International Journal on Applicationsin Information and Communication Engineering
Volume 2:Issue 5: May 2016, pp 76-80. www.aetsjournal.com ISSN (Online) : 2394 - 6237

Safe and Secure Transformation of Data on an Encrypted Image

J. Keziah, E. GoldinaEben, P. Angela Gladys

Abstract— Steganography rates how powerful are its capabilities towards hiding and encrypting various kinds of data (Jpeg, Bmp, Gif, txt). Here steganography is done using Least Significant Bit technique. The human eye cannot identify even there is any change in the last fewer bits of the image. So an unauthorized person cannot access it. Hence the last bit of each RGB color byte of the image is rounded off and the ASCII value of the message is added to it. Next image transmission is done by using e-mail service. At the receiver terminal image decryption is done without any interruption. Image steganography exploits the limited power of the Human Visual System (HVS) in which any plain text, cipher text, other images or anything that can be embedded in a bit stream can be hidden in the image.

Keywords—Steganography, Least Significant Bit Embedding

I. INTRODUCTION

Digital communication has become an essential part of infrastructure. Now a day, a lot of applications are internet-based and it is important that communication made be a secret. As a result, the security of information passed over an open channel has become a fundamental issue and therefore, the confidentiality and data integrity are required to protect against unauthorized access. This has resulted in an unstable growth in the field of information hiding. Encryption is the most effective way to achieve data security. The process of Encryption hides the contents of a message in a way that the original information is recovered only through a decryption process. The purpose of Encryption is to prevent unauthorized parties from viewing or modifying the data. Image encryption is an effective approach to protect images or videos by transforming them into completely different formats. Several data encryption algorithms like Data Encryption Standard (DES) and Advanced Encryption standard (AES) are being employed for protecting digital information.

The word steganography literally means covered writing as derived from Greek. It includes a vast array of methods of secret communication that conceal the existence of message.

J. Keziah, ME in Communication Engineering, Francis Xavier Engineering College, Tirunelveli affiliated by Anna University, Chennai. (Email: keziahjeyaseelan@gmail.com)

E. GoldinaEben, ME in Communication Engineering, Francis Xavier Engineering College, Tirunelveli affiliated by Anna University, Chennai. (Email: goldina.johnson@gmail.com)

P. Angela Gladys, ME in Communication Engineering, Francis Xavier Engineering College, Tirunelveli affiliated by Anna University, Chennai. . (Email: gladnessangi@gmail.com)

The following formula provides a generic description of steganographic process

Cover_medium + hidden_datastegno_key = stegno_medium

In this cover_medium is the file in which we will hide hidden data which may be encrypted using stegno_key. The resultant file is stegno_medium.

A. Organization Of The Paper

The paper is organized as follows: In the next section, data embedding techniques are investigated. A detailed study of cover medium is shown in section 3.Section 4 explains about flowchart. Section 5 explains about the Least Significant Bit Algorithm. Section 6 explains about the process of Data hiding on the image. Simulation results are presented in Section 7. Result is drawn in Section 8.

II. DATA EMBEDDING

One of the Current methods for the embedding of messages into images is Least Significant Bit Embedding. A digital image consists of matrix of color and intensity values. In a typical gray scale image, 8bits per pixel are used. In a typical full color image 24bits per pixel are used:8bits assigned to each color component the simplest steganographic technique embed bits of the message directly into the least significant bit plane of the cover image in a deterministic sequence.

Another method for the embedding of message into images is Transform Embedding Techniques. The message is embedded by the modulating coefficients in a transform domain such as Discrete Cosine Transform(DCT), Discrete Fourier Transform or Wavelet Transform. Spread spectrum techniques and redundant encoding of the message can be employed in this technique. The message can be thought of as a narrow band signal encoded in a larger frequency band. By spreading the energy of the embedded message across many frequency band (such as by frequency hopping) the energy at any particular band is reduced. Therefore the message becomes more difficult to detect or modify without damaging the cover.

