ISSN No. 0976-5697

Volume 8, No. 5, May – June 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

An Adaptive Lossless Image Steganographic Scheme to Conceal Audio in an Image using LSB and Key Vector Methods

K.S.Sadasiva rao
Associate Professor
Dept of CSE, Sri Indu Institute of Engineering and Technology
Hyderabad, India

Dr A. Damodaram
Professor of CSE
School of Information Technology, Jawaharlal Nehru Technological University, Hyderabad & The Vice Chancellor
SVU University, Tirupathi, India

Abstract: In recent years, innovation of technology and fast internet services make it possible to distribute the information and digital services to the overall world in a simple and cost effective manner. The rapid growth in information technology and digital communication has become very significant to protect the information transmission between sender and receiver. Steganography is the process of embedding original message bits on some carrier file. The carrier file may be text file, image file, audio file or video file etc. If that carrier file is an image file, then that technique is called Image steganography. If color image is used as a carrier file to embed data bits, then that type of steganographic technique is called as color image steganography . Therefore, Steganography introduces a strong way to conceal information and to converse a secret data in an appropriate multimedia carrier file, eg. Image, text, audio and video files. In this paper, an adaptive lossless data hiding technique is presented which is capable of hiding some bits of large size audio wave file binary information into an image using 2 bit LSB method and the remaining bits by generating decimal key vector.

Keywords: Steganography, color image steganography, multimedia carrier file, LSB method decimal key vector.

I. INTRODUCTION

Since the rapid growth of information technology and digital communication has become very important to secure the information transmission between sender and receiver [3], Cryptography and Steganography are the two techniques which are most commonly used to secure the information. Cryptography was created as a technique for securing the secrecy of communication and many methods were designed to encrypt and decrypt data in order to uphold the secrecy of the message. Unfortunately, sometimes it is not just enough to keep the content of the message secret but also the existence of the message [4]. The technique used to maintain the secrecy about the existence of the message is called Steganography. Data hiding techniques play very important roles in the era of the rapid growth of the intensive transfer of multimedia contents and secret communications. On the other hand, Steganography is one of the most important information hiding techniques. [7].

Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the transmitted information. The word steganography is derived from the Greek words “stegos” meaning “cover” and “grafia” meaning “writing” defining it as “covered writing”. In Image steganography the information is hidden exclusively in images [5].

Image steganography can be implemented either on gray scale images or on color images. The gray scale image uses 8 bits to represent a pixel element. The color image is a combination of three planes Red, Green and Blue. In color images, it requires 24 bits to represent each pixel [14]. Each pixel requires 24 bits to represent red, green and blue components with each of 8 bits. In a color image every pixel value is composed of red, green and blue components and each of which ranges a positive decimal value from 0 to 255.

The source image file which we are using to hide the information is called ‘cover image file’. After embedding the secret information on the cover file, the image which is generated for transmission is called ‘stego file’. Steganographic techniques can be used in several areas like military, commercial, anti-criminal and so on [6].

II. RELATED WORK

Steganography is a process of hiding data in other media to transfer the secured information [1]. Most of the steganographic algorithms are working on gray scale images, but some unauthorized user may suspect some useful information is going in gray scale image, because now a day’s nobody is interested in sending gray scale images as general images [8]. Actually many steganographic techniques have been implemented either in color or gray scale images, but in color images all the three planes RGB have been used to stuff the bits. Hence in color image steganography, by using LSB method 3bits/pixel can be replaced with secret data.

The Image steganographic algorithms are divided into spatial domain and Transform domain. In Spatial Domain technique the bits in pixels of the carrier color image are directly replaced by the original secret data bit. Whereas in case of transform domain techniques, the pixels are transformed into transform domain; those co-efficient values are used to embed the secret data bits.

Many papers have been presented to hide the image data into an audio file [9][10][11]. But there is less contribution about embedding the audio information in image. By using image steganographic techniques it is possible to hide the audio binary information in pixel/plane binary information of an image.

