Steganography: With Hiding Audio Message within Digital Image Based On LSB

Rupali Khot, Prof.A.S.Patil

Padmabhooshan Vasantdada Patil Institute of Technology, Pune, MS-India

***Abstract* -** To provide security in modern communication media steganography is used. Steganography is a technique of hiding message from third party. It is the technique of covering one medium of communication within another medium. Different mediums available are text, image, audio and video. Digital images are mostly used because of their frequency on the internet. Redundant bits of data from hidden message are replaced by embedding process which will create stego image. This paper will give possibility of hiding audio message data inside digital image.

***Keywords* -** *Steganography, Audio message, Image hiding, least significant bit (LSB) method.*

I. INTRODUCTION

To solve major issue of modern communication is to prevent information from third party. Steganography plays an important role in hiding data. Data is hidden inside a cover and that cover is called as carrier. Carrier may be text, image, audio or video. Depending upon this carrier steganography is classified as text steganography, image steganography, audio steganography and video steganography

A. Text Steganography

Text steganography can be achieved by altering the text formatting, or by altering certain characteristics of textual elements (e.g., characters). It includes line-shift coding, word-shift coding and feature coding.

B. Image Steganography

Images are the most popular cover objects used for steganography. . In the domain of digital images many different file formats exist and for these file formats different algorithms exist. These different algorithms used are least significant bit insertion, Masking and filtering, Redundant Pattern Encoding, Encrypt and Scatter, Algorithms and transformations.

C. Audio Steganography

In audio steganography, secret message is embedded into digitized audio signal which result slight altering of binary sequence of the corresponding audio file. There are several methods like LSB coding, Phase coding, spread spectrum, Echo hiding which are used for audio steganography.

D. Video Steganography

Video files are a collection of images and sounds, so most of the presented techniques on images and audio can be applied to video files too. The advantages of video are the large amount of data that can be hidden inside and the fact that it is a moving stream of images and sounds. Basics of steganography is as shown in figure 1.

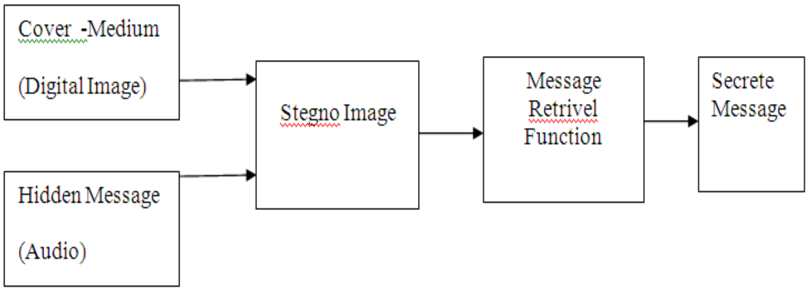


Fig.1: Basics of steganography

Message is the hidden data that will embed into carrier file.The embdding process consist of the sequential substitution of each LSB-1 of the image pixel for the bit message.This method conceal a great volume of information. To apply LSB-1 method, consider that we have to hide the secret data in cover image .The following steps illustrate how this method is used to hide the secret data in cover image.

First step: Convert the data from decimal to binary.

[Message] Dec 2 Bin → [1000001]

Second step: Read Cover Image as shown in figure 2:

182	182	180	180	180	179	176	174
181	182	181	180	179	178	175	174
178	178	178	176	173	172	169	171
174	175	175	172	166	163	164	164
172	173	173	171	167	164	163	163
175	175	175	173	171	168	166	166
177	176	175	174	173	172	169	168
173	172	171	170	171	…..	….	…..

Fig.2: The cover image

Third Step: Convert the Cover Image from decimal to binary.

10110110	10110110	10110100	10110100	10110100	10110011	10110000	10101110
10110101	10110110	10110101	10110100	10110011	10110010	10101111	10101110
10110010	10110010	10110010	10110000	10101101	10101100	10101001	10101011
10101110	10101111	10101111	10110000	10101101	10101100	10101001	10101011
10101100	10101101	10101101	10101011	10100110	10100011	10100100	10100100
10101111	10101111	10101111	10101101	10101011	10100100	10100011	10100011
10110001	10110000	10101111	10101110	10101101	10101100	10101001	10100100
10101101	10101100	10101011	10101010	10101011	……………	…………….	…………..