Another method for the embedding of message into images is Perceptual Masking Systems.“Masking” refers to the phenomenon where a signal can be imperceptible to an observer in the presence of another signal. The masking properties of the human visual system allow perceptually significant embedded to be unnoticed by an observer under normal viewing condition. Masking system performs the analysis of the image and usethe information to determine the

appropriate regions to place the message data. These systems can embed in either the spatial or transform domain.

III. Cover Medium

An image is made up of thousands and thousands of pixels. A pixel is the smallest "dot" that the user sees when viewing a bitmap on the computer screen. Also, an image is nothing more than strings and strings of bytes, each byte representing a different color. The last few bits in a color byte, however, do not hold as much significance as the first few. This is to say that two bytes that only differ in the last few bits can represent two colors that are virtually indistinguishable to the human eye. For example, 00100110 and 00100111 can be two different shades of red, but since it is only the last bit that differs between the two, it is impossible to see the color difference. LSB steganography, then, alters these last bits by hiding a message within them. Suppose a pixel is dark green. This information is expressed by a sequence of 24 bits. (Remember that eight bits equals one byte)

Byte 1 (8bits) - Red 01010110

Byte 2 (8bits) – Green 01111011

Byte 3 (8bits) – Blue 00011110

Each byte provides 256 different values for each color, much more than can be discerned by the human eye. With 256 possibilities for each, that's 16.7 million color possibilities for the 3-byte sequence (256 x 256 x 256)! If you "hijack" the least significant bit (LSB) which will be discussed later, (right-most)of each byte, you can replace it with a bit for a text message without making a noticeable difference in the color. In the 24-bit code above that describes dark green; one could hide three bits of a message. In an image of 262 x 196 pixels, there are a total of 51,352 pixels. Alterations of 20 or 30 pixels may be enough to send a whole message, but not enough for detection of the transmission. The person receiving the message would simply you have to know what to look for and where to find it. The size of the image file is directly related to number of pixels and the granularity of color definition.

IV. Procedural Flowchart

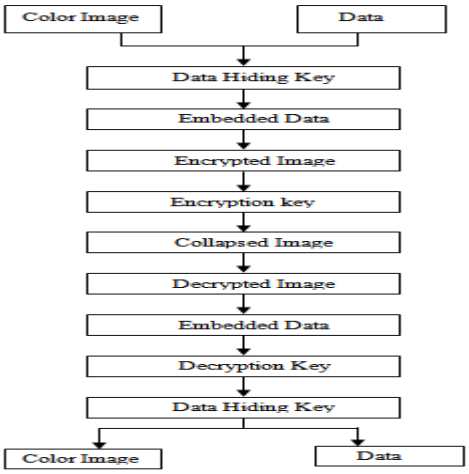

Fig 4.1: Flowchart

V. Least Significant Bit Insertion Algorithm

Least Significant Bit insertion is a most well-known steganography technique. It is the easiest to use but the most vulnerable to attack. If the LSB is applied, 3 bits can be encoded into each pixel for a 24 bit image. There 3bytes in each pixel and any changes made to the pixel bit would be unrecognizable to the human eye.

When using 24 bit images 8 bit values are devoted to each primary color (R, G, B). For example, the letter A can be hidden in 3pixels. Assume the original pixel of color. Magenta having the primary color values as (255,128,255) and the ASCII value of A is 065

The original pixel in the cover image is (255,128,255)

The ASCII value of letter to be hidden is (065)

The round off pixel value is (250,120,250)

Each digit in the ASCII value of A is added to the corresponding last digit of the rounded off pixel. After encrypting the pixel value will be (255,126,250)

The emphasized bit are the only digit that are actually change. The main advantage of LSB insertion is that data can be hidden in the least and secondary bits and still the human eye would be unable to notice it.

VI. Hiding Message Into An Image

Type of Steganography:Classical Steganography Type of data hiding techniques:Reversible data hiding

When hiding a secret message into an image there are two phases namely encryption & decryption.