III. PROPOSED SYSTEM

A file with the .WAV or .WAVE file extension is a Waveform Audio file. This is a standard audio format seen mainly on Windows computers. WAV files are usually uncompressed but compression is also supported [9]. WAV is an extension of the bit stream format Resource Interchange File Format (RIFF). WAV is similar to AIFF and 8SVX files, both of which are more commonly seen on Mac operating systems. By using MATLAB commands a wave file can be converted into binary form [10]. The 'wavread' command loads a sound file specified by the string wavfile, returning the sampled data in *y*. Amplitude values are in the range [-1,+1] supports multi-channel data in the following formats: 8-bit mu-law, 8-, 16-, and 32-bit linear, and floating point [11]. By using 'dec2bin' with 'typecast' function the wave data converted into completely binary form represented in matrix format of 'n' rows by 8 columns. But the size of the wave file binary form is too large to fit / replace with the bits of an image.

In this proposed work, we applied an Image Steganography technique that embeds the binary form information of audio file into a color image. The color image is represented with RGB planes combination for each and every pixel. A pixel indicated with a total 24 bits, out of which 8 bits are used for each and every plane [5]. The 8 bits of every pixel/plane can have the decimal value ranging from 0 to 255 to represent the respective color impression. By changing the LSB of any pixel/plane, there is no much distortion in the image quality. As the size of the audio wave file is too large, it is not possible to hide the total data bits of wave file into image file[11]. Hence in this proposed system, out of 8 bits in each row of the matrix vector only the 4^{th} bit and 8^{th} bits were placed at LSB 2 AND LSB 1 positions of each and every pixel / plane. Initially all the Red Plane bits were used to embed the data. Upon completion of all the red plane 2-LSB's, next the Green plane was chosen. Finally the Blue plane is used to embed the data bits. Out of 8 bits only the 4^{th} and 8^{th} bits are embedded in pixel / planes of color image. The remaining 1 to 3 bits and 5 to 7 of wave file each row binary information bits, each 3 bits are separately converted into decimal form and the values are stored in a separate 2 column key vector.

After completion of embedding process, the 'stego image' and the key vector are transmitted to the destination end. At receiver side, the sound wave bits are re-generated by collecting the 1 to 3 and 5 to 7 bits from key vector as well as 4^{th} and 8^{th} bits from the 2-LSB position of the color image pixel / planes. The generated binary information converted into wave data form; so that the same audio sent at sender side can be heard at receiver side.

IV. PROPOSED SYSTEM AT SENDER SIDE

Hence almost all the steganographic algorithms either spatial domain or transform domain is using bit replacement algorithms [4]. steganalysis techniques are used to find whether the data bits are stuffed in the carrier image. These Steganalysis techniques are mostly working on the statistical characteristics of an image [1] [2]. Whenever there is partial or slight change in the carrier image, those changes can be detected by commercial steganalysis tools, even though it is not identified by human naked eye. Most of the LSB based steganographic algorithms will be getting PSNR value which is much more than 20 (i.e., if this value is greater than 20, human eye cannot detect the change in the stego image comparing with cover image). Also, the LSB based and the related steganographic techniques are simple, well known and easier to identify it by the steganalyst.

