RESEARCH ARTICLE OPEN ACCESS

# Data Hiding Technique for Security by using Image Steganography

Nikhil D. Rahate*, Prof. P. R. Rothe**
*(M-Tech V. L. S. I. (4th) Dept.of Electronics Priyadarshini College of Engineering. Nagpur.
nikhil_rahate87@yahoo.co.in)
** (Dept. of Electronics Priyadarshini College Of Engineering. Nagpur
p_rrothe@rediffmail.com)

ABSTRACT
In a developing era of engineering and technology many techniques had been develop to replace older security systems for secret communication with the help of signal processing. Older techniques like Cryptography, watermarking, etc are inefficient at certain levels. To overcome their disadvantages we propose a highly secure method for secret communication "Steganography".

Technology is a double edge sword which can be used and misused depending on user. Steganography is an example of this sword such as in field of media where copy righting ensures authenticity. On the flip side, many a terrorists and anti-humanists activities have been carried out under this technique. Data hiding systems take advantages of human perpetual weaknesses, but weaknesses of their own. It seems that no system of data hiding is totally immune to attack. The advantage of Steganography is that it can't be used to secretly transmit messages without the fact of transmission being discovered.

***Keywords*-**Steganography, Data Hiding, Security System, Image Based Security System.

## I. INTRODUCTION

In today's life structure everyone is connected with each other through various modes of communication like LAN, WAN and INTERNET. These are widely used for point to point communication of information around the world. Such communication networks are open which any one can access easily. Such open point to point communication networks are regularly monitored and an intercepted by an administrative or by service providers monitoring system. Steganography is a technology that hides a message within an object, a text, or a picture. It is often confused with cryptography, not in name but in appearance and usage. The easiest way to differentiate the two is to remember steganography conceals not only the contents of the message but also the mere existence of a message. The original steganographic applications used "null ciphers", or clear text. A null cipher conveys that the message has not been encrypted in any way, whether it is using basic character shifting, substitution or advanced modern day encryption algorithm. So, the message is often in plain view but for a reason can either not be detected as being present or cannot be seen once detected. As is common with cryptography, steganography has its roots in military and government applications and has advanced in ingenuity and complexity.

## II. HISTORY

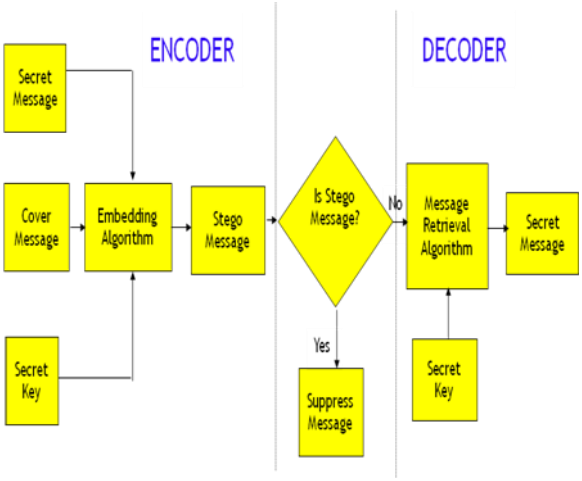
Throughout history Steganography has been used to secretly communicate information between people. Some examples of use of Steganography in past times are:

i) During World War 2 invisible ink was used to write information on pieces of paper so that the paper appeared to the average person as just being blank pieces of paper. Liquids such as urine, milk, vinegar and fruit juices were used, because when each one of these substances is heated they darken and become visible to the human eye.

ii) In Ancient Greece they used to select messengers and shave their head, they would then write a message on their head. Once the message had been written the hair was allowed to grow back. After the hair grew back the messenger was sent to deliver the message, the recipient would shave off the messengers hair to see the secret message.

iii) Another method used in Greece was where someone would peel wax off a tablet that was covered in wax, write a message underneath the wax then re-apply the wax. The recipient of the message would simply remove the wax from the tablet to view the message.

## III. MODERN TERMINOLOGY AND FRAME WORK




I) Encoder: In encoding of steganographic system first we have to choose the data that has to be hide. Then we have to select a cover image behind which the data is to be hide. Now we combine both of them with the help of a massage embedding algorithm with the help of Matlab. We also provide secret key with the massage embedding algorithm which increases level of security at decoder or reciver end.

At the end of encoding process as a result we have a stego image which is combination of secret data and cover image.

II) Decoder: At the decoder end we have a stego image which contain secret data. To retrieve that secret data we require a massage retrieval algorithm and the same secret key that has been given by the encoder to the stego image.

If system depends on secrecy of algorithm and there is no key involved – pure steganography.

Secret Key based steganography.

- Public/Private Key pair based steganography.

## IV. COVER MEDIA

i) Many options in modern communication system-

- Text
- Slack space
- Alternative Data Streams
- TCP/IP headers

ii) Perhaps most attractive are multimedia objects-

- Images
- Audio
- Video

iii) We focus on Images as cover media. Though most ideas apply to video and audio as well.

