A New Approach of Image Steganography Technique for Information Hiding using Nearest Filling Technique

S. Sreedhar Kumar, Associate Professor, Bhagyalakshmi, (M.tech, CNE)
Department of Computer Science, DBIT, Bangalore.
sree_me_261177@yahoo.co.in, bhagyachandrahasa053@gmail.com,

ABSTRACT- Steganography is an art that involves secret communication by using encryption and decryption from sender to receiver through message, images, videos etc. In this work, A new Approach of image Steganography technique is proposed, This proposed Work aims to, The secret information can be concealed in 0 to N Blocks of image. Hence the user can be achieved high Secure communication. This proposed work consists of two Stages namely Encryption stage, decryption stage. The Encryption stage consists of four steps, in the first step the text message has to convert into ASCII code. In the Second step splitting the image into number of blocks using non overlapping method. In the In Third step, We Introducing a new Method called Nearest Neighbor Filling Method (NNM) aims to hide the converted secret message into the nearest value of image block in linear manner. In the fourth step send the encrypted message with a secret key to the receiver. The receiver stage consists of four steps, in the first step the secret message has to decrypt with a secret key, In the second step the receiver has to find out the input information in the image, the third step is extracts the secret message from the image block, the final step is converting the ASCII code into the original message. Experimental result shows that the proposed approach is Simple and Better suitable to send the secret message in the stego- image.

Key words: concealed, linear manner, nearest neighbor filling, non-overlapping, overlapping.

I. INTRODUCTION

The need of security is very essential in digital transmission of information or data through internet. Steganography is applied computationally, when wrapping of works such as text files, image files, audio files and video files are used here that a secret message can be hidden inside them.[1-3]. Images are preferred medium for the current Steganography techniques. content adaptability, resilience, there exists a large number of image Steganography techniques which are accompanied by various attacks
on the Steganography systems. Security of any Steganography technique depends on the selection of
pixels for embedding.[4], There are two approaches are used to protect secret information from intruder or being attacked by others during transmission. One is encryption which is in the form of encoded in another from by using a secret key before sending the information, which we can called as cipher text. This information can be decoded by using secret key. There are several popular encryption techniques namely, AES, DES, RSA, Blowfish, Two fish etc.
there is an another way is Steganography which is Steganography is an art that involves secret communication by using encryption and decryption from sender to receiver through message, images, videos etc. Steganography technique can be used in military-defense, commercial, on-line activities, anti-criminal so on. There are many Steganography techniques available in the current technological field.[1-10] A new approach of image Steganography technique for information hiding using nearest neighbor filling method(NNM). This approach will be simple and gives a better Result than previous techniques since all works are done by using overlapping method but here introducing a new called finding the corresponding ASCII value for information and hide it into the image blocks by using nearest neighbor filling method(NNM) by linear passion. Hence it will give a better result than previous because there should not be confliction to the user of overlapping of image blocks.

II. PROPOSED SYSTEM

In this section details of the proposed system presented the proposed system consists of 2 stages Encryption and decryption fig.1 shows that the steps involved in proposed system. As per system architecture the sender having plain text that consists of alphabetical sentences or the numeric values or any special characters Ex: welcome to the Steganography world or 12345 or $%#$%^& ,these can be converted into respective ASCII value then ,at the same time, sender needs to have a image that is used to hide these ascii values for the secret communication the image has to split into blocks using non-overlapping method by linear manner that each block is having its own pixel values that involves in the Steganography then, by using vector calculation method and minimum distance formula as shown below, Here the block zero will be assumed that contains a value like

70	100	120	140
90	76	40	30
45	98	34	33
34	55	54	88

Here apply a minimum value calculation as the algorithm used.

$$Min\{d(P_i,B_{ij})|\square B_{ij}\text{€}B_{i,}\square B_i\text{€}B,P_i\text{€}P|\}\ldots \quad 1$$

Where P_i represents the i^{th} character ascii value B_{ij} is the i^{th} block that belongs to the Image and B_{ij} represents the j^{th} pixel value in the i^{th} block that is in image $d(P_i,B_{ij})$represents the distance between the i^{th} character ascii value with j^{th} pixel in i^{th} block and in distance as minimum value.

$$D(P_i,B_{ij})=\{|P_i-B_{ij}|p_i\text{€}P,B_{ij}\text{€}B_i,B_i\text{€}B\}\ldots \ldots\ldots..2$$

- Here i=0,j=0,k=0

D(65,70)=Min|df(65-70)|
Min value=5.

