ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

Advanced Steganography: Embedding High Capacity Audio in Colour Image

Amol Bhujade[1], Prof. Sonu Lal[2]

M. Tech Student (Digital Communication), Dept. of CE, IES College of Tech., Bhopal, India[1]

Professor, Dept. of CE, IES College of Tech., Bhopal, India[2]

ABSTRACT: Now a day's security and storage capacity becomes the critical factor during the transmission and storage of increasing amount of data over various mediums. This paper brings the idea of advance steganography where the data in one medium is hidden in another medium in such way that no one apart from sender and receiver suspect the existence of the message. In this we are using Least Significant Bit method to hide the content of the encoded audio message in the last two LSB bits of the pixels of the carrier color image. This paper overcome the drawback on previous method where the bits of the secrete audio data are hidden in the only last bit of the cover image thus offers more key based secure data transmission and reception with same cover medium. This paper also applied for MPEG-III(mp3) file previously was applicable to only WAVE file, so provide flexibility and versatility to the user.

KEYWORDS: steganography, RGB channels, LSB substitution, bit array conversion.

I.INTRODUCTION

Major requirement of today's computer communication is to prevent the data to be disclosed to the illegal user. Various technique of such data hiding are steganography, cryptography, watermarking etc [1][5]. Apart from these Steganography is the practice of hiding private or sensitive information within something that appears to be nothing. Both techniques are use to protect important information [1][3]. The difference between the two is that Steganography involves hiding information so it appears that no information is hidden at all. Steganography in the modern day sense of the world usually refers to information or a file that has been concealed inside a digital picture, video or audio file. What Steganography essentially does is exploit human perception, human senses are not trained to look for files that have information hidden inside them, although there are programs available that can do what is called steganalysis. Data hiding, or steganography, is a challenging area of research which has attracted much attention for centuries. As an active area of research, new techniques are constantly emerging using LSB algorithm[6][7]. In contrast to the active research focusing on image or video schemes, there is little research on data hiding in audio schemes. However, effective audio data hiding in an color image can create robust and imperceptible data thus allowing property rights protection or secret data exchange.
Basic terminologies associated with the steganography are summarized below which help in the further approach.

Payload: The information which is to be concealed, here we use audio as payload.

Carrier File: The media where payload has to be Hidden which is color image we use here.

Stego-medium: The medium in which the information is hidden.

Redundant Bits: Pieces of information inside a file which can be overwritten or altered without damaging the file.

Steganalysis: The process of detecting hidden information inside the file.

The advance steganography process can be understood properly by following rule:

Cover image+ Audio message +Stego key= stego image

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

II. RGB COLOR CHANNELS AND LSB SUBSTITUTION METHOD

An image can be represented by a collection of color pixels. The individual pixels are represented by their optical characteristics like “brightness”, “intensity””contrast”,etc. Each of these characteristics can be digitally expressed in terms of 1’s and 0’s. basic There are three color channels that present different forms for storing images. A color space is a method by which it is possible to specify, create and visualize color. The most common color space among all is RGB (Red, Green, and Blue). The RGB color model is additive in the sense that the three light beams are added together, and their light spectra add, wavelength for wavelength, to make the final color's spectrum [10]. Each pixel in a 24-bit bitmap image in this space is described by 3 sets of 8 bits (3 bytes), that each set contains the intensity value of individual red, green and blue. Combination of these values forms the characteristics of the pixel. The RGB color model already had a solid theory behind it, based in human perception of colors. One simple method is LSB, or Least Significant Bit Steganography [14]. 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 [13].

