ISSN:0975-9646

A New Efficient Approach towards Steganography

Rupinder Kaur,Mandeep Kaur, Rahul Malhotra
Adesh Institute of Engg. And Tech. Faridkot

Abstract In this paper steganography is used in a different way. Image is not transmitted over the channel rather image is used as a key between the sender and receiver means it acts as a shared key between the sender and receiver. The index array that contains the indices for our data hidden in the image is transmitted. Before transmitting divide and mean method is applied for increasing the complexity of the data.

Key Words: **steganography, compression, index array, shared image as key**

1. INTRODUCTION

Steganography is how two communicating entities can send secret messages over a public channel so that third party cannot detect the presence of the secret message. There are many reasons to hide data they all boil down to desire to prevent unauthorized persons from becoming aware of the existence of a message.

The modern secure image steganography presents a challenging task of transferring the embedded information to the destination without being detected, not just by the limited powers of the human visual system but also from powerful machine of computers.

While comparing encryption and steganography encryption encodes data such that the third party cannot come to know its meaning but in steganographic approach data is not altered to make it unusable to an unintended recipient. Instead, the steganographer attempts to prevent an unintended recipient from suspecting that the data is there.

Contribution of this paper:- in this paper steganography is achieved with a new method instead of traditional image steganography. Image is not sent over the public channel. Each character text data is converted into the indices of an image and then this converted index array is used as a stego key by both the parties and it is never sent over the public channel. The text is mapped to the image for corresponding values of the pixels shared between both the image and the text and the indices of the image containing the characters are saved in an index array

Organization of the paper: - this paper is organized in the following sections related work, proposed approach, simulation, result, future work and conclusion.

2. RELATED WORK

A lot of work is being done in the field of steganography. Artz D explained that steganography, just like cryptography is a method [1] for ensuring confidentiality of a message or information to be sent across an untrusted channel and it is, unlike cryptography, more effective art it does not attract the attention of the attacker or eavesdropper. K B Raja et al. proposed a high capacity wavelet steganography (HCWS) algorithm [2]. The cover image in this model is transformed to wavelet domain and the payload is encrypted using a random technique to increase its security. Juneja et al. proposed [3] a robust image steganographic technique based on least significant bit insertion and RSA encryption technique. They used the method of ranking a set of images in a library based on their suitability to be used as cover or carrier. Piyush marwaha and Paresh marwaha [4] developed a concept of multiple cryptography where data will be encrypted into a cipher and the cipher will be hidden into multimedia image file in encrypted format. Venkata Sai Manoj[5] discussed about the action and power of cryptography and steganography and its secured performance. T. Morkel et al. [6] gave an overview of image steganography its uses and techniques and also attempts to identify the requirements of a good steganographic algorithm and briefly reflects on which steganographic techniques are more suitable for which applications. Ali Al-Ataby et al. [7] proposed a modified high capacity image steganographic technique that depends on wavelet transform with acceptable levels of imperceptidility and distortion in the cover image and high level of overall security. Mehdi Kharrazi et al. [8] discussed some more recent image steganograhy and steganalysis techniques. They went over some general concepts and ideas that apply to steganography and steganalysis. Sanjeev Manchanda et al. [9] focused on developing the techniques that can help hiding messages on the basis of random numbers logic. Present work concentrates upon using least significant bit conversion but is not limited to it. M. Sitaram et al. [10] proposed to provide more security for key information with the combination of image compression and data encryption method. Beenish Mehboob and Rashid Aziz Faruqui [12] discussed the art and science of steganography in general and proposes a noval technique to hide data in a colourful image using least significant bit.

3. PROPOSED APPROACH

In this paper steganography is used in a different way. Text is secured in the image and the image is used as a shared key between sender and the receiver. Image is never transmitted over the channel. Using image as a key has an advantage that we can use image of indefinite size. Every character in the text

is converted into its integer value and that integer value is mapped to the single pixel value of the image. Index array are the only information required to recover the message back from the image. There is absolutely no change in the image quality because we are not changing any pixel value of the image.