Fourth step: Break the byte to be hidden into bits.

Thus [10110110] is divided into 8 bits → [1 0 1 1 0 1 1 0].

Fifth step: Take first 8 byte of original data from the Cover Image.

10110110	10110110	10110100	10110100	10110100	10110011	10110000	10101110

Sixth step: Replace the least significant bit by one bit of the data to be hidden.

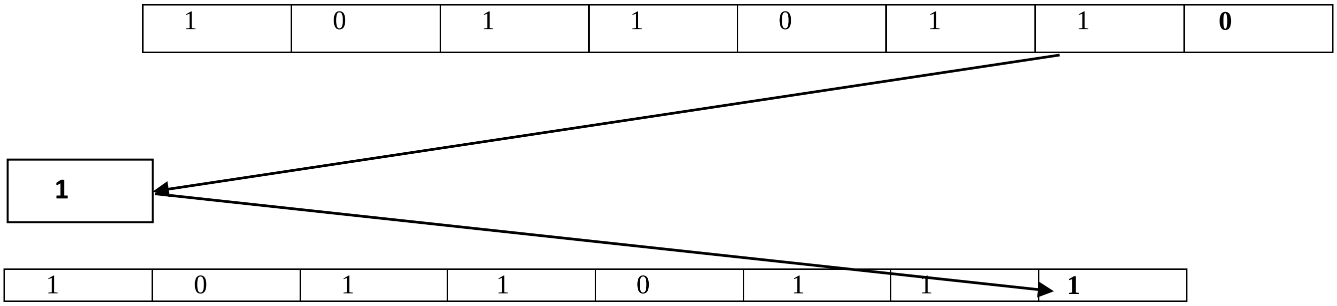
i) First byte of original data from the Cover Image :

1	0	1	1	0	1	1	0

First bit of the data to be hidden:

1

ii) Replace the least significant bit :



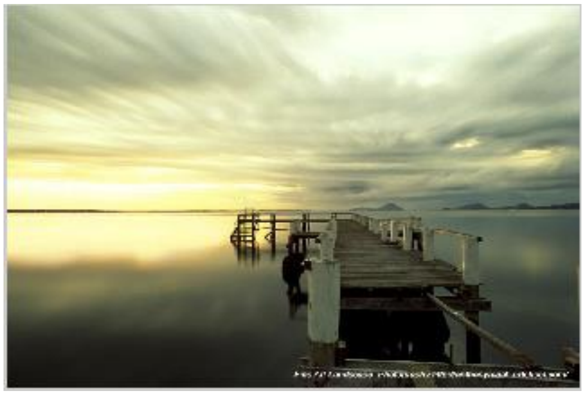
1	0	1	1	0	1	1	**0**

1

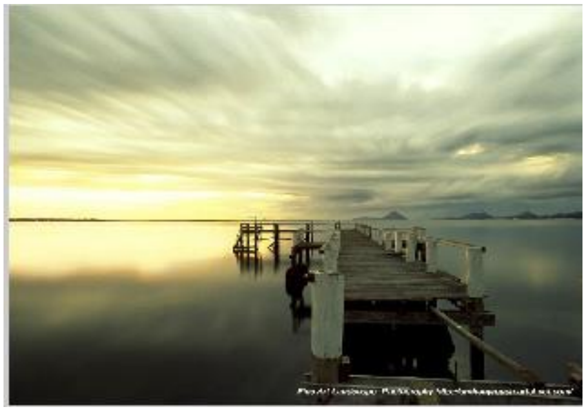
1	0	1	1	0	1	1	**1**

iii) Repeat the replace for all bytes of Cover Image :

iv) Finally the cover image before & after steganography is shown in fig 3.