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. To hide a secret message inside an image, a proper coverbimage is needed. Because this method uses bits of each pixel in the image, it is necessary to use a lossless compression format, otherwise the hidden information will get lost in the transformations of a lossy compression algorithm [21]. When using a 24-bit color image, a bit of each of the red, green and blue color components can be used, so a total of 6 bits can be stored in each pixel. For example, the following grid can be considered as 3 pixels of a 24-bit color image, using 9 bytes of memory:

(100110011 11001110 101110010)
(011010011 10101010 101111010)
(11001000 00100111 101000100)

When the character B, which binary value equals 10000010, is inserted, the following grid results

(00100111 11101000 11001000)
(00100110 11001000 11101000)
(11001000 00100111 11101000)

In this case, only three bits needed to be changed to insert the character successfully. The result changes that are made to the least significant bits are too small to be recognized by the human visual system (HVS), so the message is effectively hidden. As one can see, the least significant bit of the third color is remained without any changes. It can be used for checking the correctness of 8 bits which are embedded in these 3 pixels. In other words, it could be used as “parity bit”.

III. PROPOSED METHODOLOGY OF LSB

The conventional method says, one LSB can be replaced with the data bit. Instead of hiding a single bit in each byte, three bits of data can be hidden in a single byte as it can cause no change in the image as per the human visual system. As there are 8 bits in a byte, first and the second and third bits can be hidden in Red values and next three bits in the green value and next three in the blue value byte. For example, consider the 24 bit pixel value-

11001000 00100111 10100010

Consider the data byte- 111 010 110

Data can be hidden in the following way-

11001111 00100010 10100110

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

The main advantage of this technique is the increase in the amount of space for hiding the data. Thus 1 byte of audio data can be hidden in the one pixel of the cover image.

IV. BIT ARRAY CONVERSION

The cover image to hide the data is the 8 bit image is converted into bit array format as well as the audio file acting as secrete data is also converted into bit format only then the hiding can be achieved [10].
Bit array 1 : Header
Bit array 2 : size of audio file
Bit array 3 : contents of audio file

V. HIDING AN AUDIO MESSAGE

When an audio file divided into different field like header, size of data, and the content of audio message, bits per sample format etc each of these field is converted into bit array to hide in the digital color image. The mostly used audio files are WAVE file which have fixed byte header and all the contents are arranged in sequence but it require large memory so that less data limit this file application [14]. So in this approach we use MPEG layer 3 (mp3)file also where the data is appear in compressed form so that more content can be obtained in same memory and then hidden in the cover medium i.e. color image.

The relation between the size of the audio file in bytes(A) and that of cover image in the pixel(P) is given by,

$16*A=9*W*H,$

Where, W and H are the width and height of the cover image

Therefore maximum size of audio file given by,

$A=9*w*H/16$

Lets consider MP3 having 56 bytes dedicated for header then remaining bytes reserved for the audio content. Then,

$A=56+M,$

Where, M- actual size of the message in bytes.
Thus,

$M= [9*w*H/16]-56.$

VI. BLOCK PROCESSING

Encoder block used for hiding the audio message in the image. This audio message is first sampled and then converted into binary format and then encoded with color image using LSB technique as discussed above. Figure 2 use for extraction of the original audio content at the receiver. Firstly it obtained in binary form and then converted into audio form using appropriate MATLAB tools. Stego key is used in both transmitter and receiver block for secure communication.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