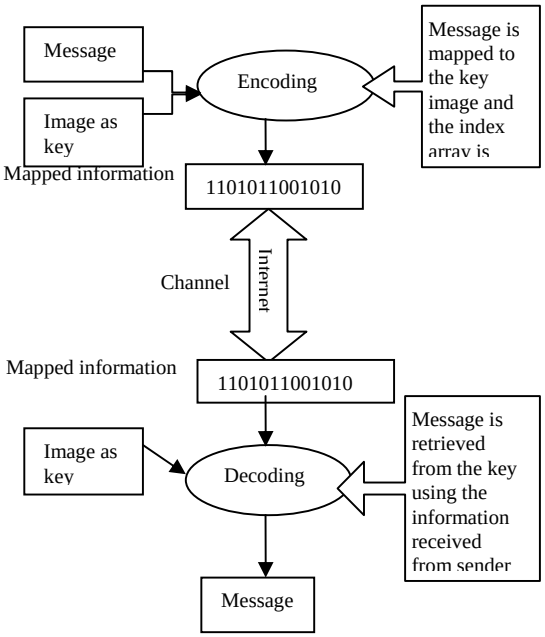

Fig. 1 encoding and decoding process

If the eavesdropper has stolen the information, it's not possible to reconstruct the message from the index array because the shared image is still unknown to the eavesdropper and it is impossible to draw the image from the available information acquired by the third party.

Compression is also achieved image of large sizes is not required to be sent over the channel only array of indices which of a few bytes is sent over the channel. Secondly we are applying divide and mean method to increase the complexity of the index array.

4. SIMULATION

MATLAB is used for the simulation purpose. Encoding is done at the sender end using encoding module and the information is sent to the receiver on the basis of which the receiver using decoding module to retrieve the original message from the key.