Cover image before steganography



Cover image after steganography

Fig.3: The cover image before and after steganography

II. PROPOSED METHOD

In this method color image has been used as carrier and hidden message is audio data.figure 4 and figure 5 shows bit encryptions and decryption methods. LSB-2 of carrier is used to embed the audio message.There are different types of audio files. Audio files are wave files and (mp3) files.format of audio file is simple as compaer to othres.wave files are store samples “in the raw”which will not requier processing.First 44 bytes describes the header.The length of audio data is stored in bytes 40-43 and audio samples occupies the remainder of the file starting from byte 44.wave file format is as shown in table-1.Digital images use either 8 bit or 24 bit color.for 8 bit each color is denoted by an 8 bit value where as for 24 bit each pixel is denoted by 3 bytes each byte reprenting the intensity of the three primary colors red,green and blue (RGB) respectively.

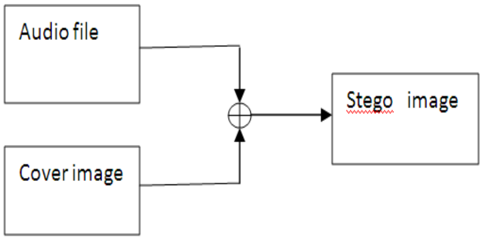


Fig.4: Bit encryption diagram

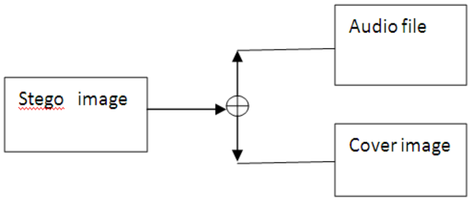


Fig.5:Bit decryption diagram

For hiding capacity the size of information to be hidden relatively depends upon on the size of cover image.The message size must be smaller than image.

Table-1

Byte Number	Description
0-3	“RIFF”(ASCII Character)
4-7	Total length of package to follow
8-11	“WAVE” (ASCII Character)
12-15	“fmt” (ASCII Character)
16-19	Length of format chunk
20-21	Always 0x01
22-23	Channel number(Always 0x01=mono,0x02=stereo)
24-27	Sample rate(binary ,in Hz)
28-31	Byte per second
32-33	Bytes per sample:1=8 bit mono,2=8 bit stereo or 16bit mono, 4=16 bit stereo
34-35	Bits per sample
36-39	“data” (ASCII Character)
40-43	Length of data to follow
44-end	Data (samples)

A. *Audio file embedding*

In embeding audio message ,the contentes of header of wave audio file are retrived as separate fields.each field is converted to a bit array and then embedded bit by bit into the least significant bit.

B. *Audio file extracting*

The retriving of the audio file from the image is stright forward. The header fields are extracted from the secrret positions and stored into bit arrays.Each bit array is converted into data type according to table-1.

C. *Changing LSB-2Bits of the cover image using encrypted audio message*

To apply the proposed method, consider the secret audio data which will converted into bits which will hide in cover image. Steps are as follows:

First step: First audio data is converted from decimal to binary.

[Message] Dec to Bin → [1001101]

Second step: Now read Cover Image

→

182	182	180	180	180	179	176	174
181	182	181	180	179	178	175	174
178	178	178	176	173	172	169	171
174	175	175	172	166	163	164	164
172	173	173	171	167	164	163	163
175	175	175	173	171	168	166	166
177	176	175	174	173	172	169	168
173	172	171	170	171	…..	….	…..

Fig.5: The cover image

Third step: Cover image is converted from decimal to binary.

10110110	10110110	10110100	10110100	10110100	10110011	10110000	10101110
10110101	10110110	10110101	10110100	10110011	10110010	10101111	10101110
10110010	10110010	10110010	10110000	10101101	10101100	10101001	10101011
10101110	10101111	10101111	10110000	10101101	10101100	10101001	10101011
10101100	10101101	10101101	10101011	10100110	10100011	10100100	10100100
10101111	10101111	10101111	10101101	10101011	10100100	10100011	10100011
10110001	10110000	10101111	10101110	10101101	10101100	10101001	10100100
10101101	10101100	10101011	10101010	10101011	……………	…………….	…………..

Fourth step: Byte which are to be hidden are se bits.

