LSB Steganography – Message Encryption in images

Challa Karthik
BTech computer science at VIT, India

Dr. Suresh Kumar Nagarajan
Associate Professor at VIT, India

ABSTRACT: Steganography is the technique of encrypting data in a data carrier (an image, in this case) in such a manner that it is impossible for an outsider to identify that a message has been encrypted into the image. The data carrier may also be an audio file or a text file, however, an image file has been considered for the following. This technique is different from other data hiding methods like watermarking, in the way that it is far subtler. The watermark's presence is often broadcasted entirely over the image, which prevents any communication/message to be secretive or discreet. Steganographic techniques are used to hide a large amount of data or files secretly into some innocuous looking digital medium such as images.

In this paper, I am providing an up-to-date review and analysis of this image encryption using steganography technique.

Keywords: The objective of this project is to attempt to successfully, discreetly encrypt a text message into an image file, and also decrypt the same text from the encrypted file using the least significant bit algorithm. The implementation overwrote the image file's bits based on the secret message's bits.

INTRODUCTION: Image steganography is the most popular form of its kind, and consists of two components – the cover image and the secret file. This secret file could be text or audio or image. This is the data that must be encrypted into the cover image. The bits of this secret file are embedded in the bits of the cover image by modifying the content of the least significant bit, in the case of the LSB Algorithm. In the Lowest Significant Bit algorithm, the information is hidden in the last bits of the pixels in the cover image**.** The LSB is the least significant bit in the byte value of a pixel in the image. In a 24-bit image, the three basic colors present that contribute to 24 bytes (8 + 8 + 8) are Red, Green and Blue. Each represents 1 byte. An 800 x 600 image can store 1440000 bits of encrypted information consequently. A change in the LSB of a pixel is evidenced by minor changes in the intensity of the colors. These changes are usually too little to be detected by the naked eye, and thus the steganogramme is generated.

LITERATURE SURVEY: Here in the first paper it is discussing about the modern steganography which is purely different from cryptography. The goal of cryptography is to secure communications by charging the data into a form that eavesdropper cannot understand. Steganography techniques, on the other hand, tend to hide the existence of the message itself, which makes it difficult for an observer to figure out where the message is. In some cases, sending encrypted information may draw attention, while invisible information will not. Accordingly, here we see that cryptography is not the best solution for secure communication; it

is only part of the solution here it is stated that both sciences can be used together to better protect information. It stated that even if steganography fails, the message cannot be recovered because the cryptography technique is used as well.
Next paper discusses about the various techniques which are capable of hiding the data within an image which have been classified on the basis of the following algorithms one is spatial based domain technique and second one is transform domain based techniques ,here the main classification of spatial domain based is steganography technique use either the LSB or Bit plane complexity segmentation algorithm, it goes in depth about the usage of LSB where LSBs of the cover the file directly changed with message bits. A significant number of methods have been proposed for LSB steganography it has proposed that the RGB true color image by enhancing designing of robust and secure image steganography based on LSB insertion and RSA encryption technique has been used. In this proposed matching which is been revisited image steganography and edge adaptive scheme which can select the embedding regions according to the size of secret message and the difference between two consecutive pixels in the cover image. In two steganography technique proposed for hiding image in an image using LSB method for 24-bit color images. Here a hash based approach proposed for secure keyless steganography in lossless RGB images that an improved steganography approach for text messages in lossless RGB images. This paper provides an overview of image steganography, its uses and analysis of various steganography techniques.

It deals with the security of text messages at the time of sending it over the network, they have asymmetric key cryptography which means different keys are needed to encrypt and decrypt the data. Here they have divided the domain of the key selection into different sub domains, we can consider a random prime number and we can take it as a decimal value of the pixel. Here in this approach they have given strength on division of the domain together with the key length but their concept so that encrypt the original text message letter by letter applying a function which involves complexity of the data hiding techniques. The generated number or according to the concept they encrypt the original text message letter by letter applying a function which involves certain mathematical operations using corresponding letters and also numbers from the original image. Then, they use two public keys and one private key for encryption and decryption. These keys are generated randomly following some constraints and equations. For encryption and decryption, we have used a mathematical operation called Multiplicative Modulo in between the text and the generated keys.