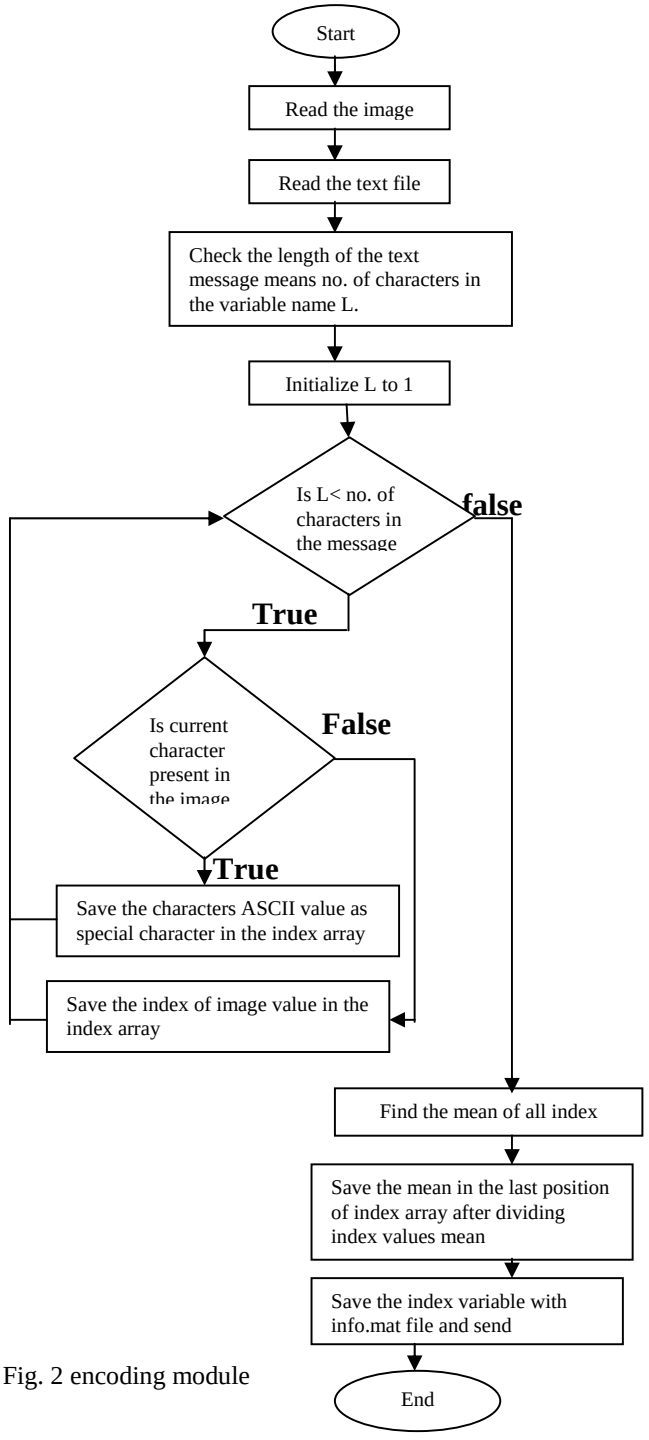

Fig. 2 encoding module

a. Encoding procedure

The encoding process is explained in the flow chart shown in fig. 2. Firstly read the image file and then read the text file. Convert the text file into ASCII Values can be called as telecast. Now check the length of the message and save it as any variable name it as length etc. Start a loop and open the

image file in an array format. Search for the ASCII value in the matrix of the grey image by increasing the index location. When the character is found in any location save the location in a variable known as index. And in case when loop part is completed with length variable becomes zero find the mean of all index values and save in last position after dividing index values with mean. Now save index variable with 'info.mat'. thus 'info.mat' file is used for decoding process.

b. Decoding procedure

Decoding module is explained with the flow chart in fig 3. In decoding module mapped info.mat file which is then extracted in mat lab as data file was 'info.mat'. We get index variable with values which are stored in it that is the index location of the character in image file. As index is our input in case of decoder and index length can be found out with the formula

s=index (size (index, 2))

Then mean value is found out using size as mean value is used to decode index location back to integer from fraction values.

Mean=index(s)

To get back the remaining index locations multiply mean with remaining index values.

Index=mean*index

To read image file and extract data from image by use index location and message is shown by using

Char (d (index))

Where d is read image.

5. EXPERIMENTAL RESULTS AND ADVANTAGES

There is no absolutely no change in the image. So, this the big advantage of using this technique for steganography. Any grey scale image can be used to carry out steganography only condition is both the sender and receiver should use the same grey scale image. In this paper 'cameraman.tiff' grey scale image file is used but we can use any grey scale image.

Image used '*camera.tiff*'

