Volume 6, Issue 6, June 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Embedding Audio in Image for Hiding Information Using MSB Technique

Dr. B. Geetha Vani
Professor, Dept of CSE
Narayana Engineering College
Nellore, Andhra Pradesh, India

L K Sathya Suneetha
M.Tech Student, Dept of CSE
Narayana Engineering College
Nellore, Andhra Pradesh, India

S. Susmitha
M.Tech Student, Dept of CSE
Narayana Engineering College
Nellore, Andhra Pradesh, India

Abstract*– *The technique used for hiding any secret information behind any cover file is Steganography which means secret writing. This paper conveys the advanced steganography where it uses another medium to hide information of one medium. In this way the existence of the secret information cannot be known to others except from sender and its intended receiver. Here the Most Significant Bit Substitution Method is used to hide the audio message in the color image.

Keywords*– *steganography, RGB guides, MSB substitution, bit conversion

I. INTRODUCTION

In the last years, Internet becomes a popular communication channel. Exchange of information using Internet channel, over far distance, is now an everyday activity. However, that information still have to face some problems, such as data security, copyright control, and …, etc. Thus, we need secure secret communication methods for transmitting massage over the Internet. Two techniques are used to transmit secrets using unprotected communication media: encryption and steganography are the preferred techniques for protection the transmitted data. Encryption conceals the message by scrambling the data being communicated, while steganography hides the message in innocent digital file. The purpose of steganography is to conceal the fact that some communication is taking place. With any type of hidden communication, the security of the message often lies in the secrecy of its existence and/or the secrecy of how to decode it. The steganography hides the secret information behind a cover so that it draws no special attention. The cover represents any digital file like audio, image, text, video and …, etc. If we used the digital image, the cover-image after embedding is called stego-image.

Major constraint of today's computer communication is to prevent the data to be revealed to the illicit user. There are various techniques for data hiding such as cryptography, steganography, etc. From these techniques, Steganography is applied for hiding confidential or susceptible information within a carrier that emerges to be nothing. Both Cryptography and steganography techniques are used to protect confidential information. The difference between the two is that Steganography involves hiding information which appears that there is no information is hidden. The most well known and simplest steganography technique is least significant bit (LSB) substitution. However, effective audio data hiding is done in color image will create robust and invisible data that allows protection for the secret message exchange.

Basic terminologies associated with the steganography are summarized below which help in the further approach.

Payload: The information which is to be covered, here audio is used as payload.

Carrier: The media where payload has to be concealed which is color image we used here.

Stego: The medium in which the information is hidden.

Steganalysis: The process of detecting hidden information inside the file

Redundant Bits: The information inside a file which can be altered without damaging the file.

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

Cover image+ Audio message +Stego key = stego image

The common well-known and widely used steganographic method today is the least significant bits (LSBs) substitution. Many public steganographical softwares, such as S-Tools, EZstego and Steganos apply this technique. On significant advantage of this method is that it is simple to understand and implement. This technique replaces the fixed-length LSBs of pixels with the embedding data. However, not all pixels in cover image can tolerate equal amount of changes occur in smooth areas can be easily noticed by human eyes. Adaptive methods for steganography are introduced in which the amount of embedding data in a pixel is variable. These adaptive methods provide more imperceptible results than those employed by simple LSBs substitution schemes. In our proposed method, we will hide an embedded data by using variable-length LSBs of pixels, and determined depending on the correlation between eight neighboring pixels. Therefore, this method does not replace the bits of embedded data directly, but changes the pixel value into another similar value according to the result of correlation and still nearest to its neighbors especially in smooth areas. The range of changeable pixel value in smooth areas is small and in edge areas is large, so that the stego image still maintains good perceptual quality. This steganographic method provides an acceptable embedding capacity with little perceptual distortion.

II. RELATED WORK

LSB Substitution Method

LSB (Least Significant Bit) is the popular algorithm, which replaces the least significant bit in some bytes of the cover file to hide a sequence of bytes containing the hidden data. This is usually an effective technique in cases where the LSB substitution does not cause significant quality degradation.

The message 'HEY' is encoded in a 16-bit CD quality sample using the LSB method is as illustrated in Fig.1. Here the secret information is „HEY‟ and the cover file is audio file. HEY is to be embedded inside the audio file. First the secret information „HEY‟ and the audio file are converted into bit stream. The least significant column of the audio file is replaced by the bit stream of secret information „HEY‟. The resulting file after embedding secret information „HEY‟ is called Stego-file.