### I) Reasons for using digital images

- It is the most widely used medium being used today.
- Takes advantage of our limited visual perception of colors.
- This field is expected to continually grow as computer graphics power also grows

### II) Image Attribute

- Digital images are made up of pixels.
- The arrangement of pixels makes up the image's "raster data".
- 8-bit and 24-bit images are common.
- The larger the image size, the more information you can hide. However, larger images may require compression to avoid detection.

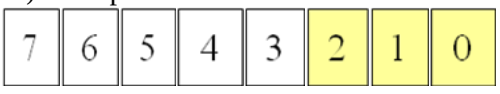
## V. IMAGE BASED TECHNIQUES

- Least Significant Bit Insertion
- Masking and Filtering

### I) LSB Insertion

- Replaces least significant bits with the message to be encoded.
- Most popular technique when dealing with images.
- Simple, but susceptible to lossy compression and image manipulation.

### II) Example of LSB Insertion




8 bits/Pixle

LSB

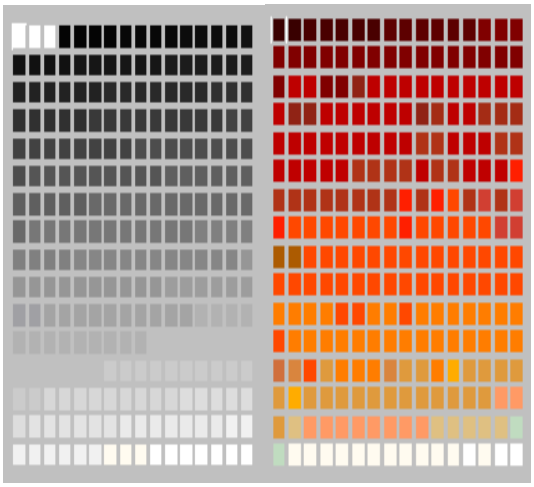
- LSB Embedding

  It is not easy to be detected by average human vision.
- 'G': 01000111 (ASCII)

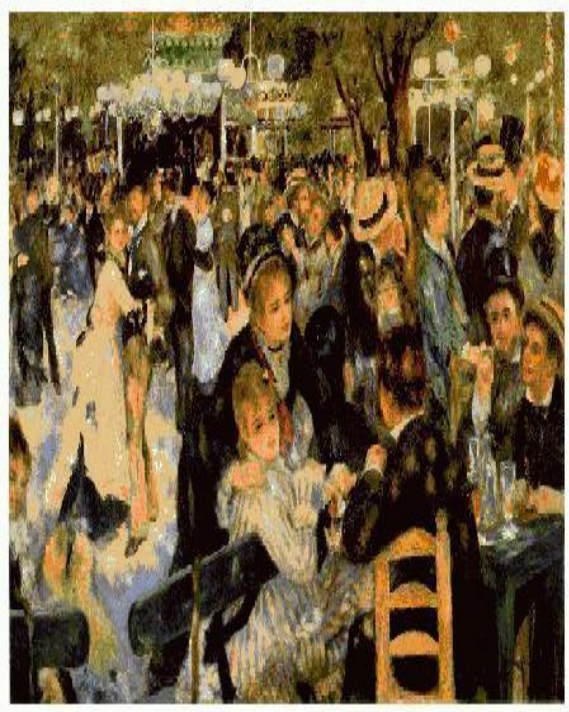
  The eight carrier bytes as follows:

  1001010*0* 0000110*1* 1100100*0* 1001011*0*
  0000111*0* 1100101*1* 1001111*1* 0001000*1*