Here in this paper their research work reviewed many papers on steganography techniques, by this they have observed that most of the steganography work is done in the year 2012 and 2013. In these years, LSB is the most widely used technique, spatial technique for steganography here some researchers have also used the techniques like water marking, distortion technique, spatial technique, ISB, MSB in their work and provided a strong means of secure information transmission. Most of the papers that are discussed here are taken from IEEE Explore, AICCSA, IJET, IJCSE, IJCA etc.

These papers provide a lot of help to the initiator for starting their work in this field. This review paper is enough for them to start their work in this field. The different security and data hiding techniques are used to implement steganography using LSB, ISB, MLSB in further research they are going to use more advance schemes like steganography with some hybrid cryptographic algorithm for enhancing the data security.

In this paper they describe about the “A GA Based Audio Steganography with enhanced security”. Here they take a text file as a text message, using RSA encryption algorithm encrypt the text message and store the encrypted text message into another file "encrypt.txt". Now they read the audio .wav file byte wise, and convert the encrypted text file into byte. Then applying proposed LSB algorithm, embed message bits to the audio bit steam in random positions (to increase the robustness) to get the stego-audio, here Genetic Algorithm operators are used to minimize the bit level deviation occurred between host audio and stego-audio. Now to get the original message apply reverse LSB method and Characteristics of steganography can be expressed as hereunder: Carrier File—A file which has hidden information inside of it. Steganalysis—The process of detecting hidden information inside of a file.

Stego-Medium—The medium in which the information is hidden. Redundant Bits Pieces of information inside a file which can be overwritten or altered without damaging the file. Payload—The information which is to be concealed. Steganographic algorithms can be characterized by a number of defining properties. Three of them, which are most important for audio steganography algorithms, are defined below. Transparency evaluates the audible distortion due to signal modifications like message embedding or attacking. In order to meet fidelity constraint of the embedded information, the perceptual distortion introduced due to embedding should be below the masking threshold estimated based on the HAS/HVS and the host media. Capacity of an information hiding scheme refers to the amount of information that a data hiding scheme can successfully embed without introducing perceptual distortion in the marked media.

Here it describes the use of steganography which as A hash based least significant bit technique is proposed. A color image is considered as a cover media and secret data is embedded in this cover media as payload. The proposed technique takes eight bits of secret data at a time and put them in LSB of RGB (Red, Green and Blue) pixel value of the cover image in order respectively. The detailed technique has been depicted. This distribution pattern is taken because it is giving better results in terms of MSE and PSNR. The proposed method is not tested for the case of compressed images. The need for information security is increasing day by day as many people are depending on internet for their daily needs. An algorithm hash based least significant bit image steganography is proposed. The proposed algorithm provides better results compared previous method in terms of MSE and PSNR, NAE, SSIM values. The results of proposed method and method are provided. With a comparison between the proposed algorithm and previous technique considered by this study, the proposed technique shows promising results. There is a drastic improvement in MSE and PSNR values. As an example in case of Cover image pic400.jpg and secret image lena128.jpg, proposed method gets MSE value as 3.7532 and previous method gets MSE value as 11.1738. So we can conclude that proposed method provides clearly better results. About security enhancing, as a future work Implementing an encryption algorithm for providing more security for secret image can be done.

