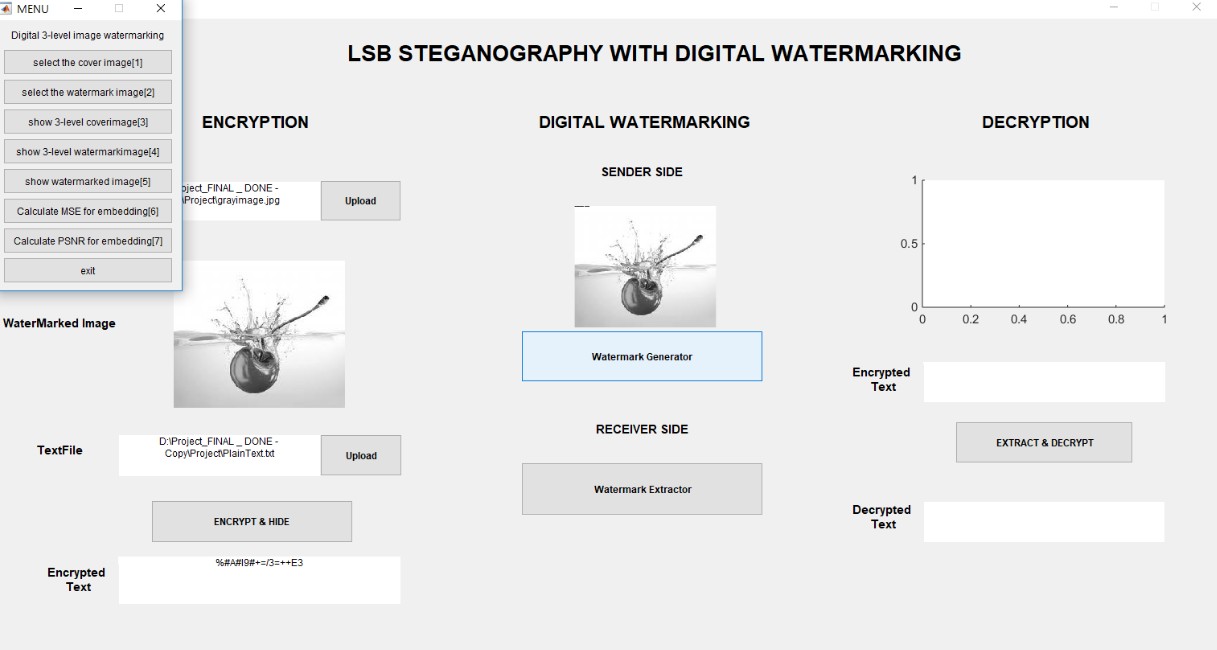
**Fig.5.3 Text File Uploading**

Encrypting the text and placing inside the LSB of the image , generation of stegano image.