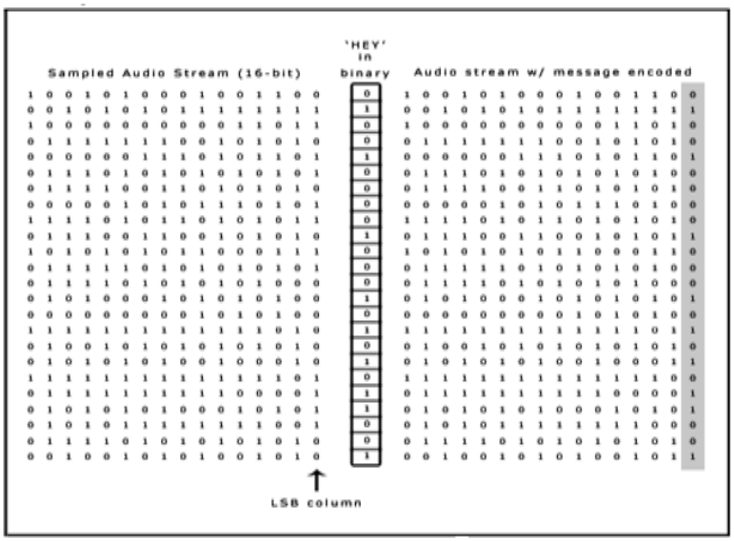


Fig 1: LSB Coding Example

MSB Substitution Method

MSB (Most Significant Bit) is also an algorithm, which replaces the most significant bit in some bytes of the cover file to hide a sequence of bytes containing the hidden data. This is usually an effective technique in cases where the MSB substitution does not cause significant quality degradation.

It is very similar to the above LSB Substitution Method. The only difference is the “HEY” in binary is embedded in the most significant bits of the sampled audio stream for the above example.

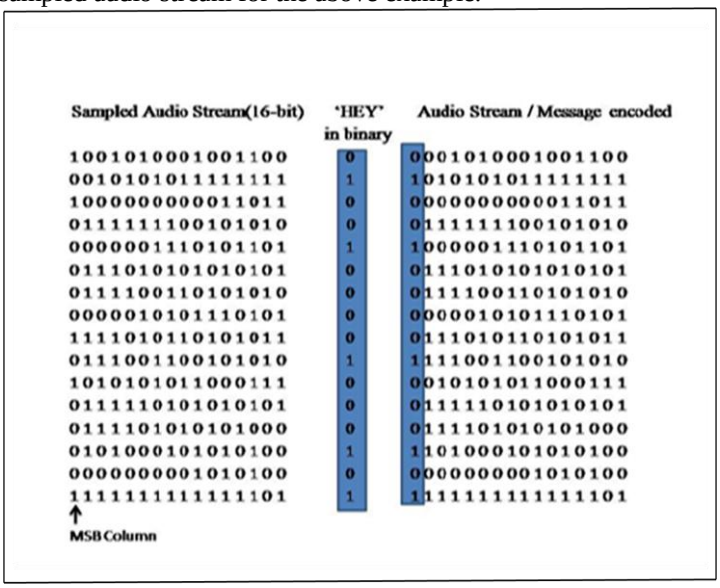


Fig 2: MSB Coding Example

RGB Color Channels

An image can be signified by a group of color pixels. The individual pixels are represented by their visual features like “clarity”, “power”, ”disparity”, etc. Each of these features can be digitally uttered in terms of 1’s and 0’s basic. Different forms for storing images are presented by the three color channels, RGB. To specify, create and visualize color, color space is a method by which it is feasible. The RGB (Red, Green, and Blue) is the most common color space among all. To make the final color's spectrum, the RGB color form is an additive in the sense that the three light beams are added together, and their light spectra also added. 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. The characteristics of the pixel formed by the Combination of these values. The RGB color model already had a solid theory behind it, based on human insight of colors.

An image is nothing but the strings and strings of bytes, each byte indicating a different color. The first few bits in a color byte, however, holds much important. But it is to say that two bytes that vary in the first few bits can specify two colors that are nearly impossible to differentiate to the human eye.

III. PROPOSED METHODOLOGY

In this paper, the possibility of hiding audio information within the digital image is studied. As we know there are various types of audio files such as wave file (wav) and MPEG Layer-3 (mp3) file etc. It has been seen that the any of the audio file is used for hiding the information. Here the long process is not required. It can be directly converted into the digital form, as there are 8 bits in each byte, and the one pixel is having basically three colors Red, Green and Blue so it forms 24-bit format we can hide first three bit in the first red color byte and next three bit in the next green color byte and next three bit in the next blue color byte. By this we can observe that the capacity of hiding information is increased in each pixel. So it can be possible to hide large audio file within the color image.