The potential of steganography is evident at hiding the existence of confidential data, the difficulty there exists in detecting the presence of hidden data, and the enhancement in security due to the increase in difficulty of decrypting the encrypted data. Steganography is also used in modern printers, wherein brand color Laster printers add small yellow dots to each page. These dots encode printer serial numbers and date-and-time stamps for traceability and additional information. Steganography is also used in digital watermarking messages, acting as identifiers, by hiding in images and allowing images to be tracked and verified. Reports from the Federal Bureau of Investigation also claim that the Russian Foreign Intelligence service use customized steganography software to encrypt text messages inside cover images for discreet communication with agents stationed abroad

Another context of the paper taken describes the random pixel selection as Steganography is an art and science of writing hidden messages in such a way that no one apart from a intended recipient will know the existence of the message which will be a growing need for the security of a data image, steganography is a gaining popularity. The goal of steganography is to communicate securely in a completely undetectable way and to first avoid a drawing suspicion to the transmission of a hidden data in the process. This will enable the idea of data hiding is not a novelty; it has been used for centuries all across the world under different regimes but up to date it will be a unknown to most of the people i.e. tool for hiding the information so that it does not even appear to be existed. However, steganography will be operating at a complex level as its detection will be dependent on recognizing the underlying hidden data.

Historical tricks will also include all the invisible inks, tiny pin punctures on the selected characters, minute differences between handwritten characters, pencil marks on type written characters, grilles which cover the most of messages except for a few characters, and so on. This Steganography is a different concept from cryptography. The objective of cryptography is to secure communications by changing the data into a form so it cannot be understanding by an eavesdropper properly. On the other hand, steganography techniques will tend to hide the existence of the message itself, which would make it difficult for an observer to find out where exactly the message is encrypted. The information which is been hidden in the cover data is known as “embedded” data.

Analysis on A novel hash based least significant bit (2-3-3) image steganography in spatial domain gives a brief description about the steganography that The “steno” data is the data containing both cover signal and “embedded” information. Apparently, it is the process of putting the hidden or the embedded data, into the cover data, and it is sometimes known as embedding process. Occasionally, when referring to image steganography, the cover image is known as the container. The term “cover” will be used to describe the original, innocent message, data, audio, still, video etc. When we referring to an audio signal steganography the cover signal is sometimes called “host” signal. Cryptography was being created as a technique for securing the secrecy of the communication and many different methods have been developed to encrypt and decrypt the data in an order to keep the encrypted message secret.

Unfortunately, it is sometimes not capable to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement is called steganography. Steganography is a technique where it is used to hide information within images. Using this stenography, watermarks and copyrights can be placed on an image to protect the rights of its owner without altering the appearance of the image. Almost like a magic, images, executable programs, and text messages can hide in images. This cover image does not appear to be altered. Few people look at the cover image and never suspect something is hidden in it. Your information is hidden in plain sight.

PROBLEM STATEMENT: My papers main objective is to encrypt a message in an image using LSB steganography technique