In this proposed paper, at sender side, the 'wavread' command reads a gray scale or color image from the file specified by the string FILENAME. The text string FMT specifies the format of the file by its standard file extension. The return value A is an array containing the image data. If the file contains a gray scale image, A is an M-by-N array. If the file contains a true color image, A is an M-by-N-by-3 array. By using 'dec2bin' with 'typecast' function the wave data converted into completely binary form represented in matrix format of 'n' rows by 8 columns, but the size of the wave file binary form is too large to fit / replace with the bits of an image file. By changing the LSB of any pixel/plane, there is no much distortion in the image quality. As the size of the audio wave file is too large, it is not possible to hide the total data bits of wave file into image file [12]. Hence in this proposed system, out of 8 bits in each row of the matrix vector only the 4^{th} bit and 8^{th} bits were placed at LSB 2 AND LSB 1 positions respectively for each and every pixel / plane. Initially all the Red Plane bits were used to embed the data. Upon completion of all the red plane 2-LSB's next the Green plane was chosen. Upon completion of all the Green plane bits, finally the Blue plane is used to embed the data bits. Out of 8 bits only the 4^{th} and 8^{th} bits are embedded in pixel / planes of color image. The remaining 1 to 3 bits and 5 to 7 bits are separately converted into decimal form and the values are stored in a separate 2 column key vector i.e. key(x,2). The first column of the key vector i.e. key(x, 1) represented with the decimal equal value of the 1 to 3 bits of the corresponding pixel / plane. The second column of the key vector i.e. key(x, 2) represented with the decimal equal value of the 5 to 7 bits of the corresponding pixel / plane.

Algorithm at Sender Side:-

1. Read the Wave file data in wave file format i.e. wavdata(x, 2).
2. Convert the wavdata into binary format i.e. wavbin(x, 8).
3. Read the RGB pixel/plane binary values of Cover Image file.
4. Place all the Wave file binary values into Cover Image RGB vectors and Key vector k(x, 2).
   a. Read each row (for x in 1 to all) binary 8 bits of wavbin(x, i) for each i,(1 to 8).
   b. Hide the 4^{th} it and 8^{th} bit of 'wavbin' into LSB 2 and LSB 1 position of RGB key vectors.
   c. Place the 1 to 3 bits and 5 to 7 bits of 'wavbin' into 1^{st} and 2^{nd} columns of key vector i.e. key(x, 1) and key(x, 2) in decimal value format.
5. Generate 'Stego Image' with modified RGB plane vector values.
6. Transfer the Stego Image and Key vector values to destination (Receiver).
7. Terminate the program.

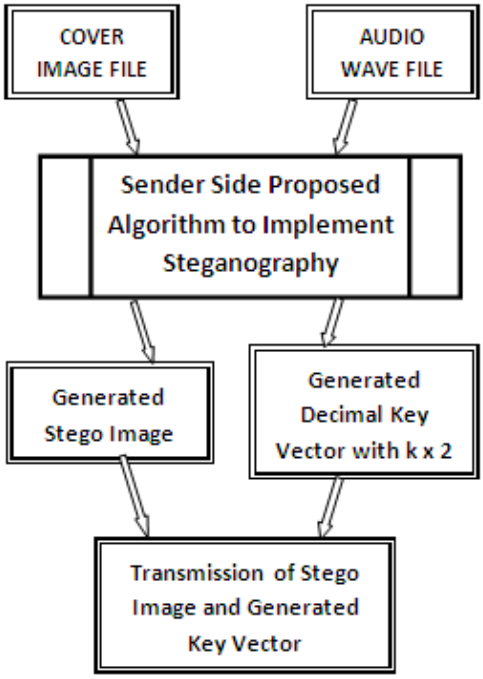

Fig 1: Proposed system at Sender Side.

V. PROPOSED SYSTEM AT RECEIVER SIDE

In this proposed paper, at Receiver side, both the stego image file and a two column key vector file were received. It is algorithm at receiver side, which takes an active participation in reconstructing the original wave file by collecting the bits from both the stego image file and key vector. It serially regenerates the 8 bits columns at each row by collecting the 1 to 3 bits from 1st column of the key vector, 4th bit from 2nd LSB of the stego image corresponding pixel / plane, again 5 to7 bits from 2nd column of the key vector and the last 8th bit from 1st LSB of the stego image corresponding pixel / plane. It continuously collects all the bits of the binary wave file and regenerates the wave data. The generated wave data vector used to play the audio information.

