ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 1, Issue 8, October 2013**

# A New Approach to Secure Communication with Steganography and Cryptography

Sourav Dinda

Department of CSE, Bengal Institute of Technology & Management, Santiniketan,India

**Abstract**: In this paper we hide the message (data), using the concept of Steganography; in such a way that on-one apart from the sender and intended recipient even realizes there is a hidden message. The proposed method hides the secret message based on searching about the identical bits between the secret messages and image pixels values. The new approach is based on the LSB (Least Significant Bit) method. Also a new approach is proposed to securely sending the message using Cryptographic concept in Steganography. From the sender side the encrypted message is send and hides it in a saved picture and encodes the message. At the receiver side decryption is done to get original message.

**Keywords**: Steganography, Cryptography, LSB (Least Significant Bit), Image Pixel.

## I. INTRODUCTION

Today, the term steganography includes the concealment of digital information within computer files. At that time, computational security needs have been focused on different features secrecy or confidentiality. This has resulted in an explosive growth of the field of information hiding. Moreover, the rapid growth of publishing and broadcasting technology also requires an alternative solution in hiding information. The copyright of digital media such as audio, video and other media available in digital form may lead to large-scale unauthorized copying. The problem of unauthorized copying is of great concern especially to the music, film, book and software publishing industries.

To overcome, here I have proposed a new approach so that from the sender's side the data will be send securely to the receiver's side. By proposed method user can select an image file for data hiding and save it as the output file. The saved output image file will contain the secret message hidden inside it. Only receiver will able to read actual message after decoding the image file containing the hidden data. To retrieve the messages from the picture select the particular image. Then we get the information about the picture.

The purpose of the paper is to create a medium to transfer data securely using steganography. In this paper we use the image file as a cover and encode the text message into the image. After encoding we will save the encoded image file (containing the actual message) with the new file name. The encoded image file is sent to the destination point. The receiver at the destination can get the actual text message by decoding the image file.

## II. PROPOSED METHODOLOGY

The proposed system provides facility to hide data within the file, before the end of the file. This is efficient while transferring the image through the network. In this system the data will be Steganographic using LSB method. The simplest approach to hiding data within an image file is called least significant bit (LSB) insertion. In this method, we can take the binary representation of the hidden data and overwrite the LSB of each byte within the cover image. If we are using 24-bit colour, the amount of change will be minimal and indiscernible to the human eye. Any colour pixel is made of a combination of RED-GREEN-BLUE (RGB) .Where in each RGB components consists of 8 bits. If the letters in ASCII are to be represented within the colour pixels, the rightmost digit, called the Least Significant Bit (LSB), can be altered. Any variation in the value of this bit leads to minimal variation in colour. GIF and 8-bit BMP files employ what is known as lossless compression, a scheme that allows the software to exactly reconstruct the original image. JPEG, on the other hand, uses lossy compression, which means that the expanded image is very nearly the same as the original but not an exact duplicate. If we have to hide word 'AIG' in the image, we take the LSB of every colour and hide each bit of the word in its RGB Combination. To insert letter "A", we modify three colour pixels with 3 bits in each colour pixel.

Let us think of our original pixel (a single image pixel) as bits:

(R7 R6 R5 R4 R3 R2 R1 R0, G7 G6 G5 G4 G3 G2 G1 G0, B7 B6 B5 B4 B3 B2 B1 B0)

Our message (single message character) bits look likes – (c7 c6 c5 c4 c3 c2 c1 c0)

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013

Then we can place three of these character bits in the lowest red pixel, three more in the lowest green pixel, and the last two
in the lowest blue pixel as follows:

(R7 R6 R5 R4 R3 c7 c6 c5, G7 G6 G5 G4 G3 c4 c3 c2, B7 B6 B5 B4 B3 B2 c1 c0)

Original pixel of image (225, 100, 100)

- Original pixel of image= (11100001, 01100100, 01100100 )
- Message character – "a" value= (0 1 1 0 0 0 0 1) //ASCII VALUE
- After applying steganography theory, we got Image's pixel + message bits = (11100100, 01100100, 01100101)

i.e. New pixel = (11100100, 01100100, 01100101)

new pixel = ( 228,100, 101 ) and old pixel = (225, 100, 100)

So, we find there is small change in pixel value, so the actual image and encoded image looks almost same.