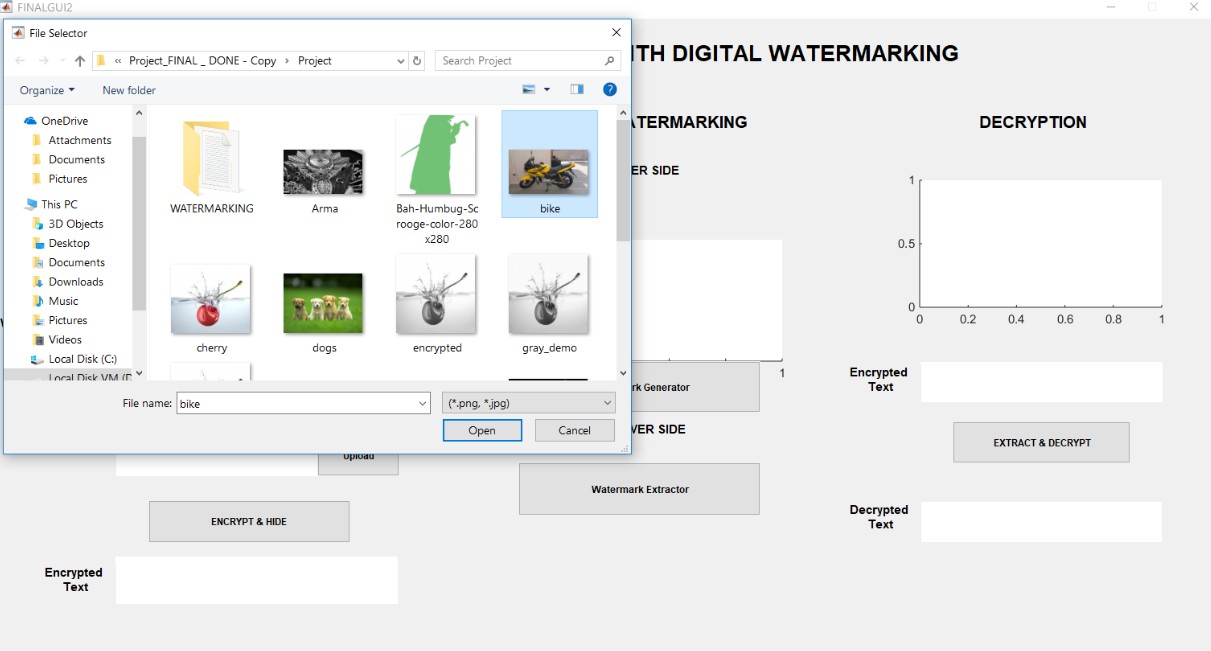


## Fig.5.4 Encryption along with Steganograpghy

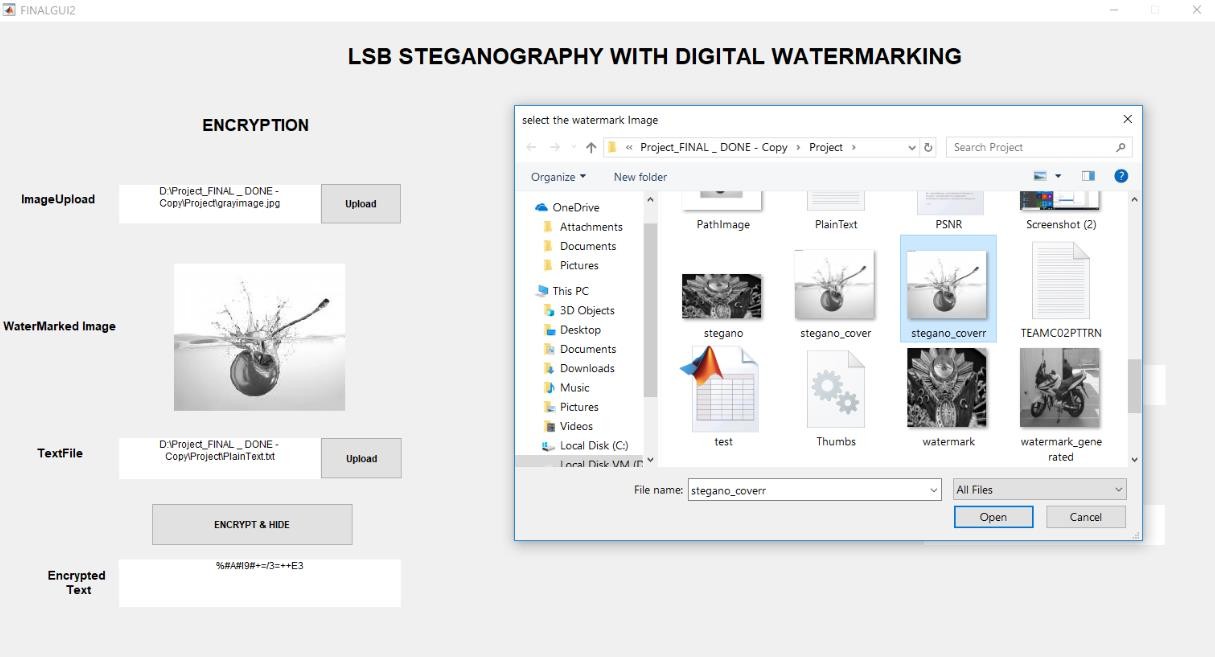
Watermark generation to the existing stegno image to provide the authentication.