A. Data Encryption

The message which is given as input by the user is processed character by character. For security purpose the key has to be given which is verified at the receiver. Each character is converted into its corresponding ASCII value. After that the values are transformed and grouped into 8 rows and number of columns equal to the number of characters. Then the matrix values are converted into the single binary string by using the function (ex: binary String = binary String ().The image is also given as input by the user. The least significant bit consists of the minute changes in the pixel value so changing this pixel value will not affect the image. The image is digitally represented by combination of the 3 matrix values R, G, B. The length of the binary string is found out. The modulo two division is performed in the LSB bit of the matrix value and the resultant value is compared with original binary string value. If it is found to be equal no change is made to the matrix value and it is just copied as it is to the new matrix. Otherwise there may be two chances it may be 1 or 0.if it is 1,it has to be changed to 0 by decrementing the matrix value by 1.Thereafter the resultant is stored in a new matrix. If it is 0, it has to be changed to 1 by incrementing the matrix value by 1 and resultant is stored in a new matrix. In order to improve the security the bit is inserted using a data hiding key. The place for each bit is fixed by password. The place value is found by converting the password character into the particular ASCII value. Then the matrix value corresponding to the

particular ASCII value is chosen for the bit value to be embedded this is repeated for all the rows. It is not at all possible to recover the data without knowing the password. The length of the message is also embedded into a particular matrix value. The Data hiding key is used to position the bit in the particular matrix value. The ASCII value for the each character in the data hiding key is found out and the position corresponding to the ASCII value is chosen to embed the message data. This technique is repeated for the other data to be embedded in each row. The process is explained in Fig 6.1.

B. Image Encryption

Next step in the encryption process is to scramble the image so that no one can able to view it or recover the original data from the image. Image encryption is a technique used to change the original view of the image. Here, the image encryption is done through the pixel interchange. The color image is digitally represented by the 3 different types of pixels such Red, Blue and Green. In a 400*400 image it consists of

R type pixels-400*400
G type pixels-400*400
B type pixels-400*400

There are around 480000 pixels in a simple 400*400 image. If the pixels are interchanged the original view of the image will change as shown in Fig 6.2

After the pixel interchange, in order to improve the security, the pixels of the image are changed by pixel modulo division method. The logic used behind is such that any two of the three pixel values are summed and it is modulo divided by 256 and the remainder after the division is stored in the first pixel value. Then the next consecutive pixel values are added and the remainder after the division by 256 is stored in second and so on for ex:

Take three pixels
A B C
78 133 198
A= (A+B) %256
A B C
211 133 198
B= (B+C) %256
A B C
211 75 198
C= (C+A) %256
A B C
211 75 153

Image encryption key is also used to change the pixel value. To get the image identifier keys, we require the dimensions such as height and width and also the image encryption key.

Let image encryption key be 'ae0de2fe'

ASCII values of bold terms in above key are b3, b2 and b1.

Three other random positions are chosen from three other random numbers such as r1, r2, r3. The three random positions be p1=L-r1, p2=L-r2, p3=L-r3.

ASCII values of terms in positions p1, p2, p3 are a1, a2 and a3.

Modular formula can be used to find the of image identifier keys such as k1, k2 and k3 as follows

K1= (height-b1+a1) %256
K2= (width-b2+a2) %256
K3= (height-b3+a3) %256

These image identifier keys are superimposed with certain pixels and transmitted with encrypted image.

C. Image Decryption

This technique recovers original image from encrypted image. In order to recover original image, 'image encryption key' and image identifier keys are used. Decryption obtains image encryption key and image identifier keys from user.