Also, the proposed following Algorithm for sending encrypted data through the Image Steganography:

Encryption:

Step-0:Check whether Client is properly connected with the Server or not.

Step-1:Accept Plain Text (generally called Text) from the sender.

Step-2:Make sure the Key, generated by the Sender's side, received by Receiver.

Step-3:Find out the ASCII value for each character of the Plain Text.

Step-4:Find out Encrypted value by adding the ASCII value and RANDOM key value. The character for the corresponding
Encrypted value will be the Cipher Character.

Step-5:Form the Cipher Text or Encrypted Text from the each encrypted characters.

Step-6: Embedded the Encrypted Text in an image and encode it (using above proposed method)and send through a medium to the Receiver's side.

Decryption:

Step-7:decode the message from the image using our proposed method.

Step-8: decoded message decompose into a character array for the Cipher Text.

Step-8:Find out the ASCII value for each character for cipher text.

Step-9:Find out the ASCII Value for the Plain Text character by deducting the Key value from the ASCII Value.

Step-10:Generate the character for the corresponding ASCII Value.

Step-11:Form the Original Text or Plain Text from array of characters and get original Message from the Sender.

## III. DESIGN FLOW, INTERFACE DESIGN & ALGORITHM

In figure (1.1), the text message and image file are encoded with the proposed encoder algorithm. The Encoded

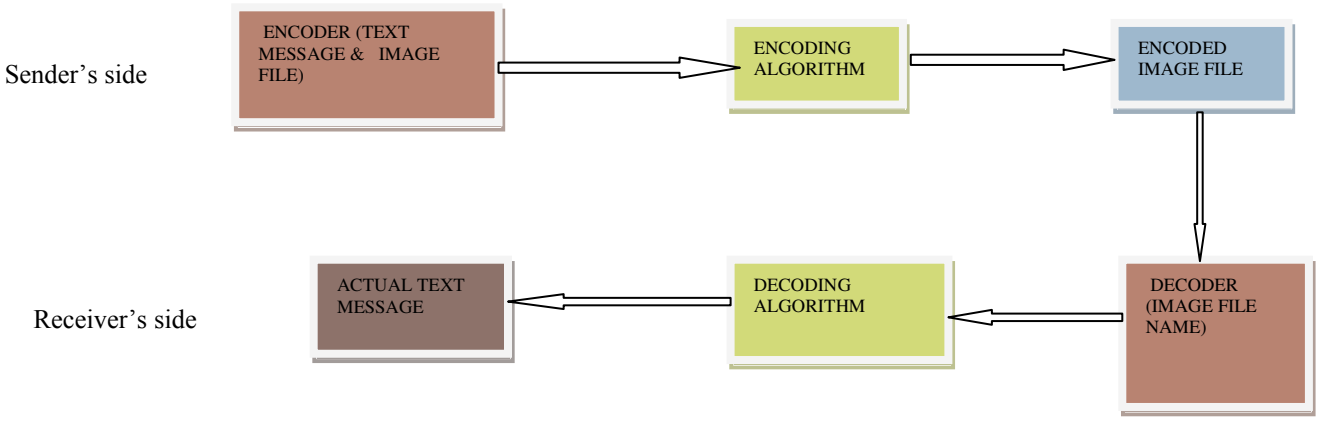



Figure (1.1): Flow Diagram for proposed Image Steganography

Image file is now sent through a medium to the intendant recipient. In the receiver's side, by using the decoding algorithm

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013

hiding text message in the image is decoded & original text will be shown.

In Figure (1.2), the interface design has been shown in the following. In Encoding section user will type the intendant
message and select the image file (in bmp format) where the message's character ASCII value & RGB value (in terms of 8