- **Research Framework/Architecture:**

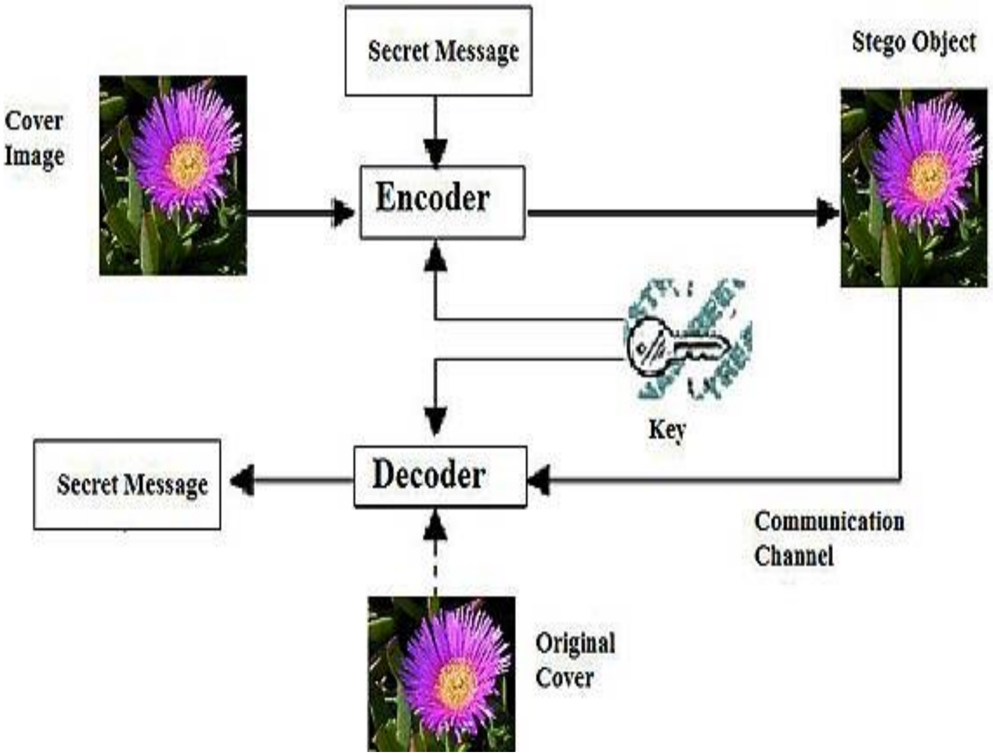


Figure.1

- **MODULES:**

Encoder: It is used to encrypt any secret message which can be a text or a number which is confidential and is used to store any type of data in one format to another format.

Decoder: It is used to extract the message which is stored
in the encrypted image.

LSB Steganography Algorithm:
LSB-Steganography is a steganography technique in which we hide messages inside an image by replacing Least significant bit of image with the bits of message of an image.We can insert our secret message and it also make the picture unnoticeable, but if our message is too large it will start modifying the second right most bit and so on and an attacker can notice the changes in picture

- **ALGORITHM:**

1) Encoding Algorithm

```
Begin
Load the cover image
Convert image to byte array
Convert message data to byte array
If message cannot be contained in cover image
 Exit with error message
 Else
 For each bit in the message byte
 Begin
 If LSB
Hide message bit in the lsb of the corresponding cover image byte
 If MSB
Hide message bit in the msb of the corresponding cover image byte
If HYBRID
 Get two message bits
Hide the first message bit in the lsb of the corresponding cover image byte
Hide the second message bit in the msb of the corresponding cover image byte
 End
 End
```

2) Decoding Algorithm

```
 Begin
Load stego image
Convert stego image into byte array
If decoding type is LSB
 Begin
 For the first 32 byte
Copy the lsb into an array of length 32
Convert the array into integer value
```

```
Create an array of length of the integer value
 Starting from length 32+1 of the stego-
 image array
 Begin
Copy the lsb of the equivalent stego array into an array of length 8
Convert the array into a byte value and save in the corresponding index of the
created array
Convert the array value into string or image
End
End
```

- **FORMULA:**

1) Mean-Squared Error (MSE)

$$MSE = \sum M, (N[l1(M.N) - l2(M, M, N)]^2)/(M \times N)$$

2) Peak Signal-to-Noise Ratio [PSNR]

$$PSNR = \frac{10\log_{10}R^2}{MSE}$$

- **IMPLEMENTATION:**

a. Take an input image.

b. Find out the pixel values.

c. Select the pixel on which we want to insert data.

This process of selection of pixel is done as user's choice he may choose pixel continuous or alternate or at a fixed distance.

i. Insert the data values in pixels e.g.

For example, a grid for 3 pixels of a 24-bit image can be as follows:

00101101 00011100 11011100

10100110 11000100 00001100

11010010 10101101 01100011

When the number 200, which binary representation is 11001000, is embedded into the least significant bits of this part of the image, the resulting grid is as follows:

00101101 00011101 11011100

10100110 11000101 00001101

11010010 10101100 01100011

In the Lowest Significant Bit algorithm, the information is hidden in the last bits of the pixels in the cover image. The LSB is the least significant bit in the byte value of a pixel in the image. In a

24-bit image, the three basic colors present that contribute to 24 bytes (8 + 8 + 8) are Red, Green and Blue. Each represents 1 byte. An 800 x 600 image can store 1440000 bits of encrypted information consequently. A change in the LSB of a pixel is evidenced by minor changes in the intensity of the colors. These changes are usually too little to be detected by the naked eye, and thus the steganogramme is generated.