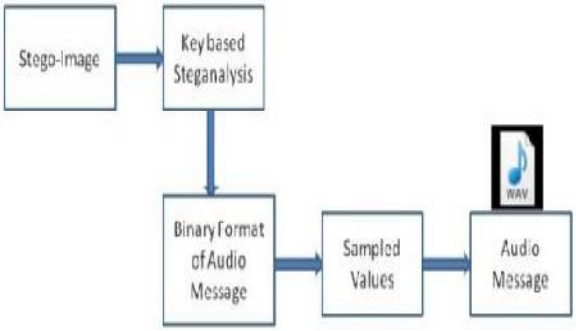

Figure 1. Hiding the audio message

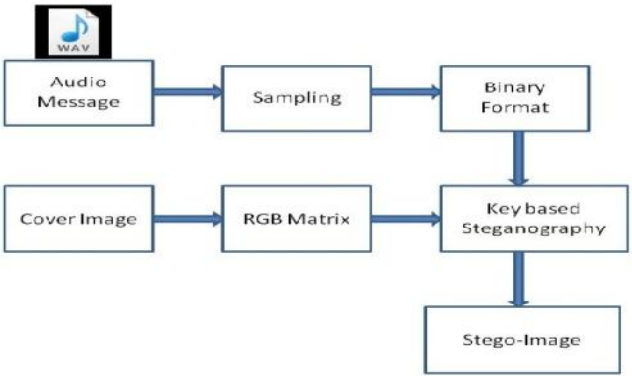

Figure 2. Recovering the audio message

VII. IMPLEMENTATION AND OUTPUT

Using image processing toolbox above proposed work has been implemented. We obtained the snapshot of the result which show the color image converted into the binary form shown in fig 3. A group of images shown in fig 4 and fig 5, before and after hiding the content of audio information using method mentioned previously. The last three least significant bit are replaced by the mp3 audio message content using encryption technique. The mp3 or wave audio content are recovered using decryption technique. The changes in the cover image in which the audio is hidden are so small that cannot be observed by the human perception. Thus, stego image looks like the cover image and the recovered audio message will also appears identical to the original data that was sent.

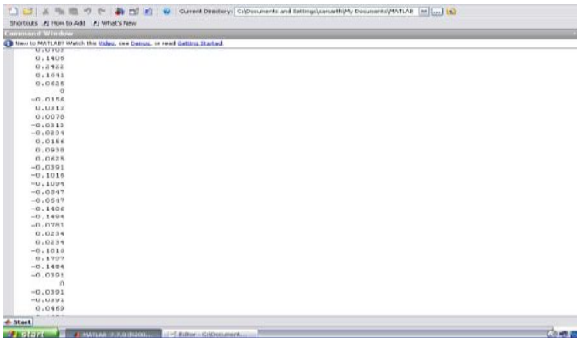

Figure 3. Snapshot of color image in bit array form

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

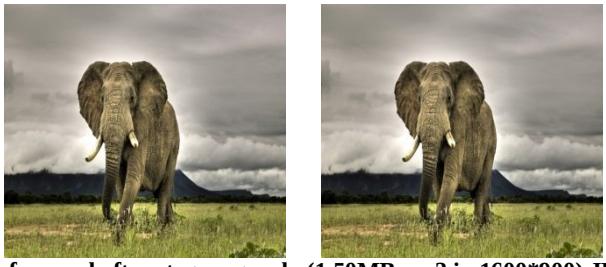

Figure 4. Before and after steganography(1.50MB mp3 in 1600*900) JPEG image

Figure 5.Before and after Steganography(810KB wave file in 553*428 JPEG image.

VIII. CONCLUSION

This technique provide greater amount of flexibility to the user since it allow the hide the audio content in the last three bit of each byte. Therefore it avoids the major limitation of conventional method so more data can be hidden within same medium.. More than three bit for data hiding gives the blurred stego image which can easily suspected by intruders. The future work could be extending to embed the audio message in the video file. The secrete audio channel can also be hide within the broadcasting medium using this technique.