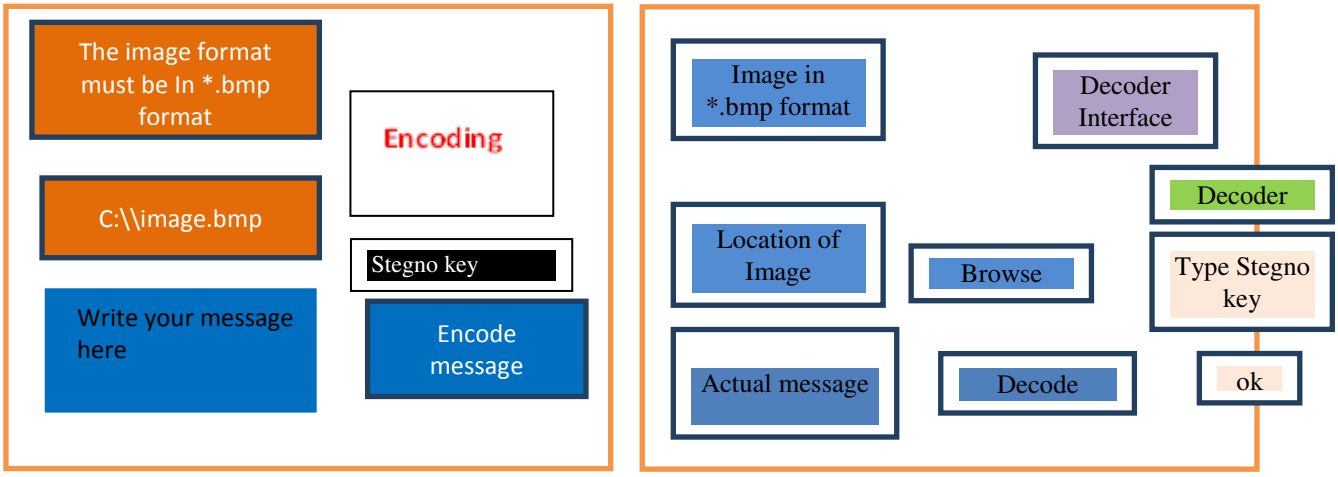



Figure (1.2): Interface Design for proposed new approach Image Steganography

bits) are formulated(i.e., encoding) with my proposed algorithm and the hiding message in the image are saved in the another file with a given stegno key.

In decoding interface section, first we have to select the saved encoded image file. By means of decoded key and stegno
key, decode the image file and extract the original message which is send by the sender.

In figure (2.1), from the sender's side the original text message is decomposed into a character set and by using a random
key the ASCII value of each character is encrypted. The encrypted message is then send to the proposed Image

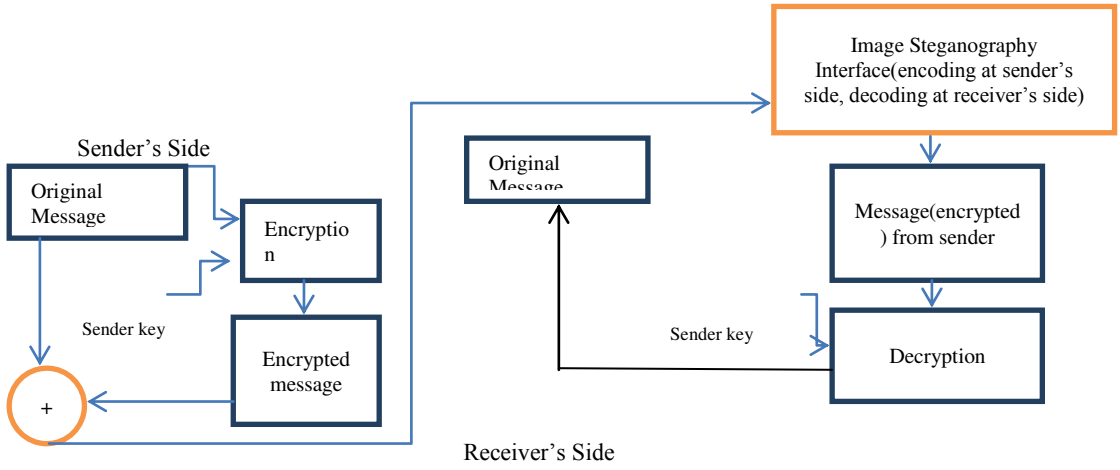



Figure (2.1): Flow Diagram for secure communication using Cryptography & Steganography

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013

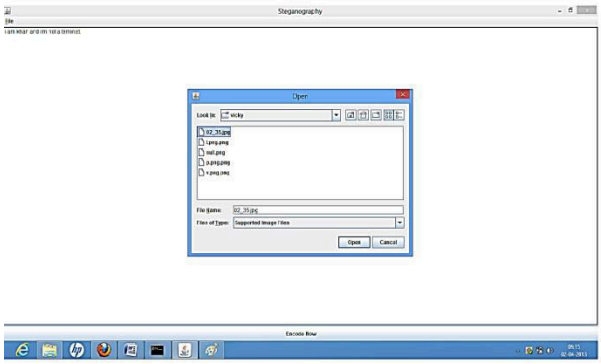
Steganographic interface, we will found the original encrypted message. Now by using sender key, the encrypted message is

Decrypted (block: decryption) and original message is received by the receiver.