Thus [11100100] is divided into 8 bits → [1 1 1 0 0 1 0 0]

Fifth step: Take first 8 byte of original data from the cover image .

10110110	10110110	10110100	10110100	10110100	10110011	10110000	10101110

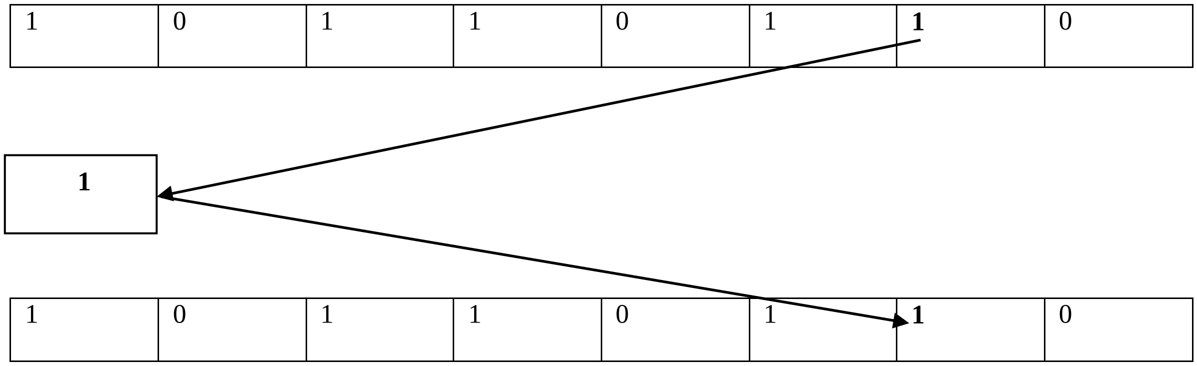
Sixth step: Replace LSB2 by one bit of the data to be hidden.
First byte of original data from the cover image is:

1	0	1	1	0	1	1	0

i) First bit of the data to be hidden is

1

ii) Replace the LSB2



1	0	1	1	0	1	**1**	0

1	0	1	1	0	1	**1**	0

iii) if the bit of the data to be hidden = = 1 and LSB2= =0 then

1-we change LSB1 of image to 0 after replacement.

1	0	0	1	0	0	1	**0**

2-we subtract 1 .

1	0	0	1	0	0	0	0

So we have No change in cover image

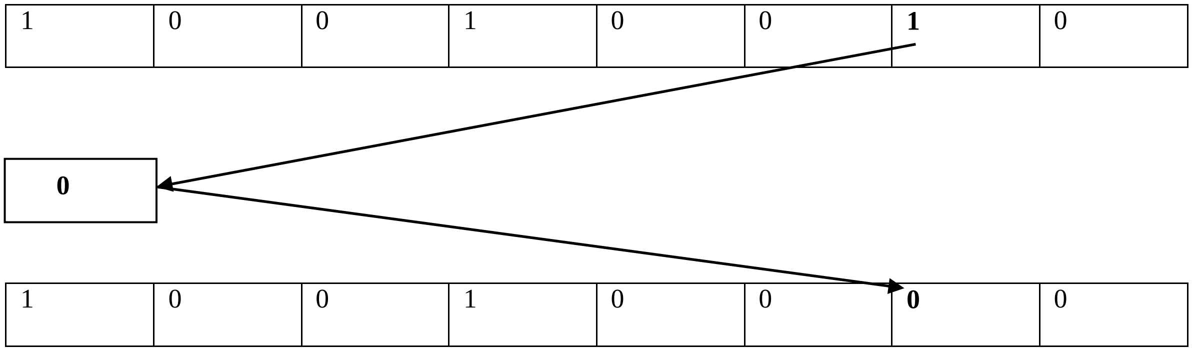
Second byte of original data from the cover image:

1	0	0	1	0	0	1	0

Second bit of the data to be hidden :

0

Replace the LSB2 :