Let image encryption key be 'ae0de2fe' ASCII values of bold terms in above key are b3, b2 and b1.Three other random positions are chosen from three other random numbers such as r1, r2, r3. The three random positions be p1=L-r1, p2=L-r2, p3=L-r3. ASCII values of terms in positions p1, p2, p3 are a1, a2 and a3. Already we discussed about the image identifier keys and the way to find those keys in encryption algorithm. The three image identifier keys be k1, k2 and k3. Reverse modular formula can be used to find the dimensions of image as follows

Height1= (k1+ b1-a1-256)%256 Height = (k3+b3-a3-256)%256

Width= (k2+b2-a2-256)%256

In image encryption, the data encoded image encrypted in order to improve security. The reverse pixel modulo division technique is used to obtain pixel interchanged message. Let us consider the first three pixels of encrypted image as A0, B0, C0 and first three pixels of pixel interchanged image as A, B, C

Then reverse pixel modulo division can be used to find A, B, C as follows

A B C
211 75 153
C = (-A+C+256) % 256
B = (B-C+256) % 256
A = (A-B+256) % 256
A B C
8 133 198

(image with corrected pixel values/ Pixel interchanged image)

As a reversal to the pixel interchange method of the image encryption technique, in image decryption back tracking of interchanged pixels is done Encrypted image obtained contains the data bits included in the raw image whose positions are determined by the ASCII values of terms in the image encryption key which is discussed in the encryption algorithm. As a method of reversal, we are able to find data bits for the positions obtained from ASCII values of terms in the image encryption key. The process is explained in Fig 6.3.

For a image encryption key of word length n, n number of bits can be encrypted in a row of pixels.

D.Data Decryption

The length of the message is just retrieved via a particular matrix value. Then modulo division is made to the matrix values and the resultant remainder is stored in the array. The

array is converted into the string. To convert the received binary values to the corresponding ASCII value. The multiples of two from right to left up to 128 is stored in a string. Then the string which contains the message is verified whether the recovered bits are the multiples of 8.If it is not the multiple of 8, the error must be shown. Then the message string is resized into 8 rows and the columns equal to the length of the message. After that both the strings are multiplied then ASCII value of the particular character is recovered. The value corresponding to the ASCII value is found from the code table and the value is displayed to the user. Suppose the data decryption key is "acefghik" the data can be decrypted as 01100001 which is nothing but the ASCII value of A. hence A is recovered from the image

VII. SIMULATION RESULT

Algorithm steps for data detection using Least significant bit embedding is given here. The detection steps are as follows.

• Message:**It is a technique to send secret messages.**
Data hiding key:**abdulkalam**
Encryption key:**ae0de2fegh**