Algorithm at Receiver Side:-

1. Read the Stego Image and convert into RGB plane vectors.
2. Read the values at n x 2 columns of the key vector.
3. Frame the binary values for the vector (conwav) for generating new wave file :-

a. For each row (with 8 bits) generating of 'conwav' vector
b. Select first 3 bits from 1st column of key vector and convert into binary i.e. dec2bin(key(x,1)).
c. Select the 4th bit from 2nd LSB of corresponding pixel / plane.
d. Select the next 3 bits (5 to 7 bits) from 2nd column of key vector and convert into binary dec2bin(key(x,2)).
e. Select the 8th bit from 1st LSB of corresponding pixel / plane.

4. Reconstruct the total wave file binary vector (conbin(x, 8)).
5. Regenerate the new wavdata1(x, 2) file and play it with wavplay(wavedata1, frequency).
6. Terminate the program.

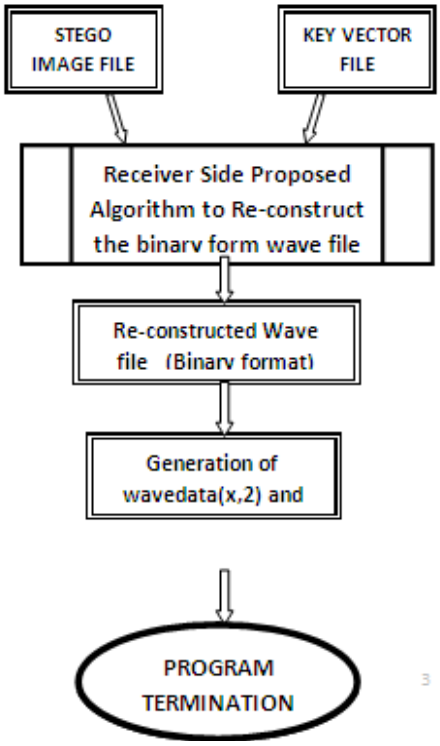

Fig 2: Proposed system at Receiver Side.

VI. RESULTS

The following are the results produced while transmitting six different wave files using six different cover images. In all the examples out of 8 bits of a wave binary file row, 2 bits were embedded at 2 LSB positions of RGB pixel / planes of the cover images and rest of the 6 bits were placed in 2 column key vector by dividing 3 bits equivalent decimal value in each column. At receiver end, again to reconstruct the original wave file, the bits are recollected back from stego image and key vectors. The following are the sample wave files and cover images used in implementing image steganography to embed audio waves in cover image file.

Table 1: Table showing the number bits embedded in experiments

Experiment Code	Wave file used (.wav)	Image file used (.jpg)	Number of bits embedded in image	Number of bits stored in key vector (n X 2)
T1	trees	flower	23,35,968	70,07,904
T2	safety	lena	29,24,448	87,73,344
T3	silence	Lion	55,10,224	1,65,30,672
T4	greenery	rocket	39,58,768	1,18,76,304
T5	bell	swan	14,09,856	42,29,568
T6	alupannadi	flight	38,50,240	1,15,50,720

Table 2: Table showing the MSE & PSNR values for experiments

Experi-ment Code	RED PLANE MSE	GREEN PLANE MSE	BLUE PLANE MSE	TOTAL IMAGE MSE	PSNR VALUE
T1	3.0681	0.3398	0	1.136	59.6523
T2	3.0162	1.1504	0	1.3889	58.7794
T3	2.8577	2.8633	1.7702	2.4971	56.2317
T4	2.9722	2.5908	0	1.8543	57.5241
T5	2.0156	0	0	0.6719	61.9332
T6	2.9342	2.4734	0	1.8025	57.6472

Fig 3: Sample picture used to hide the wave file (T3)