1	0	0	1	0	0	**1**	0

1	0	0	1	0	0	**0**	0

iv) if the bit of the data to be hidden = = 0 and LSB2= =1 then

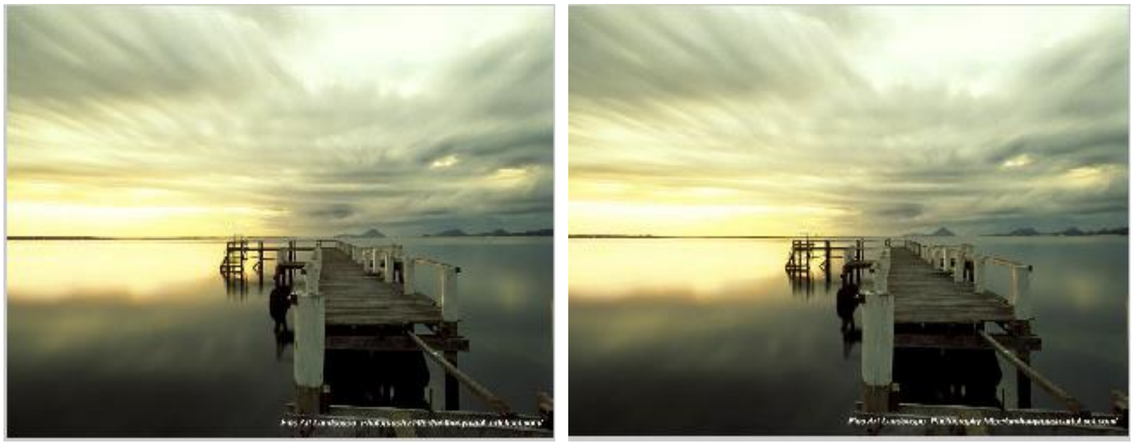
1-we change LSB1 of image to 1 after replacement.

1	0	0	1	0	0	1	**1**

2-we increase 1 .

1	0	0	1	0	0	1	0

- So we have No change in cover image
- Repeat the replace for all bytes of cover image.
- The cover image before and after applying the proposed steganography is shown in figure 6.



Cover image before steganography

Cover image after steganography

Fig.6: The cover image before and after steganography

III. IMPLEMENTATION AND RESULTS

We use 800 x 600 jpeg image as shown in figure 2.Audio data is of 11.9 KB of wav type. The proposed method has been implemented using MATLAB R-210.The least significant bits of the image pixels were encrypted using bit streams obtained from audio files. Audio message have been extracted from the stego image using the decryption technique.Stego image will look identical to the cover image. The extracted audio message are compared to original audio files and were identical with them.Difference between LSB-2 and LSB-1 is no change in cover image but LSB-2 is more robust and keep distortion is low.tabl2-2 shows comparison between LSB methods.

IV. CONCLUSION

This paper presents the possibility of hiding audio message inside the digital images with minimum distortion.this method is implemented for JPEG, BMP and PNG images.The embedding process creates a stego medium by replacing LSB-2 bits from hidden audio message. Experimental results shows that PSNR is greater than the conventional LSB replacement method.

V. REFERENCES

[1] "An effective implementation of LSB Steganography using DWT techniques", K.P.Uday kanth and D.Vidyasagar, June2014.

[2] "An Improved Inverted LSB Image Steganography" Nadeem Akhtar, Shahbaaz Khan, Pragati Johri,IEEE,2014.

[3]. International Journal of "Advanced Research in Computer Science and Software Engineering," Steganography Using Various Quantization Techniques",Tara Bansal,Ruuchika Lamba,Volume 3,Issue 7,July 2013.

[4] "A New Approach for LSB Based Image Steganography using Secret Key" S. M. Masud Karim, Md. Saifur Rahman,Md. Ismail Hossain,,IEEE ,December 2011.

[5] Research Journal ON "A Proposed Algorithm ForSteganography In Digital Image Based on Least Significant Bit "BY A. E.Mustafa, A.M.F.ElGamal, M.E.ElAlmi, Ahmed.BD,April,2011.

[6]"Image Steganography : Hiding short audio message within digital image",M. I. Khalil, Reactor physical department, nuclear research center, Atomic energy authority, cairo,Egypt,October,2011