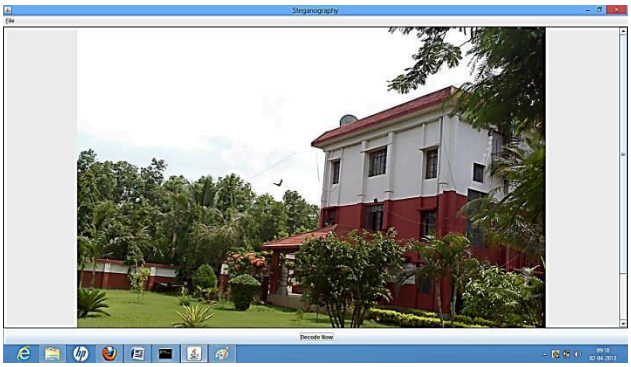
## IV. EXPERIMENTAL RESULTS & DISCUSSION

From the proposed methodology, I develop an interface for Image Steganography, where user can type his/her message in

the text area (see Output Window: 1.1) then select the image file in which the text will be encoded (in Output Window: 1.2).

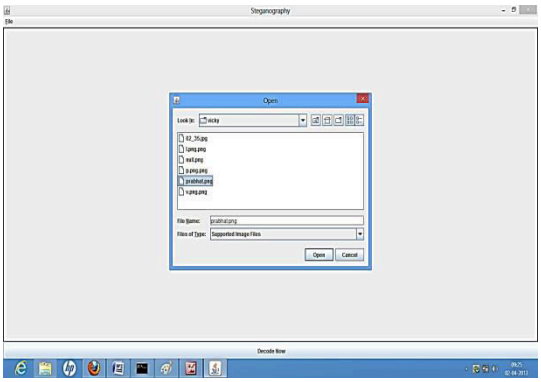


Output Window: 1.1



Output Window: 1.2

Then we have to save the encoded image file in another name that is shown in output window: 1.3



Output Window: 1.3

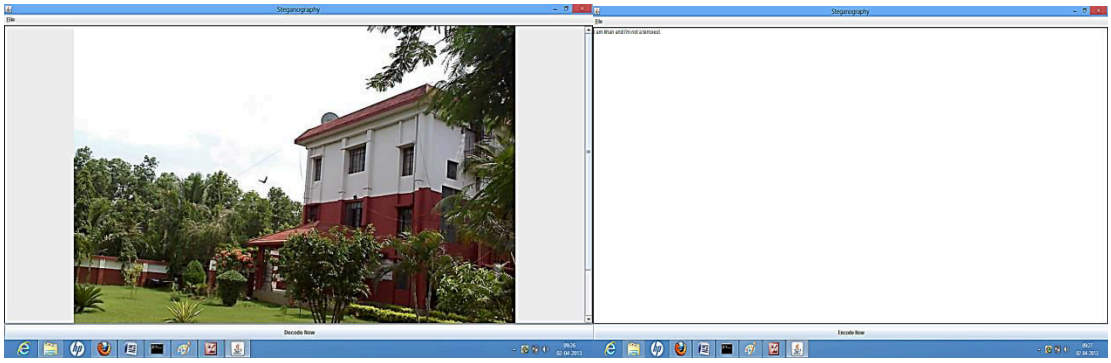
When we want to get original message, the select the saved encoded image file (see Output Window: 1.4) and the select decode option for original output.(in Output Window: 1.5)

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

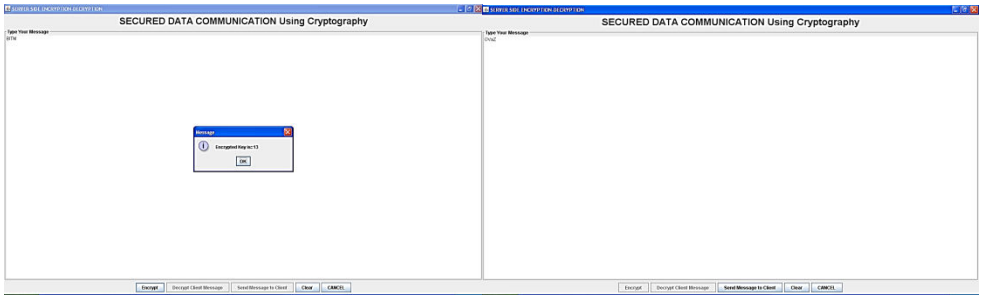
*(An ISO 3297: 2007 Certified Organization)*

**Vol. 1, Issue 8, October 2013**



OUTPUT WINDOW: 1.4OUTPUT WINDOW: 1.5

In another proposed algorithm by using own cryptographic principle the message "BITM" is encrypted with random generated key 13 (see Output Window: 2.1) and shown the decrypted message(shown in Output Window: 2.2).