- $D(P_i,B_i)$=Min $|df(p_i-B_{ijk})|$

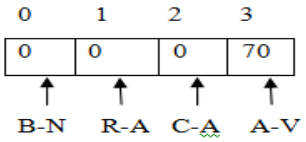
Here i=0,j=0,k=0
D(100,70)=Min|df(100-70)|
Min value=30

- $D(P_i,B_i)$=Min $|df(p_i-B_{ijk})|$

Here i=0,j=0,k=0
D(120,70)=Min|df(120-70)|
Min value=50

- $D(P_i,B_i)$=Min $|df(p_i-B_{ijk})|$

Here i=0,j=0,k=0
D(140,70)=Min|df(140-70)|
Min value=70
Here the value is



B-N:-Block Information
R-A:-Row Address
C-A:-Column Address
A-V:-Actual value

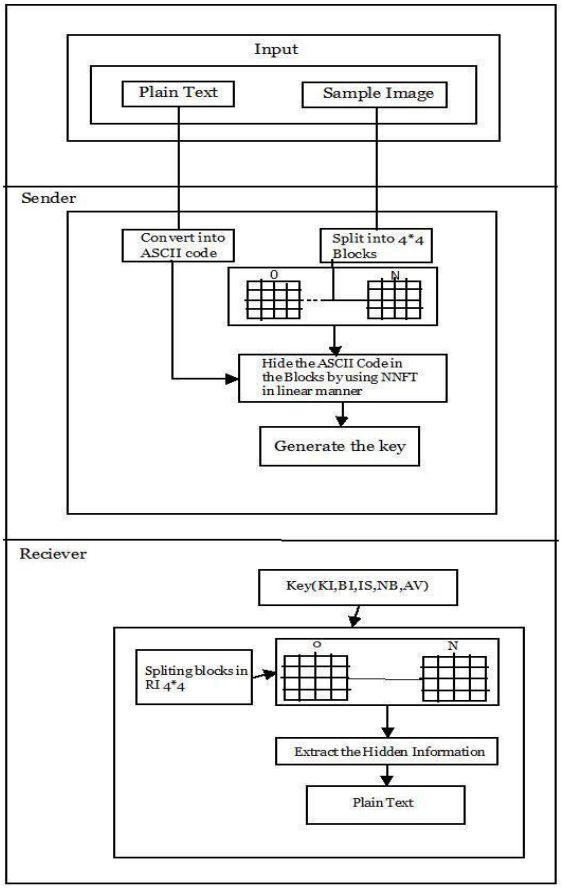


Fig. 1 System Architecture

So here got a nearest value as 70 is the nearest to 65 hence Replace 65 with 70 so encryption has done. Sender send this coded information to receiver with these key values. Receiver receives the message with key. Split the K-I into values then Extract the hidden value Get the ASCII value of each character Get a original information or message.

Algorithm:

Encryption Process
Input: Plain Text, Image
Output: Ascii Code , Encrypted image
Begin
Sender:
Step 1: Plain text converted to ascii code
Step 2: Fetch the original image.
Step 3: Split the image in to 0-N Blocks by using non-overlapping method.
Step 4: Place the ascii value in to the image blocks by using nearest filling method.
Step 5: Send the encrypted message with key to the receiver side.

Decryption process
Receiver:
Step 1: The receiver decrypts the message with the key.
Step 2: Find the input information in the image.
Step 3: Then extract the secret message from the image blocks.
Step 4: Convert the ascii code into original message.
End

III. EXPERIMENTAL RESULT

The experimental result climes the analysis that the implementation can be done by using java, here is the text message result shown below.

Example

- Input

Sample message-> ABC

- Output

ABC=656667
WELCOME=119101108111109101
so that result is as shown below
The Fig 2 shows the original image before get into the encryption,