## Fig.5.5 WaterMark Generation

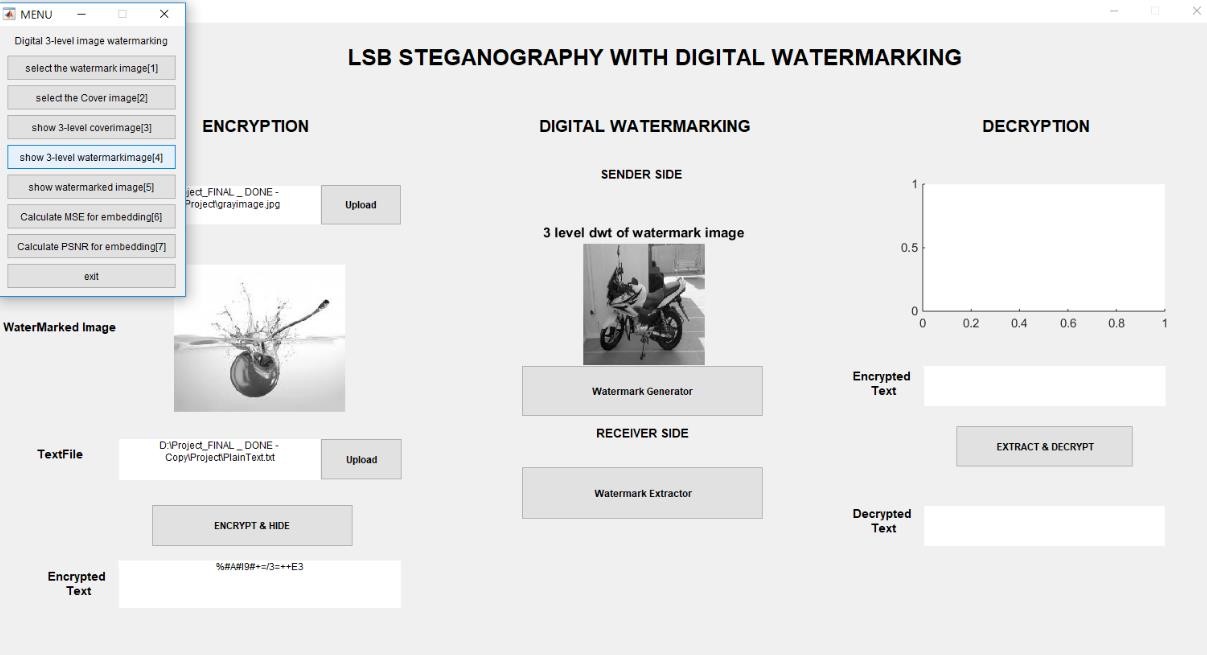


**Fig.5.6 Watermark Upload**

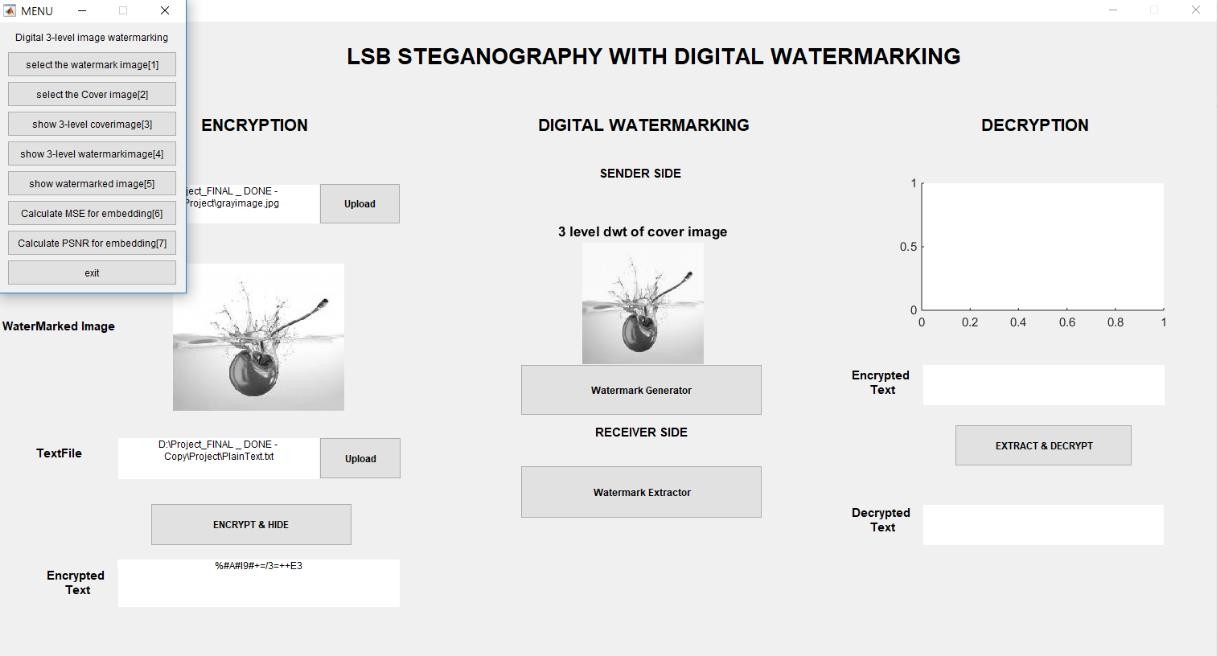


**Fig.5.7 Cover image Upload**

Performing 3 level DWT tranformation for inserting the cover image information at LL band.