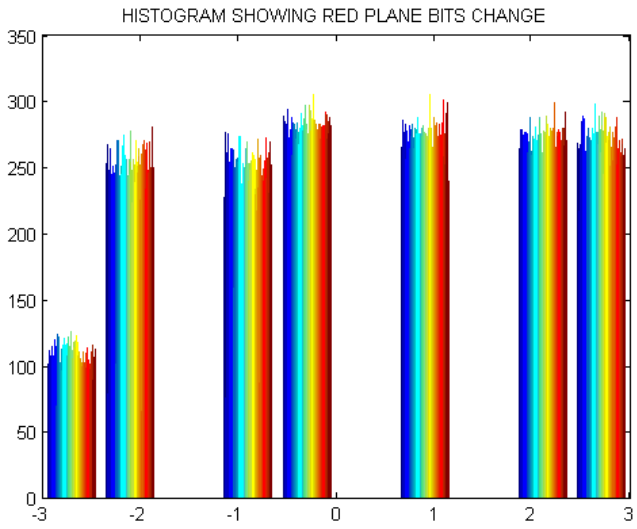

Fig 4: Histogram showing the variation in Red plane while embedding the wave file (T3) at 2 LSB's.

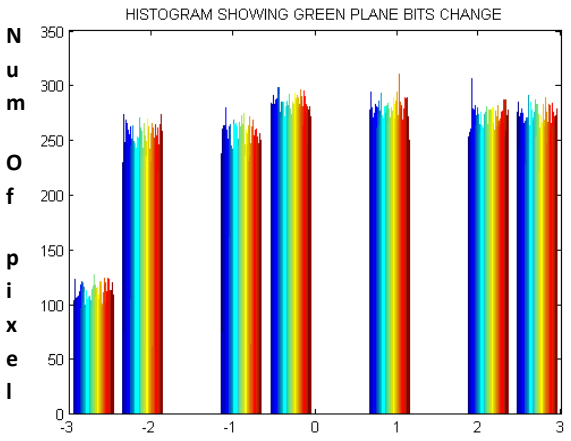

Fig 5: Histogram showing the variation in Green plane while embedding the wave file (T3) at 2 LSB's.

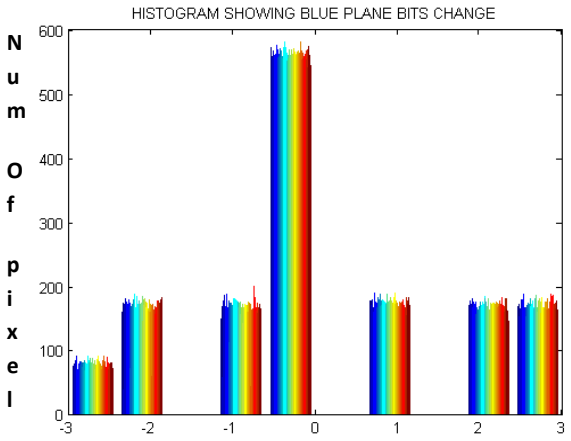

Fig 6: Histogram showing the variation in Blue plane while embedding the wave file (T3) at 2 LSB's.

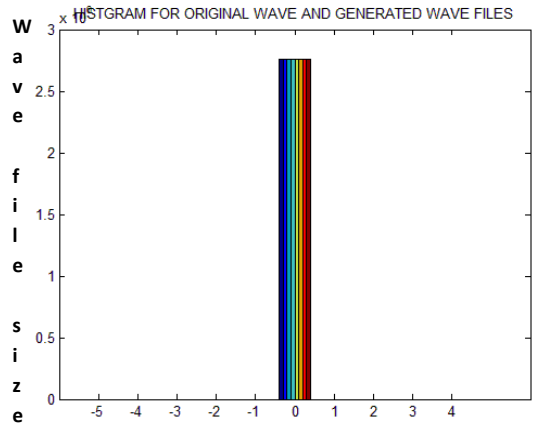

Fig 7: Histogram showing the variation between the source wave file at Sender side and the re-constructed wave file at Receiver side.