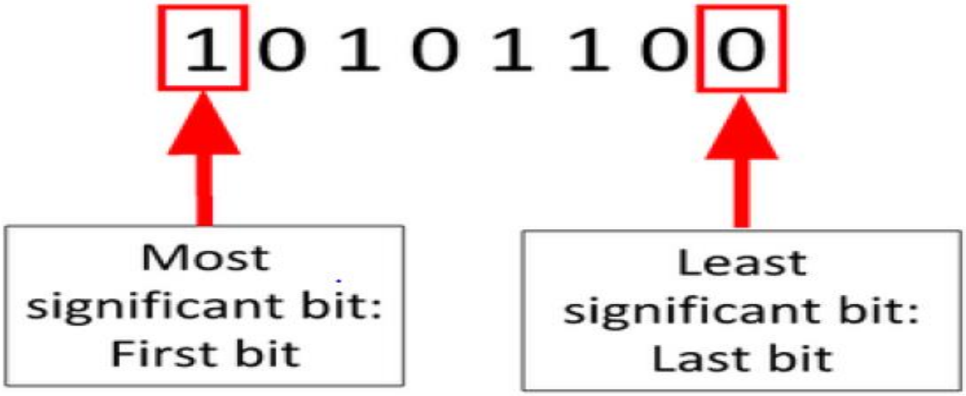

1 0 1 0 1 1 0 0
Most significant bit: First bit
Least significant bit: Last bit