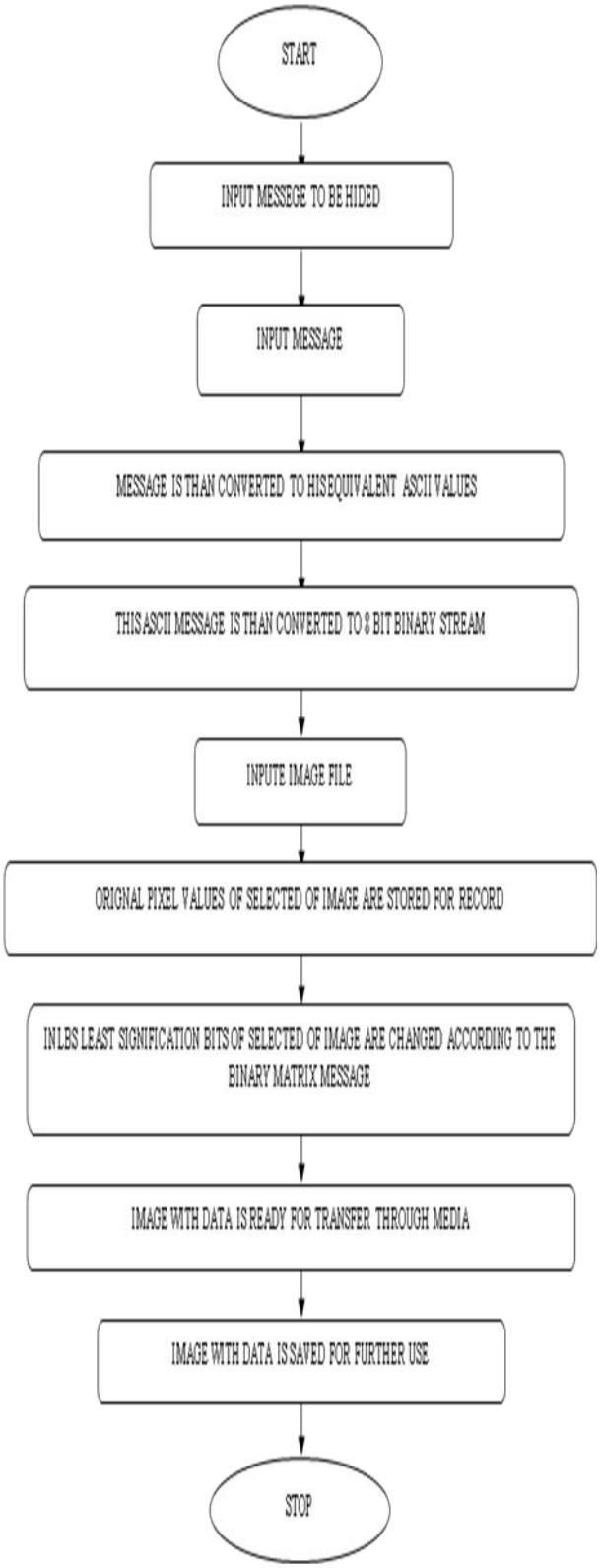
Best to use a grayscale palette or one with gradual changes in shades.



Otherwise, it is best to use images with "noisy areas" – areas with ample color variation and without large areas of solid color



III) Flow Chart for LSB Embedding



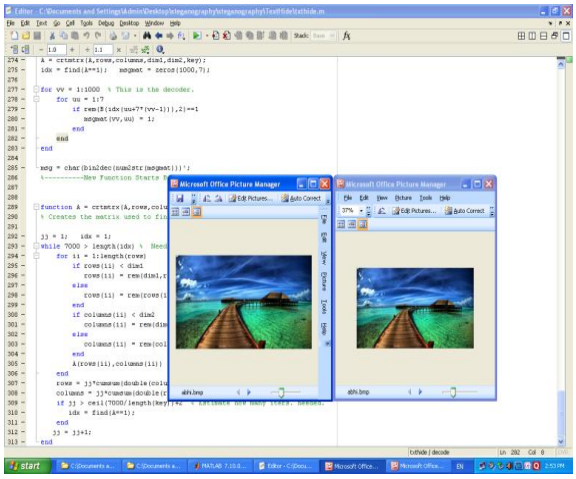
## VI. APPLICATIONS

- Storing passwords and/or other confidential information.
- Covert communication of sensitive data.
- Speculated uses in terrorist activities.
- Being widely used to hide and/or transfer illegal content.

## VII. CONCLUSION

It is understood that as less information is embedded in a cover-object the more secure the system will be. But due to difficulties in statistical modeling of image features, the security versus capacity trade-off has not been theoretically explored and quantified within an analytical framework. Private Key LSB Insertion technique and MSB Insertion technique of Steganography are being implemented on Digital Images using Tool MATLAB. The Message to be sent is first encrypted with the help of Caesar's Cipher & then it is hidden inside image so to prevent the system from Hackers. LSB Insertion proves to be safer than MSB Insertion technique as we can detect presence of data within MSB insertion implemented Image, since the Pixel values of MSB Image largely differ from Pixel values of Original Image where as there is a little difference in case of LSB inserted Images, which cannot be pointed out by Human Eye. So LSB Inserted Image appears just like the Original Image.

## VIII. RESULT



## References

[1.] Chunfang Yang, Fenlin Liu, Xiangyang Luo, Xin Ge. Investigation of Typical Digital Steganography Methods. Recent Patents on Engineering, Volume 4, Number 2, pp. 86-91(6), June 2010.

[2.] Xiang-yang Luo, Dao-shun Wang, Ping Wang, and Fen-lin Liu. A review on blind detection for image steganography. Volume 88, Issue 9, Pages 2138-2157, September 2008.

[3.] Bell, G, Yeuan-Kuen Lee. A Method for Automatic Identification of Signatures of Steganography Software. Information Forensics and Security, IEEE Transactions on, Volume: 5 Issue:2, Pages 354-358, June 2010.

[4.] M. Sitaram Prasad , S. Naganjaneyulu ,Ch. Gopi Krishna ,C. Nagaraju , Professor of School of computing, K.L. University, Vaddeswaram, Guntur-522 502,A.P.,India , Associate Professor of IT, LBR College of Engineering, Mylavaram-521 230, A.P.,India.