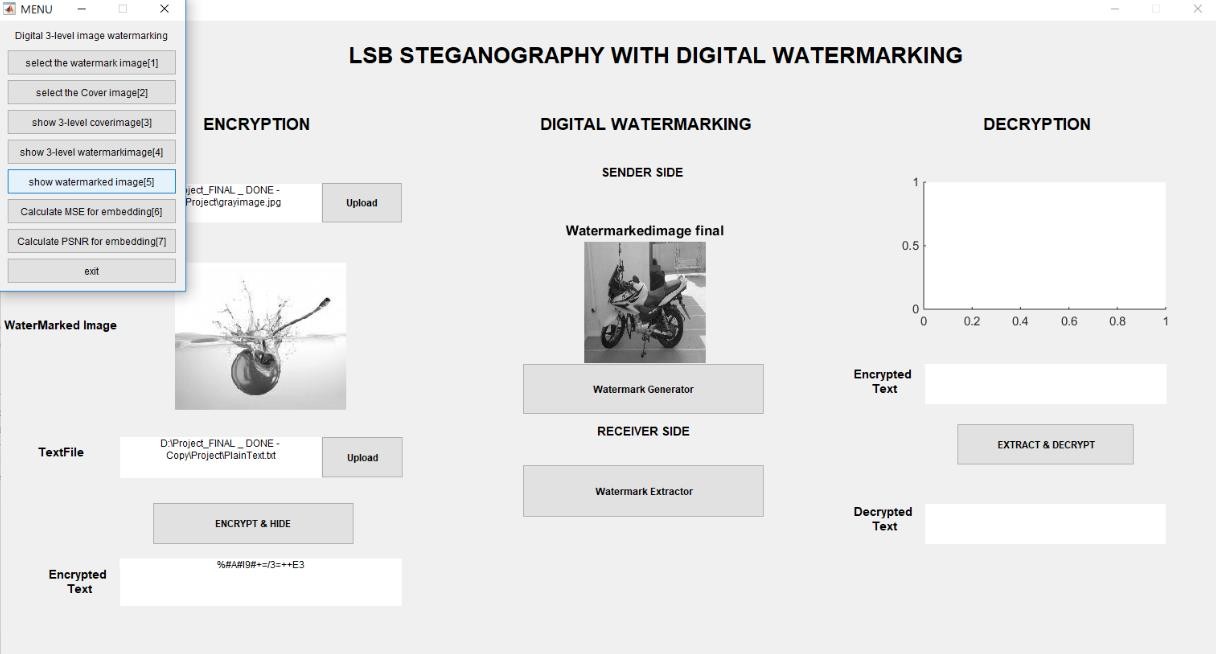


## Fig.5.8 3 level DWT transformation of watermark



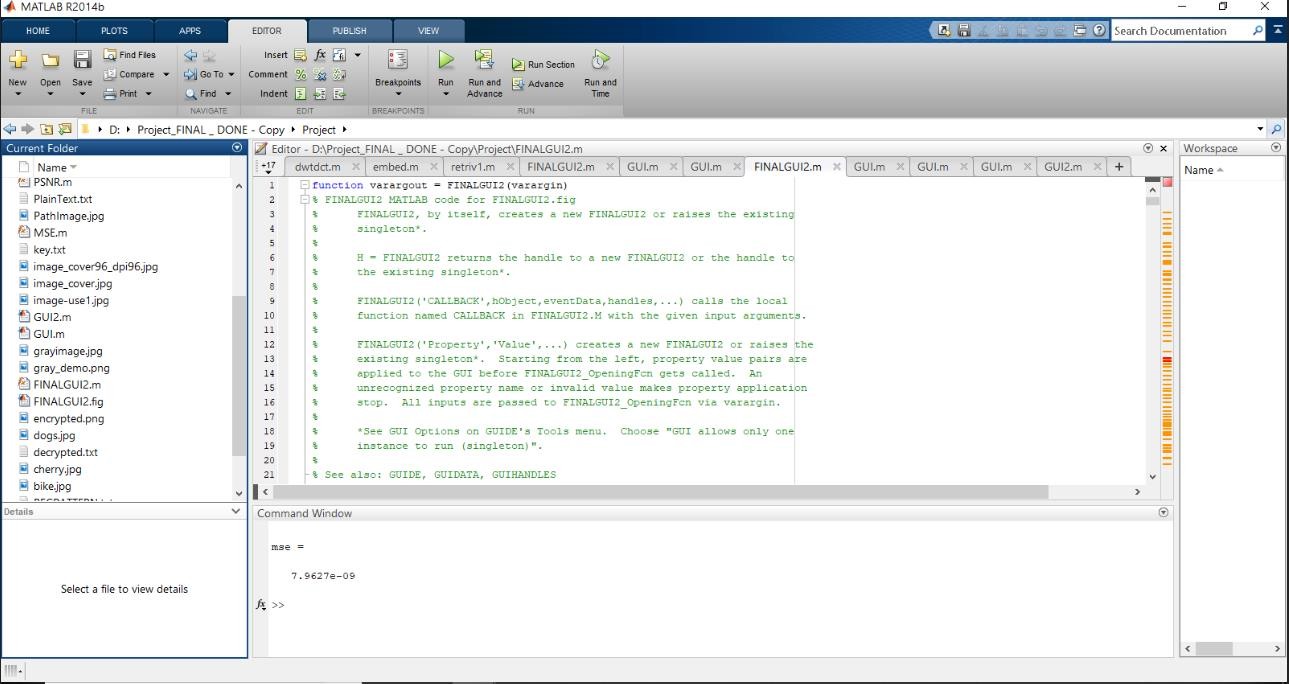
**Fig.5.9 3 level DWT transformation of watermark**

Watermark generated image is shown at the sender side and this image is tranmitted to the receiver.