Figure.2

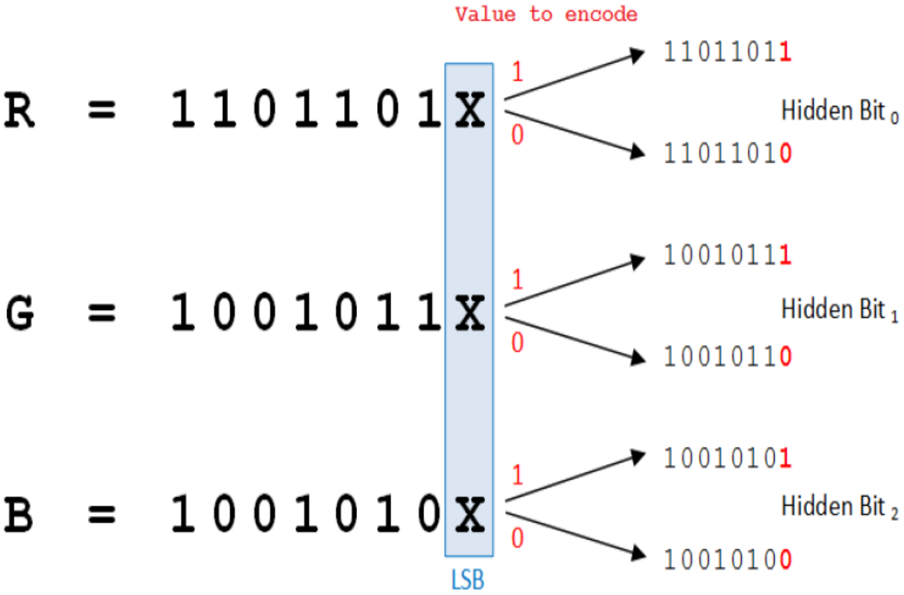
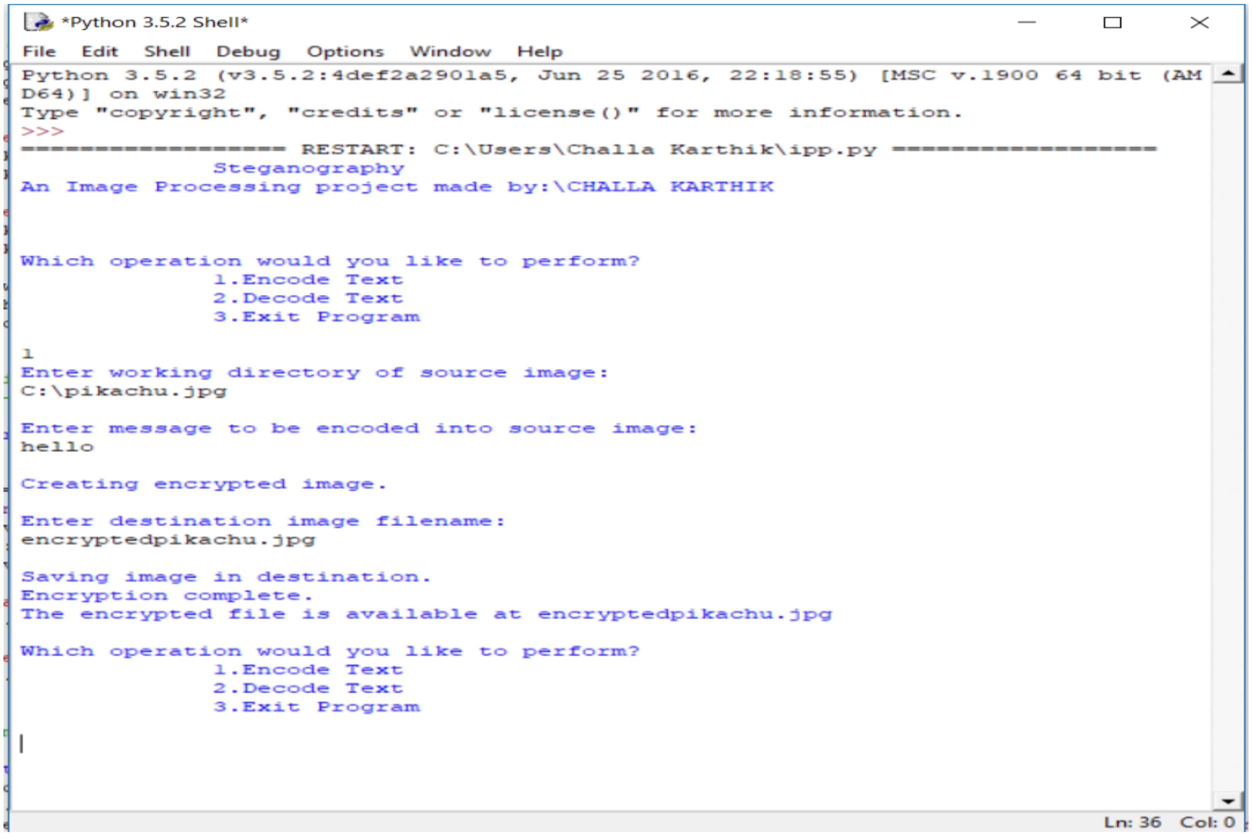