Fig 7.1:Input Image

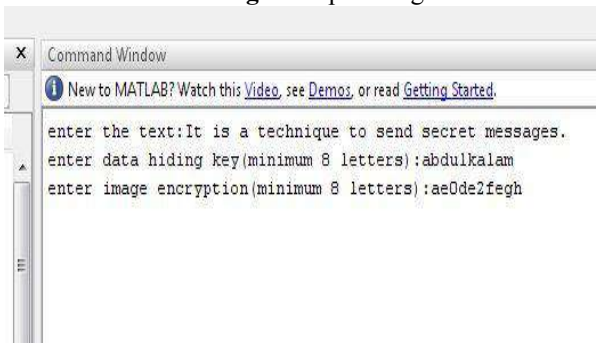

Fig 7.2: Inputs

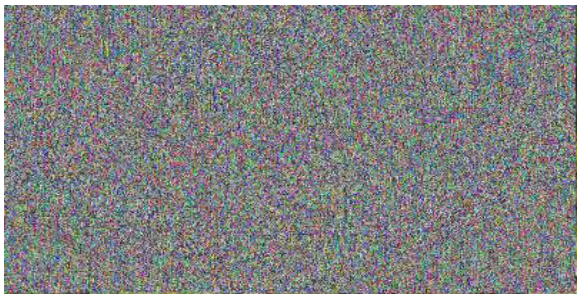

Fig 7.3: Encrypted Image

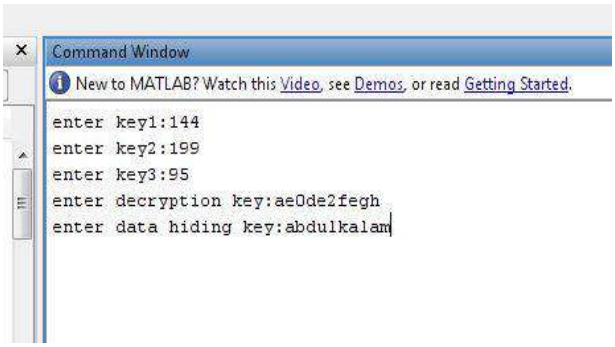

Fig 7.4 Decryption Side

Fig 7.5 Decrypted Image

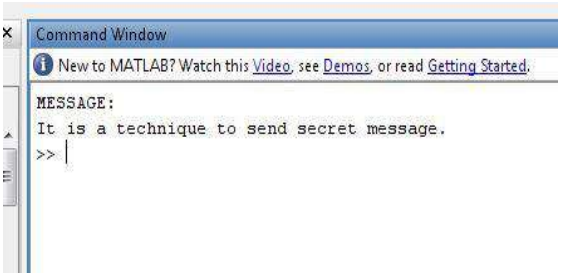

Fig 7.6 Extracted Image from this image

VIII. CONCLUSION

Steganography has its place in security. By using this software for encrypting message into an image, efficient transformation of messages is possible. In secure transformation of data in encrypted image is to provide high network security for data transformation. Extract the hidden data and recover the original content without any error by exploiting spatial correlation in natural image if the amount of data is not too large. The proposed scheme of reversible data hiding technique is achieved through colour image instead of gray scale image to improving the capacity of hidden data. To considering gray scale image the amount of additional data is small. When using a colour image instead of gray, each bit of the red, green and blue colour components can be used, so a total of 3 bits can be stored in each pixel. It gives a relatively large amount of space to hide data. The image based data 67 hiding technique is tried to improve the capacity of hidden

data since, there is a limitation on how much information can be hidden into an image. To overcome the capacity problem, in future the video based data hiding has been achieved and to provide high security separate key should be used for encryption and decryption.

REFERENCES

[1] S.Poongodi, Dr.B.Kalavathi, M.Shanmugapriya "Secure Transformation of Data in Encrypted Image Using Reversible Data hiding Technique" International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 4.

[2] K. Thangadurai; G. Sudha Devi "An analysis of LSB based image steganography techniques" Computer Communication and Informatics (ICCCI), 2014 International Conference on Year: 2014 Pages: 1 - 4, DOI: 10.1109 / ICCCI.2014. 6921751

[3] Jessica Fridrich, "Reliable Detection of LSB Steganography in Color and Grayscale Images"

[4] M. DarvishMorshediHosseini; M. Mahdavi "Modification n spatial, extraction from transform: A new approach for JPEG steganography" Information Security and Cryptology (ISCISC), 2015 12th International Iranian Society of Cryptology Conference onYear: 2015 Pages: 134 - 140, DOI: 10.1109/ISCISC.2015.7387911

[5] V. Thanikaiselvan; P. Arulmozhivarman, "High security image steganography using IWT and graph theory" Signal and Image Processing Applications (ICSIPA), 2013 IEEE International Conference onYear: 2013Pages: 337 -342, DOI: 10.1109/ICSIPA.2013.6708029

[6] Yi Zhang; XiangyangLuo; Chunfang Yang; Dengpan Ye; Fenlin Liu, "A JPEG-Compression Resistant Adaptive Steganography Based on Relative Relationship between DCT Coefficients" Availability, Reliability and Security (ARES), 2015 10th International Conference onYear: 2015Pages: 461 - 466, DOI: 10.1109/ARES.2015.53

[7] M. R. Islam; A. Siddiqa; M. P. Uddin; A. K. Mandal; M. D. Hossain, "An efficient filtering based approach improving LSB image steganographyusing status bit along with AES cryptography" Informatics, Electronics & Vision (ICIEV), 2014 International Conference onYear: 2014Pages: 1 - 6, DOI: 10.1109/ICIEV.2014.6850714