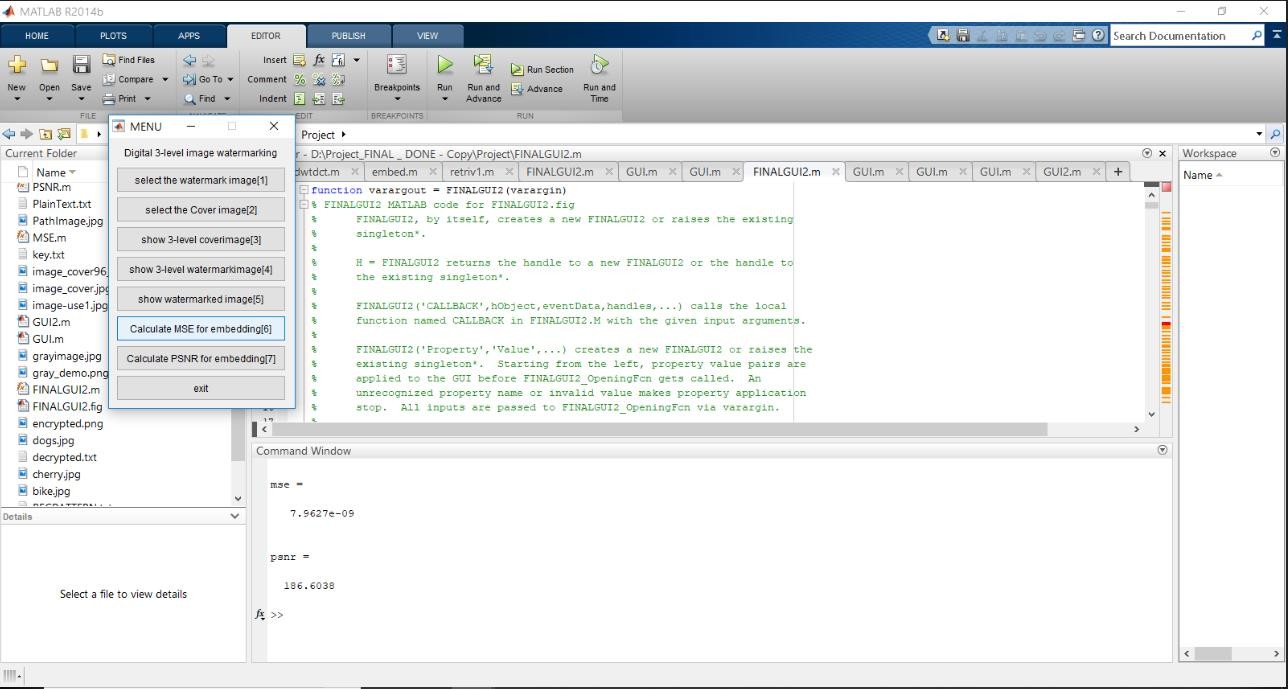
## Fig.5.10 Generated Watermark

Calculation of MSE can be computed by performing byte by byte comparison of the cover image and Final stego-image.at sender side.