Hiding an Audio Message within Color Image Using MSB Technique

An audio file divided into different type of field like header, size of data, and content of audio message bit per sample format etc. Each of these fields is converted into bit array format for hiding in digital image. The mostly used audio files are wave file but which is having fix byte of header and all the content should arranged in sequence but the problem is that it required large memory space so the hiding data limit are less. In this approach we are using MPEG Layer-3 (mp3) file and the advantages is that the audio file in mp3 form can be compressed so the more data can be hidden in same memory size. The relationship between the size of the audio file and the cover image is given by-

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

Where W and H are the width and height of the cover image and A is the size of the audio file.

Therefore the maximum size of audio file are A= (9*W*H)/16.

Here we proposed the MSB substitution method for hiding audio information within the color image. It is similar to the process of hiding audio message within the color image using LSB method. But only the difference is instead of replacing the least significant bits of color image by the sampled bits of audio message, here the replacement is done on the most significant bits of the color image by the sampled audio message. The entire process is represented in the following flow chart.

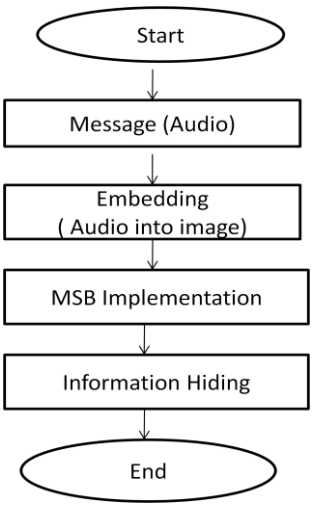


Fig 3: Flow Chart

There are some steps need to be follow until the research will be completed. These steps will helpful to design the hiding technique. These are elaborated as:

1. Study the Steganography and Advanced Steganography Working.
2. Analyze the Point of Security Implementation and study the flow of working.
3. Implement the proposed technique in any of the programming language.
4. Generate appropriate results and graphs.
5. Source of Research will be internet, Websites and Journals

BUILDING BLOCK OF PROCESSING

Steps for Data Embedding:

1. Read the cover image.
2. Write the audio file to be embedded. Convert it into a sequence of binary bits.
3. Every message bit from step 2 is embedded into the MSB bits of the samples of the digitized cover image.
4. The modified cover image samples are then written to the file forming the stego-image.

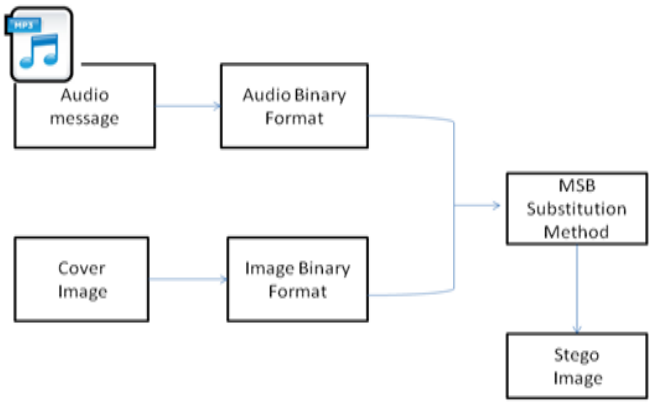


Fig 4: hiding the audio message in cover image

Steps for Data Retrieval:

1. Read the stego-image.
2. Retrieval of redundant bits is done by checking MSB bits of the samples.
3. After every such redundant bits retrieved, they are converted into their decimal equivalents and finally the secret audio signal reconstructed.

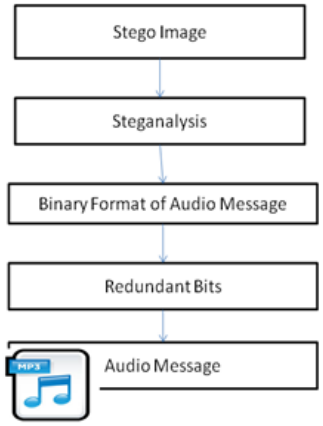


Fig 5: Receiving the audio message

IV. IMPLEMENTATION AND OUTPUT

By using image processing toolbox our proposed work has been implemented. We obtained the snapshot of the result which shows the color image converted into the binary form shown in Fig.6. Before and after hiding the content of audio information using MSB method that mentioned above have a group of images as shown in Fig.7 and Fig.8. The first two most significant bits are replaced by the mp3 or wave audio message content using encryption technique. The mp3 or wave audio content are recovered using decryption technique. The alterations in the cover image in which the audio is concealed are so minute that cannot be observed by the human insight. Thus, stego image looks like the cover image and the recovered audio message will also appears identical to the original data that was sent.