REFERENCES

[1] Sheetal a. kulkarni, shubhangi B. patil, High capacity and robust speech data hiding in color image IEEE-2014 "Global Conference On Wireless Computing And Networking"
[2] M.I.Khalil, "Image Steganography, Hiding short audio messages in digital images", JCS&T Vol 11 No.2.
[3] V. J. Rehna, Member, IACSIT and M. K. Jeya Kumar ,"A Strong Encryption Method of Sound Steganography by Encoding an Image to Audio", International Journal of Information and Electronics Engineering, Vol. 2, No. 3, May 2012.
[4] Jeremiah J. Harmsen," Capacity of Steganographic Channels" IEEE Transactions On Information Theory, Vol. 55, No. 4, April 2009.
[5] Nicholas Hopper, Luis von Ahn, and John Langford" Provably Secure Steganography" IEEE Transactions On Computers, Vol. 58, No. 5, May 2009.
[6] Tao Zhang, Wenxiang Li, Yan Zhang, Xijian Ping, "Detection of LSB matching steganography based on distribution of pixel differences in natural images", IEEE International conference on image analysis and signal processing, pp. 548-552, April 2010.
[7] V. Sathya, K. Balasubramaniyam, N. Murali, Rajkumaran M.,Vigneshwari, "Data hiding in audio signal, video signal text and Jpeg images", IEEE International conference on advances in engineering science and management, pp. 741-746, March 2012.
[8] Mauro Barni" Watermark Embedding: Hiding a Signal within a Cover Image", IEEE Communications Magazine August 2001.
[9] N. Cvejic, T. Seppanen , "A wavlet domain LSB insertion algorithm for high capacity audio steganography," in proc. IEEE Digital signal processing workshop, Callway, GA, pp. 53-55, October 2002.
[10] M. I. Khalil, "Image steganography: Hiding short audio messages within digital images", Journal of Computer Science and Technology, vol. 11, no. 2, pp. 68-73, October 2011.
[11] Chang-Chou Lin, Wen-Hsiang Tsai, "Secret image sharing with steganography and authentication", Journal of systems and software 73 , pp. 405-414, 2004.
[12] Parul Sehgal, Vijay Kumar Sharma, "Eliminating cover image requirement in Discrete Wavelet Transform based Digital Image Steganography, Int. Journal Computer Applications", vol. 68, no. 3, April 2013.
[13] K. Sakthisudhan, P. Prabhu, P. Thangaraj, "Secure audio steganogra- phy for hiding secret information", International Journal of Computer Applications, 2012.
[14] Chi-Kway Chan, L M. Chang, "Hiding data in images by simple LSB Substitution", Journal of pattern recognition society, pp. 469-474,2012.M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.
[15] Agniswar Dutta, Sankar Das, Asoke Nath, "New data hiding algorithm in MATLAB using encrypted secret message", International conference on communication systems and network Technologies, IEEE computer society, 2011.
[16] Joyshree Nath, Saima Ghosh, Asoke Nath, "Advanced Steganography Algorithm using Encrypted secret message and Encrypted embedded cover file", IJACA, vol. 46, no. 14, pp. 1-7, May 2012.
[17] Andrew D. Ker, "Improved Detection of LSB Steganography in grayscale images", Springer, pp. 97-115, 2004.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

[18] Min Wu, Bede Liu, "Data hiding in image and video: Part IFundamental Issues and solutions", IEEE transactions on Image Processing, vol. 12, no. 6, June 2003.
[19] Andrew D. Ker, "Steganalysis of LSB matching in Grayscale Images", IEEE Signal Processing Letters, vol. 12, no. 6, pp. 441-444, June 2005.
[20] Kirti Saroha, Pradeep Kumar Singh, "A Variant of LSB steganography for hiding images in audio", IJCA , vol. 11, no. 6, pp. 12-16, December 2010.
[21] Harvinder Singh, Anuj Kumar, Prateek Bansal, "Analysis and implementation of algorithm to hide secret message", IJARCSSE, vol. 3, Issue 2, pp. 327-333, February 2013.
[22] Rajeev Aggarwal, Jai Karan Singh, Vijay Kumar Gupta, Sanjay Rathore, Mukesh Tiwari and Anubhuti Khare, "Noise reduction of speech signal using wavwlet transform with modified universal threshold", IJCA, vol. 20, no. 5, pp. 14-19, April 2011
[23] Guoshen Yu, "Stephone Mallat, Emmanuel Bacry, "Audio denoising by Time- frequency block thresholding", IEEE transaction on signal processing , vol. vol. 56, no. 5, pp. 1830-1839, May 2008.