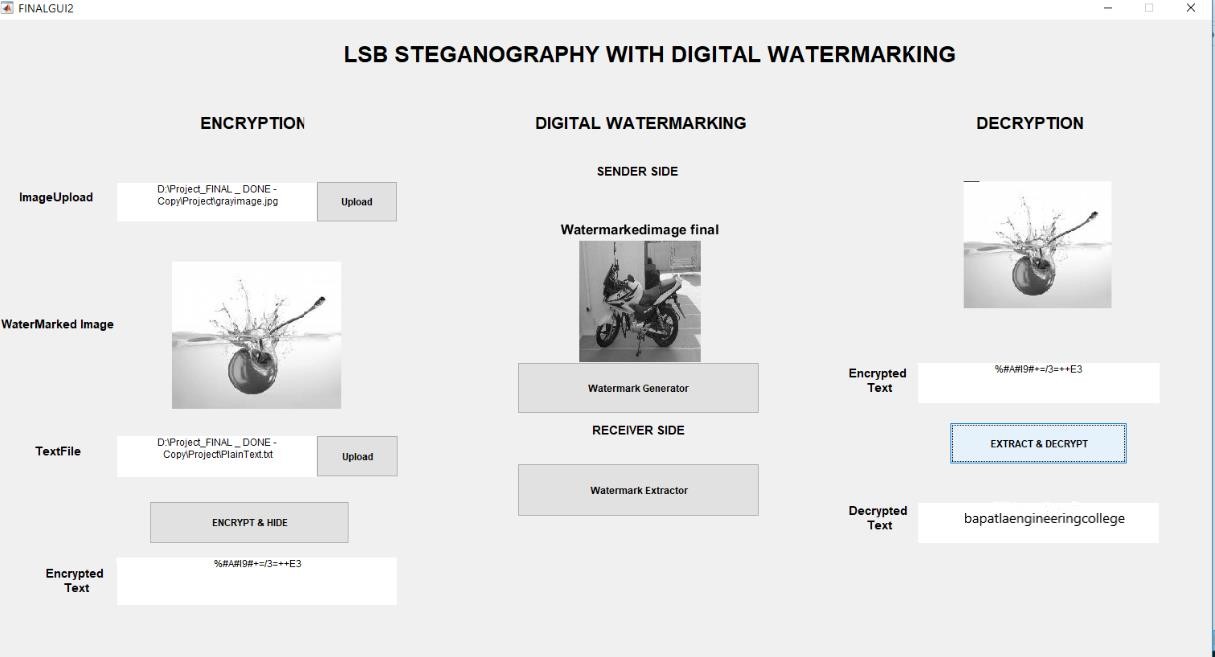


## Fig.5.11 Generated MSE value

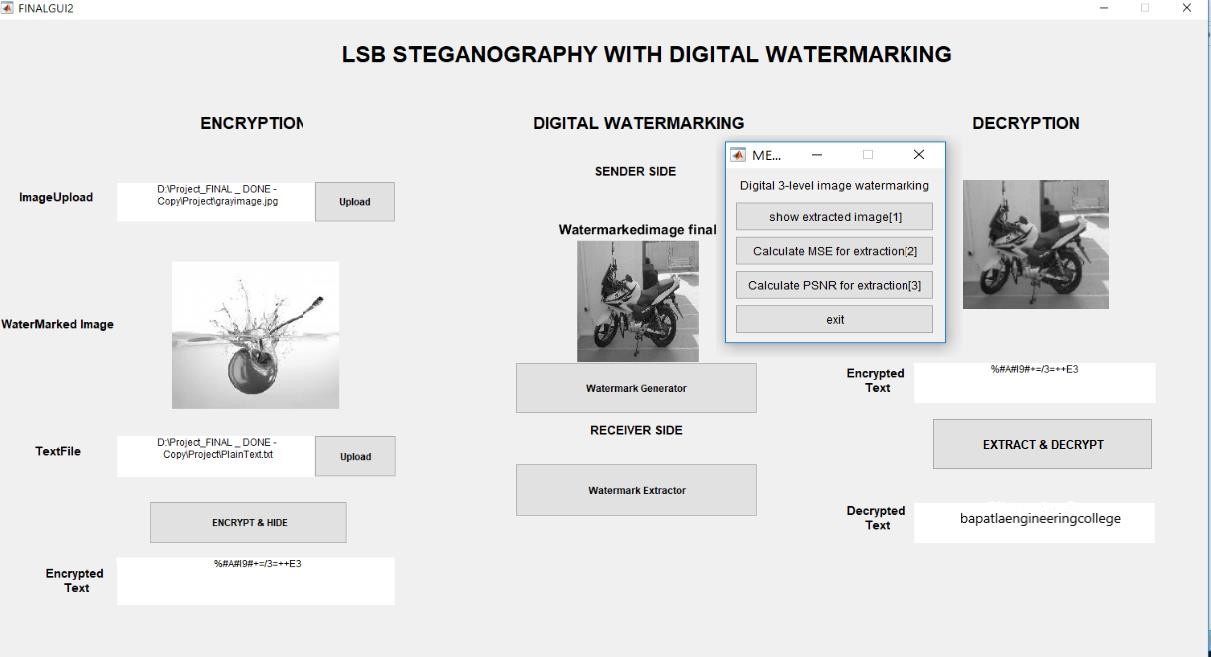
Calculation of PSNR measures the quality of the Final stegno-image with cover image at sender side.