Figure.3

SCREENSHOTS:



```
Python 3.5.2 (v3.5.2:4def2a2901a5, Jun 25 2016, 22:18:55) [MSC v.1900 64 bit (AM
D64)] on win32
Type "copyright", "credits" or "license()" for more information.
>>> 
================== RESTART: C:\Users\Challa Karthik\ipp.py ==================
             Steganography
An Image Processing project made by:\CHALLA KARTHIK


Which operation would you like to perform?
             1.Encode Text
             2.Decode Text
             3.Exit Program

1
Enter working directory of source image:
C:\pikachu.jpg

Enter message to be encoded into source image:
hello

Creating encrypted image.

Enter destination image filename:
encryptedpikachu.jpg

Saving image in destination.
Encryption complete.
The encrypted file is available at encryptedpikachu.jpg

Which operation would you like to perform?
             1.Encode Text
             2.Decode Text
             3.Exit Program

|
```

Figure.4 (program execution)

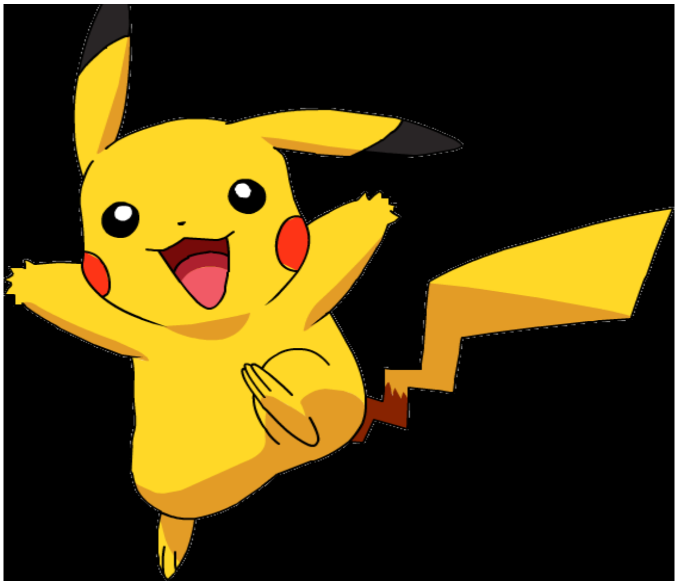


Figure.5 Encrypted text message in the following image(Pikachu.jpg).

Figure.6 Decoded text image by LSB algorithm message as “hello”.

LIMITATIONS: The primary issue however is that the LSB method limits the size of data that can be encrypted to about 1/8th of the size of the cover image, as each pixel can only store one bit of encrypted information in its last bit, and consequently, the larger the message to be encrypted, either the cover image must be larger, or more number of bits must be used from the cover image to hide more in lesser space. However, the problem with using more number of bits to store the encrypted image/message in the cover image, is that as the number of bits used to store the encrypted message increases, the likelihood of the image being morphed and modified being detected also increases, consequently lowering its subtlety. Thus, this is the largest limitation of this algorithm.

RESULT: The above implementation only implements text encryption however image encryption and potentially audio encryption are also feasible possibilities provided the size of the message is lesser than the one-eighth the size of the image.

FUTURE WORK: Yet, its applications are many, and the algorithm is found to be used in the following -

- Secret data storing and communication
- Media database systems
- Access control systems for digital content distribution and marketing

Reports from the Federal Bureau of Investigation also claim that the Russian Foreign Intelligence service use customized steganography software to encrypt text messages inside cover images for discreet communication with agents stationed abroad.

Conclusion: The potential of steganography is evident at hiding the existence of confidential data, the difficulty exists in detecting the presence of hidden data, and the enhancement in security due to the increase in difficulty of decrypting the encrypted data. Steganography is also used in modern printers, wherein brand color Laster printers add small yellow dots to each page. These dots encode printed serial numbers and date-and-time stamps for traceability and additional information. Steganography is also used in digital watermarking messages, acting as identifiers, by hiding in images and allowing images to be tracked and verified.

References: [1] Image Steganography Techniques: An Overview-Nagham Hamid, Abid Yahya, R. Badlishah Ahmad & Osamah M. Al-Qershi, 06 October 2016.

[2] A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique, Anil Kumar, Roshini Sharma, 7th July 2013.

[3] Text Steganography: A Novel Approach, Debanath Bhattacharya, Poulomi Das. Samir Kumar Bandyopadhyay and Tai-hoon Kim, Computer Science and Engineering Department, Hannam University, Darejon, Korea, February ,2009.

[4] Steganography Techniques, Jasleen Kour, Deepankar Verma, Mtech computer Science, R.B.I.E.B.T, India, May 2014.

[5] A GA based audio steganography with enhanced security, Krishna Bhowal, Debnath Bhattacharya, Anindya Jyoti Pal, Tai-Hoon Kim, 23rd July 2011.

[6] A novel hash based least significant bit (2-3-3) image steganography in spatial domain, G.R. Manjula and Ajit Danti, 1st February 2015.

[7] A survey on performance analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique, B. Padmavathi, S. Ranjitha Kumari, April 2013.

[8] Analysis of LSB based image steganography techniques, R. Chandramouli, Nasir Memon, February 2011.

[9] An improved image steganography method based on LSB technique with random pixel selection, 3rd November 2016.

[10] New LSB based color image steganography method to enhance in payload capacity, security and integrity check, Mustafa Cem Kasapbasi and Wisam Elmasry,27th April 2018.