VII. CONCLUSION

In our proposed system, we have constructed and sent the Key vector with two columns consisting of 1 to 3 bits and 5 to 7 bits equivalent decimal values as well as a stego image consisting of 4^{th} bit and 8^{th} bit of wave file at 2-LSB positions. At receiver end by re-constructing the wave file in binary form data, it is possible to play the audio without any distortion. As the size of the wave file is very large, it is not possible to embed the whole wave file data into any image. Hence to maintain the security 4^{th} and 8^{th} positional bits of wave file binary information was embedded at 2-LSB positions of the RGB planes of the pixel/planes of the picture. The remaining 1 to 3 bits and 5 to 7 bits of the wave file binary data placed at two columns of the key vector by converting each 3 bits into its equivalent decimal form. The generated key vector and stego image file were transmitted through channel from sender to receiver. At the Receiver end, the key vectors and the Stego image file are used as input for the proposed algorithm. The proposed algorithm at receiver end recollects all the data bits represented by the mapping vector and 2 LSB values of Stego file and makes each 8 bits group. Each 8 bits group is useful in Re-constructing the original Wave file. In this proposed algorithm, we are using a logic with which we can transfer a wave file data bits without disturbing the quality of audio.

REFERENCES

[1]. Niels Provos and Peter Honeyman, "Hide and Seek: An Introduction to Steganography", IEEE Security & Privacy, 2003, pp. 32-44.

[2]. Niel F Johnson, Sushil Jajodia, "Exploring Steganography: Seeing The Unseen", IEEE, 1998

[3]. Odai M. Al-Shatanawi and Nameer N.El. Emam, "A New Image Steganography Algorithm Based on MLSB Method with Random Pixels Selection", IJNSA, Vol.7, No. 2, March 2015, pp. 37-53.

[4]. Tahir Ali, Amt Doegar, "A Novel Approach of LSB Based Steganography Using Parity Checker", IJARCSSE, Vol.5, Issue 1, January 2015, pp. 314-321..

[5]. T. Morkel, J.H.P. Eloff, M.S. Oliver, "An Overview of image steganography", Pretoria, South Africa, Information and Computer Security Architecture (ICSA) Research Group, pp 1-11, June 2005.

[6]. J.K. Mandal and Debashis Das, "Color Image Steganography Based on Pixel value Differencing in Spatial Domain", IJIST, Vol. 2, No. 4, July 2012.

[7]. MARWA M Emam, Abdelmgeid A Aly, Fatma A. Omara, "A modified Image Steganography Method based on LSB Technque", IJCA, Vol. 125, No. 5, September 2015.

[8]. Neha Gupta, Nidhi Sharma, "Hiding Image in Audio using DWT and LSB", IJCA, Vol. 81, No. 2, November 2013, pp.11-14.

[9]. Jayaram P, Ranganatha H R, Anupama H S, "Information Hiding Using Audio Steganography-A Survey", IJMA, Vol. 3, No. 3, August 2011.

[10]. Ankit Chadha, Neha Satam, Rakshak Sood, Dattatray Bade, "An Efficient Method for Image and Audio Steganography using Least Significant Bit (LSB) Sustitution", IJCA, Vol. 77, No. 13, September 2013, pp. 37-45.

[11]. Sudha Lakshmi N, "Audio Steganography Using Least Significant Bit", IJIRCCE, Vol.2, Special Issue 1, March 2014.

[12]. Ramadhan Mstafa, Christian Bach, "Information Hiding in Images Using Steganography Techniques", ASEE Northeast Section Conference, Norwich University, March 14-16, 2013.

[13]. Tahir Ali, Amit Doegar, "A Novel Approach of LSB Based Steganography Using Parity Checker", IJARCSSE, Vo 4, Issue 1, January 2015, pp 314-321.

[14]. Mehdi hussain and Mureed hussian, "A survey of image steganography technique", International Journal of Advanced science and technology, vol.54, May 2013, pp.113-123.

[15]. B. Geethavani, L.K. Satya suneetha, S. Susmitha, "Embedding Audio in Image for Hiding Information using MSB Technique", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 6. No. 6, June 2016, pp. 444-449.