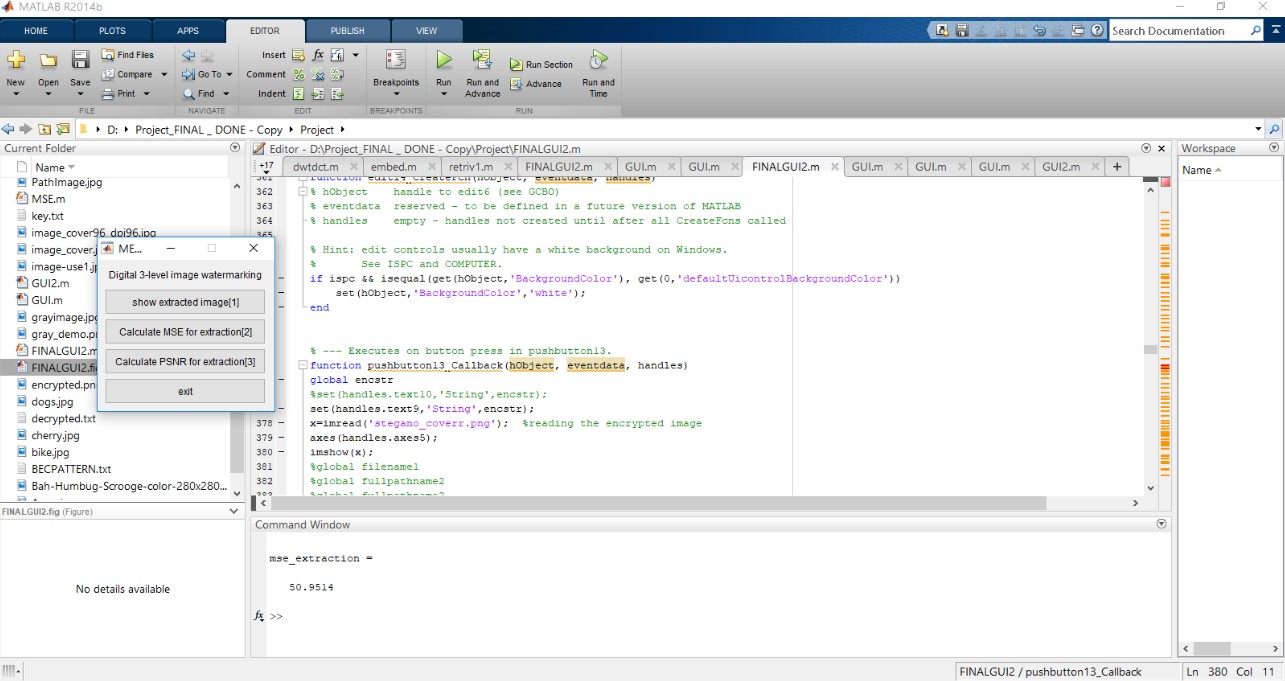
## Fig.5.12 Generated PSNR value



**Fig.5.13 Extraction and Decryption of text from the watermarked image**

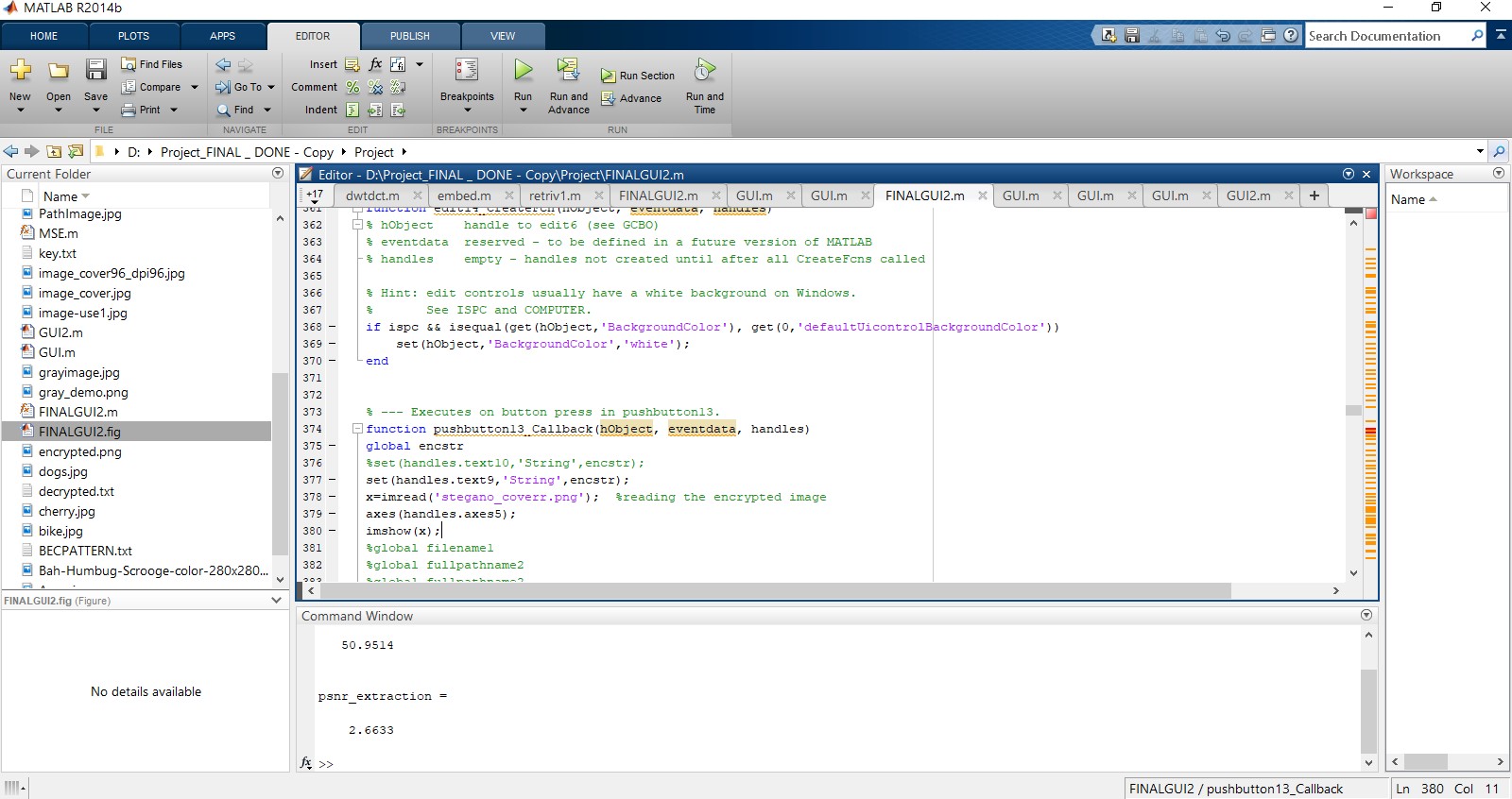


**Fig.5.14 Extraction of the watermarked image**

MSE can be computed by performing byte by byte comparison of the cover image and Final stego-image at the receiver side. The small value of MSE will represent more efficient image steganography technique.

## Fig.5.15 Generated MSE value

Calculation of PSNR measures the quality of the Final stegno-image with cover image at receiver side. If PSNR value is higher, then the quality of an image will be better.



## Fig.5.16 Generated PSNR value

## CONCLUSION

During data transmission if data is intercepted then it can be used successfully by an unauthorized person over the internet. Therefore to provide more security to the information at the time of communication over unsecured channel a Steganography and digital watermarking advance technique for data security is needed. In this paper, proposed highly secured data hiding both steganography and digital watermarking scheme which is based on status LSB and 3-D Haar-DWT algorithms. A new stegno-digital watermarking is a technique which combines steganography and digital watermarking that offers an ideal system for secret data transmission with respect to stand-alone cryptographic and steganographic techniques. This technique hides the secret message in binary form in two cover images due to which double protection has been provided to confidential data. The Final Stego-image is looking perfectly intact and