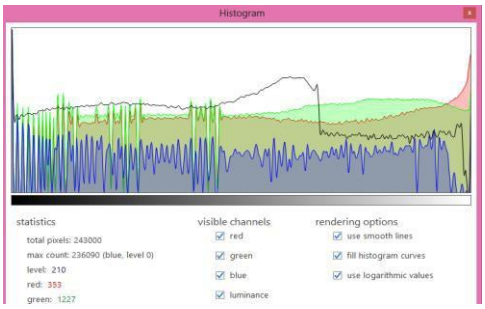


Fig 2 shows the original image before encryption

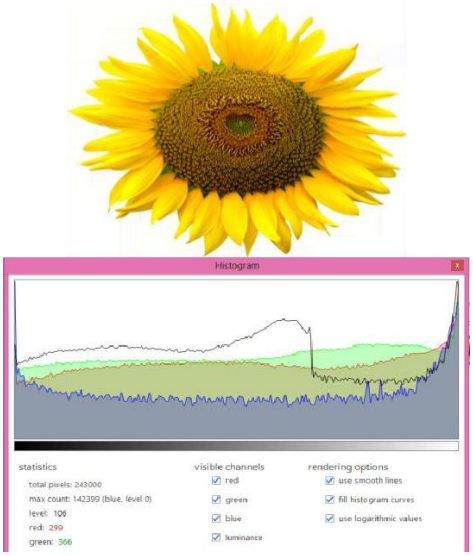


Fig 3 shows the encrypted image

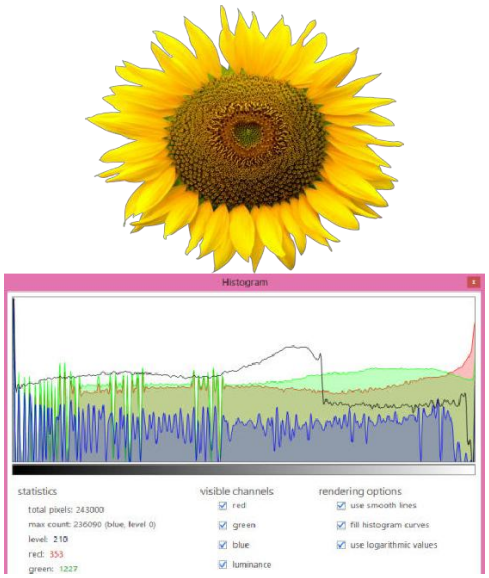


Fig 3 shows the actual image after Decryption

IV. CONCLUSION

In this paper, an ascii formatted message has been hidden into the blocks of image and here the encryption and decryption process plays a major role in this proposed method. In order to obtain the secure Data communication, this proposed work deploys the Steganography using Mainly Nearest neighbor Filling Method, The secret information can be concealed in 0 to N Blocks of image with non overlapping. and decrypt the message with key in linear passion hence the user can be achieved high secure communication.

REFERENCES

[1] J. K. Mandal and Debashis DasColour Image Steganography Based on Pixel Value Differencing in Spatial Domain International Journal of Information Sciences and Techniques (IJIST) Vol.2, No.4, July 2012.

[2] Ajit Singhand UpasanaJauhari , Data Security by Preprocessing the Text with Secret Hiding , Advanced Computing: An International Journal(ACIJ),Vol.3,No.3,May2012DOI:10.5121/acij.2012.3307 63

[3] Hamdan Lateef Jaheel And Zou Beiji A Novel Approach Of Combining Steganography Algorithms International Journal On Smart Sensing And Intelligent Systems Vol. 8, No. 1, March 2015.

[4] Saiful Islam, Mangat R Modi and Phalguni GuptaEdge-based image steganographyIslam *et al. EURASIP Journal on Information Security* 2014, 2014:8http://jis.eurasipjournals.com/content/2014/1/8

[5] BablooSaha and Shuchi Sharma , Steganographic Techniques of Data Hiding using Digital Images, Received 11 November 2011, online published 23 January 2012 ,Defence Science Journal, Vol. 62, No. 1, January 2012, pp. 11-18, DOI: 10.14429/dsj.62.14362012, DESIDOC

[6] Ross J. Anderson, Fabien A.P. Petit colas, "On the limits of Steganography‖

[7] N. Provos, and P. Honeyman, "Hide and Seek: An Introduction to Steganography," IEEE Security and Privacy, 1(3): 32-44,May 2003.

[8] C. Kim, E.-J. Yoon, Y.-S. Hong, and H. 1. Kim, "Secret Sharing Scheme Using Gray Code basedon Steganography," Journal of the Institute of Electronics Engineers of korea, 46(1): 96-102, January 2009.[3] C. C. Thien, and J. C. Lin, "Secret Image Sharing," Computers and Graphics, 26(1):765-770, February 2002.

[9] Graphics, 26[8] Yang, Li –Digital Watermarking‖. Canada, Ontario. University of Windsor, November 13, 2003.

[10] F. Shih, Digital watermarking and Steganography, fundamentals and techniques. Us SA: CRC Press, 2008. (1):765-770, February 2002.