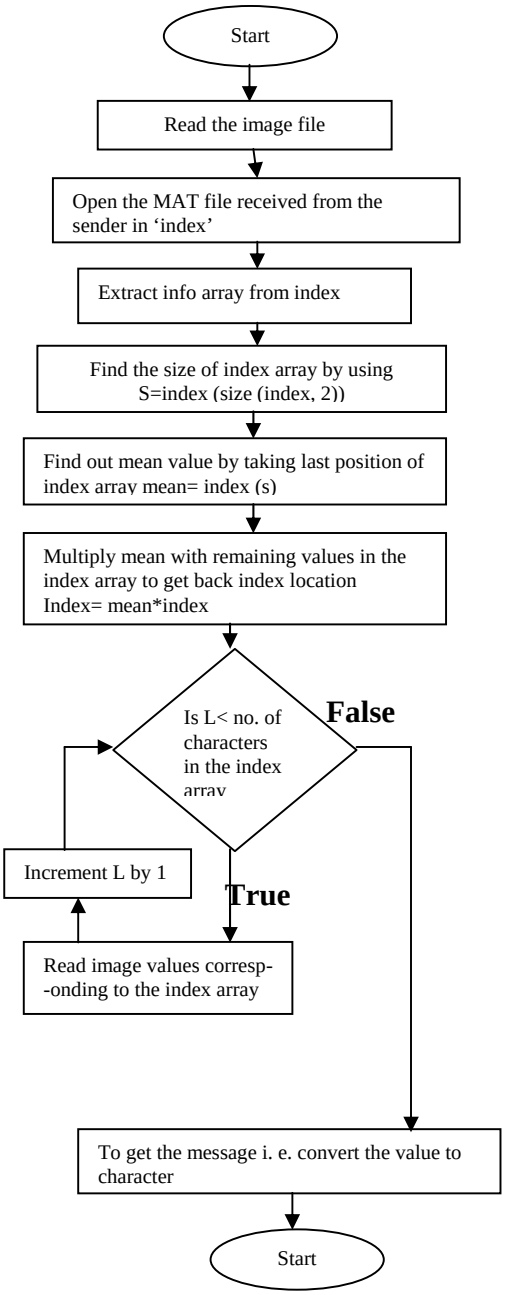

Fig.3 decoding module

Text data HELLO and HELLO SIR was sent over the channel. So, index arrays formed for the text files formed for the text files are given in the table 1 and table 2

Table 1
Index array for text data HELLO

	1	2	3	4	5	6	7
1	0.7613	0.7645	0.9397	1.1618	1.1618	1.2109	1.89953e+03

Table 2
Index array for text data HELLO SIR

	1	2	3	4	5	6	7	8	**9**	10	11
1	0.3554	0.3569	0.4386	0.5423	0.5623	0.5652	1.6841	1.6942	1.8880	1.9329	4.0603e+03

6. FUTURE WORK

In future colored image can be used which will be having large size instead of using grey scale image as used in the research.

7. CONCLUSION

In this paper, steganography is used in an efficient way that is instead of sending the carrier across the channel, the image is used only to encode text and the index array generated after encoding. Secondly there is no need to compare the original and encoded image because there is no change in the image used so image of any size can be used. Any grey scale image can be used. To increase the complexity of the index array divide and mean method is applied.

8. REFERENCES

[1] Artz D,"Digital steganography: hiding data within data;" internet computing, IEEE, pp 75-80, may/ June 2001.

[2] Raja K. B., Vikas, Venugopal K. R. and Patnaik L.M.,"High capacity lossless secure image steganography using wavelets," advanced computing and communications, pp 30-235, Dec 2006

[3] Juneja M and Sandhu P.S., "designing of robust image steganography technique based on LSB insertion and encryption" advances in recent technologies in communication and computing, pp. 302-305, Oct 2009

[4] Piyush Marwaha, Parvesh Marwaha, "visual cryptographic steganography in images" second international conference on computing, communication and networking technologies,2010

[5] I. Venkata Sai Manoj, "cryptography and steganography" international journal of computer applications (0975-8887) volume no. 12, 2010

[6] T.Morkel J.H.P Eloff, M.S.Olivier,"an overview of image steganography" information and computer security architecture (ICSA) research group.

[7] Ali Al-Ataby and Fawzi Al-Naima, "A modified high capacity image steganography technique based on wavelet transforms" the international Arab Journal of information technology volume 7, no. 4, October 2010

[8] Mehdi kharrazi, husrev T. Sencar and Nasir Memon, "Image Steganography: concepts and practice" WSPC/ Lecture Notes series, April, 2004.

[9] Sanjeev Manchanda, Mayank Dave and S.B. Singh, "customized and secure image steganography through random number logic" signal processing and international journal, volume 1

[10] M. Sitaram Prasad, S.Naganjaneyulu, Ch. Gopi Krishna and C. Nagaraju, "a noval information hiding technique for security by using image steganography" journal of theoretical and applied information technoloty, 2005-2005

[11] Beenish Mehboob and Rashid Aziz Faruqui,"A steganography implementation" IEEE, 2008