has high PSNR value and low MSE value. Hence, an unintended observer will not be aware of existence of the secret message inside the cover image. The extracted secret data is perceptually similar to the original secret data. This method is one of the safest forms of the digital data transmission and communication with the internet and other communication system in this digital world.

## REFERENCES

1. Modified Vigenere Encryption Algorithm and Its Hybrid Implementation With Base 64 And AES. Gurpreet Singh,Computer Science and Engineering Department, Sri GuruGranth Sahib Worldwide University, Fatehgarh Sahib,Punjab, INDIA.
2. Zhang, T., Li, W., Zhang, Y. and Ping, X.; “Detection of LSB Matching Steganography Based on Distribution of Pixel Difference in Natural Images”. International Conference on Image Analysis and Signal Processing (IASP), Pp.629-632,2010.
3. Johnson, N.F. and Katzenbeisser, S.C.; “A survey of steganographic Techniques”, International Journal of Computer Applications, 2004.
4. Digital Image Watermarking: An Overview H. B Basanth Kumar,Pooja Bhagavat Memorial Mahajana Education Centre,DoS in Computer Science, KRS Road, Metagalli, Mysuru 570016

, India. \*Corresponding author [E-mail:basanth.10@gmail.com,](mailto:basanth.10@gmail.com) <http://dx.doi.org/10.13005/ojcst/901.02>

1. Dual Steganography Technique Using Status LSB and DWT Algorithms

Manisha#1, Deepkiran Munjal\*2,M Tech Scholar, Dept. of Computer Science & Engineering, BSAITM, M.D.U. Rohtak, Faridabad, India#1,Assistant Professor, Dept. of Computer Science & Engineering, BSAITM, M.D.U. Rohtak, Faridabad, India\*2.