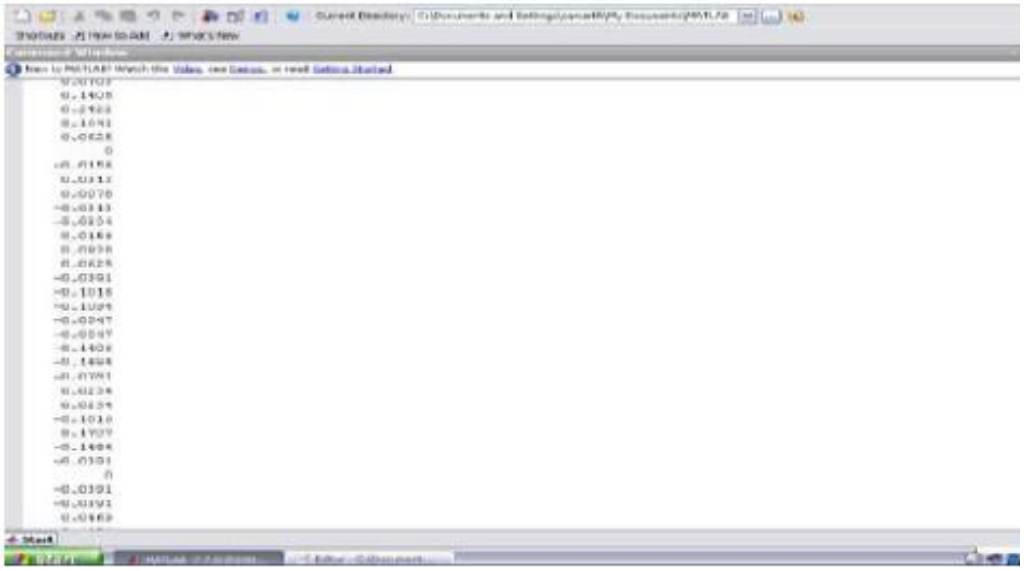
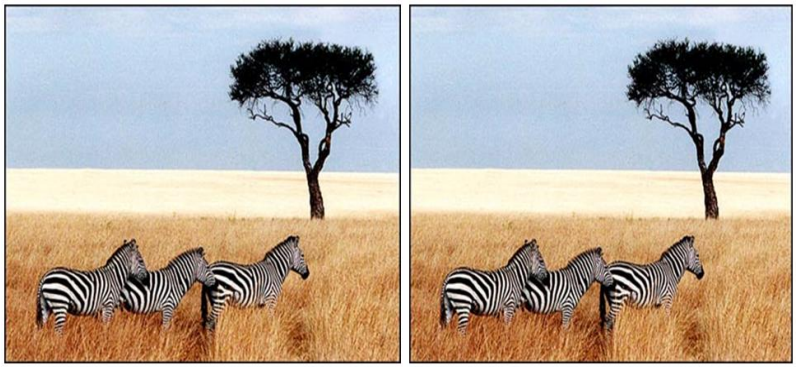


Fig 6: Snapshot of color image in bit array form



Before After

Fig 7: Before and after steganography (wave) JPEG image

Before After

Fig 8: Before and after steganography (mp3) JPEG image

V. CONCLUSION

In our advanced steganography algorithm, there is no need of referencing the original image when extracting the embedded data from a stego-image. The stego image depends on itself to extract the secret message by finding the value of difference using the pixels of stego image only. The pixels in edge areas embed more data than those in non-edge areas because the value of difference is large. The explanation for this large value of difference in edge area is that in edge area there is a large change in image brightness (gray levels) over a short spatial distance.

This technique provide greater flexibility to the user because it allows hiding the secret information in the first two bits of each byte of color image so that it also avoids the major limitation which arise in conventional method, audio steganography by using this technique. But if we use more than two bits of each color byte it may give a blurred stego image which can be easily susceptible.

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] 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.

[9] 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.

[10] Andrew D. Ker, "Improved Detection of LSB Steganography in grayscale images", Springer, pp. 97-115, 2004.

[11] Ping Wah Wong and Edward J. Delp, editors, Security and Watermarking of Multimedia Contents‖, Volume 3657, Society of Photo-optical Instrumentation Engineers, 1999.

[12] R.Anderson, and F.Petitcolas, On the limits of the Steganography‖, IEEE Journal Selected Areas in Communications, vol .16, no. 4 , May 1998.

[13] W. Bender, D. Gruhl , N. Morimoto, and A. Lu, Techniques For Data Hiding‖, IBM Systems Journal, vol. 35, nos 3&4, 1996.

[14] Ping Wah Wong and Edward J. Delp, editors, Security and Watermarking of Multimedia Contents II‖, Vol. 3971, Society of Photo-optical Instrumentation Engineers, 2000.

[15] Poulami Dutta, Debnath Bhattacharyya, and Tai-hoon Kim, Data Hiding in Audio Signal: A Review‖, International Journal of Database Theory and Application, vol. 2, no. 2, June 2009.