Output Window: 2.1Output Window: 2.2

The decrypted message is then send to the Image Steganographic interface and lastly we found the original message. Here the data will be more secured.

## V. CONCLUSION

I conclude by finding that Steganography offers a great potential for security of data copyright and detection of infringers. Through Steganography all artistic creations pictures and songs can be protected from piracy. Most data hiding systems take advantage of human perceptual weaknesses, but have weakness of their own. It seems that no system of data hiding is totally immune to attack. However Steganography has its place in security. So, I have doing to secure the user data in a new approach with the concept of steganography and in other way I have coded double security so that no one can hack, except the sender & receiver, the data. It will be useful in Government & Law enforcement section for secured ITES related work, in Banking sector and Communication between two diplomats of two countries.

## REFERENCES

*[1.]* Saleh Saraireh "A Secure Data Communication System Using Cryptography and Steganography" International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.3, May 2013.

*[2.]* B. Geetha Vani , Prof. E. V. Prasad "Scalable And Highly Secured Image Steganography Based On Hopfield Chaotic Neural Network and Wavelet Transforms" IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 3, No 1, ISSN (Print): 1694-0814 | ISSN (Online): 1694-0784,May 2013

*[3.]* Vijay Kumar Sharma, Vishal Shrivastavaa "Steganography Algorithm for Hiding Image in Image by Improved LSB Substitution by Minimize Detection" Journal of Theoretical and Applied Information Technology,Vol. 36 No.1, and ISSN: 1992-8645, E-ISSN: 1817-3195.15th February 2012.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 1, Issue 8, October 2013**

*[4.]* K.Yugala,, K.Venkata Rao "Steganography" International Journal of Engineering Trends and Technology (IJETT) – Volume 4, issue 5, May 2013.
*[5.]* Mr. Vikas Tyagi, Mr. Atul Kumar, Roshan Patel, Sachin Tyagi, Saurabh Singh Gangwar "Image Steganography Using Least Significant Bit With Cryptography", Journal of Global Research in Computer Science(JGRCS) Volume 3, No. 3,ISSN-2229-371X,March 2012.
*[6.]* Wang, Y., Moulin, P. "Steganalysis of Block- DCT Image Steganography", BeckmanInstitute, CSL & ECE Department, University of Illinois at Urbana-Champaign, 2003
*[7.]* Eric Cole, Ronald D. Krutz, "Hiding in Plain Sight: Steganography and the Art of Covert Communication", Wiley Publishing Inc. (2003).
*[8.]* Amanpreet Kaur1, Renu Dhir2, and Geeta Sikka3 "A New Image Steganography Based on First Component Alteration Technique",((IJCSIS) International Journal of ComputerScience and Information Security, Vol. 6, No.3, 2009)
*[9.]* J. Fridrich, R. Du, and L. Meng,"Steganalysis of LSB Encoding in ColorImages," Proc. IEEE Int'l Conf.Multimediaand Expo, CD-ROM, IEEE Press,Piscataway, N.J., 2000.
*[10.]* Arvind Kumar, Km. Pooja, "Steganography-A Data Hiding Technique" InternationalJournal of Computer Applications ISSN 0975– 8887, Volume 9– No.7, November 2010.

## BIOGRAPHY

Mr. Sourav Dinda is currently working as an assistant professor for CSE Department inBengal Institute of Technology and Management, Santiniketan,West Bengal, India. He completed his MCS(Master in ComputerScience) degree with Distinction from SRTM University, India in the year 2003 &M.Phil. inComputer Science from Annamalai University in the year 2011. He has served in IT Sector more than 5 years in different positions. He has publications in International journals and his research area includes Network Security, 3-D IC Design,Quantum Cellular Automata andQuantum Computing.