INVERTED LSB IMAGE STEGANOGRAPHY AT RUN TIME WITH SECRETE KEY

[1]Rupali khot
Padmabhooshan Vasantdada Patil Institute of Technology, Pune, MS-India

ABSRACT: This paper consist of an enhancement in the LSB based steganography. In this paper, technique of hiding audio data into digital image is proposed and implemented. This technique uses bit inversion to get better the stegoimage quality. This paper also gives the possibility of embedding run time audio into digital image. To get better security level of hidden information secrete key is used. As a result, it is difficult to take out the hidden information as the decryption methods are known.

KEYWORDS: Steganography, Audio message, bit inversion, 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. Digital images are mostly used because of their frequency on the internet. If LSBs of some bits of the pixels are occur with a particular pattern then they are inverted. As less number of pixels is customized in assessment to plain LSB method. So PSNR of stegoimage is improved. For correct de-steganography, the bit patterns for which LSBs has inverted needs to be stored within the stegoimage somewhere. The proposed bit inversion method provides good development to LSB steganography.

Related Work:

Before applying proposed method ,LSB-1 method is applied. The following steps illustrate how this LSB-1 method is used to hide the secret data in cover image.

First step: Convert the data from decimal to binary. For example:

[message] Dec 2 Bin → [1000001]

Second step : Read Cover Image " a.jpeg " as shown in figure 1:

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

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	…..	….	…..

Figure 1: The cover image "a.jpeg"

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 :

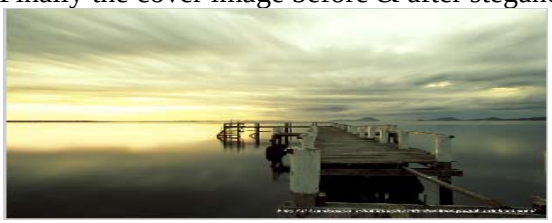
1	0	1	1	0	1	1	**0**

1

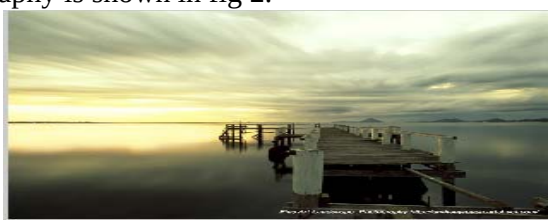
1	0	1	1	0	1	1	**1**

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

iv)Finally the cover image before & after steganography is shown in fig 2.



Cover image before steganography



Cover image after steganography

Figure 2: The cover image before and after steganography

II. PROPOSED METHOD

Bit Inversion:

In this method color image has been used as carrier and hidden message is audio data.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.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.

Steganography With secret Password:

The modern secure image steganography presents a challenging task of transferring the embedded information to the destination without being detected. So to provide security secret password is used. First fifty pixels are used to store the size of secret audio message, next fifty pixels are used to store the secret password and next onwards secret message is embedded. While on receviewing side secret message size and secret key is extracted. if password matches then only next embedded secret data is extracted.

Steganography with run time:

In run time steganography, run time audio and still image ,run time image and still audio and run time audio and run time image ,these three methods are implemented using bit inversion steganography. In run time audio ,voice is recorded , Where as for run time image ,video recording is done and one snap shot is taken as carrier 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)

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.

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.

BIT inversion:

To understand the method consider four bit data 1100 are to be hidden into 10101000 ,10101101,10001001 and 10101000 pixels of cover image.when LSB-1 repalcement steganography is applied then pixels becomes 10101001 ,10101101,10001000 and 10101000. Only one pixel that is fourth of

cover image have changed.Now see second and third LSB of cover image.Possible combinations for two bits are 00,01,10 and 11.Analyse the stego image for all these combinations and find changed and unchanged first LSB.If changed bits are moer then invert first LSB.In above example for combination 00 two pixels are changed so inverting that bit.so cover image pixels are 10101000,10101101,10001001 and 10101001. As only one pixel of stego image is different from cover image so PSNR ratio is improved.

For decryption it is necessary to store pattern for which corresponding LSB bits are inverted.from stego image to recover audio data analyse first,second and third LSB pattern of stego image. In that second and third are same but first LSB are changed.So for correct decryption ,receiver must have original image.

III. Implementation and results

We use 800 x 600 jpeg image as shown in figure 1.The proposed method has been implemented using MATLABR-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. Cover image before and after bit inversion are as shown in figure 3.

Cover image before steganography

Cover image after Bit Inversion steganography

Figure 3: The cover image before and after Bit Inversion steganography

Cover image

+

Audio data

Secrete data

+

vedant

Secrete key

=

Stego image

Figure 4: Stego image with secrete key

Secrete key is inserted into cover image along with secrete data to obtain stego image. It is as shown in figure 4. In run time steganography, run time audio is embedded into run time digital image with secrete key. Procedure is similar as shown in figure 4.

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. Bit inversion improves the stego image quality.PSNR ratio is larger for some images but may be small for some images. In our proposed method, we used a secret key to hide hidden information into cover image. This process provides a new aspect for image

steganography. It is very complicated to recover the hidden information for third party without knowing the secret key. Our proposed method provides better PSNR value where larger PSNR indicates superior quality of the image. Run time steganography gives the better PSNR ratio.

V. References

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

[2]. 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.

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

[4] 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.

[5]"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