Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 7, Issue. 7, July 2018, pg.73 – 82

A Secure and Randomize Approach for Data Carrying Methodology with Higher LSB Bit Replacement of Compressed/Uncompressed Video Channels

Ms. Manisha D. Rakhonde[1], Prof. A. A. Chinchamalatpure[2]
[1]PG Scholar, Department of Computer Science & Engineering, K.G.I.E.T., Darapur, & Sant Gadge Baba Amravati University, India
[2]Assistant Professor, Department of Computer Science & Engineering, K.G.I.E.T., Darapur, & Sant Gadge Baba Amravati University, India
[1] rakhondemanisha1668@gmail.com; [2] 1212.atul@gmail.com

Abstract — A new compressed video secure steganography (CVSS) rule is planned. Within the rule, embedding and detection operations square measure each dead entirely within the compressed domain, with no would like for the compression method. The new criteria using applied math visibility of contiguous frames is employed to regulate the embedding strategy and capability that will increase the safety of planned rule. Therefore, the collusion resistant properties square measure obtained. Video stegnoanalysis with closed-loop system feedback manner is style as a checker to search out obvious bugs. Experimental results showed this theme is applied on compressed video steganography with high security properties.

Keywords— Higher LSB, Data Hiding, Extraction, Mean Square Error, PSNR, AVI Video.

I. INTRODUCTION

This document is a template. An electronic copy can be downloaded from the conference website. For questions on paper guidelines, please contact the conference publications committee as indicated on the conference website. Information about final paper submission is available from the conference website.

Steganography is the transmission of a secret message hidden within an ordinary carrier without revealing its existence. The container (cover file) may be a digital still image, audio file, or video file. Once the secret message has been embedded, it may be transferred across insecure lines or posted in public places. Usually, the data rate of covert data transmission using steganography is low in order to keep the covert data imperceptible within the cover medium. This data rate is somewhat proportional to the volume of the cover medium. For this reason, digital video is a convenient choice for steganography. Nowadays, given the high degree of collaboration and cooperation in modern information systems such as emerging multimedia sensor networks, covert communications becomes a greater threat to forensic analysis than ever. It is imperative to investigate methods to detect and discourage covert communications such as steganography in multimedia networks that acquire highly correlated data.

This work will focus on the particular problem of the compressed video steganography. General speaking, digital video appears in two main distinct encoding formats: the uncompressed and the compressed. The most popular compressed format by far is motion compensated compressed video, specifically the widely accepted standard MPEGx. It achieves compression through the elimination of temporal, spatial and statistical redundancies and with this compression operation. The video bit-stream consists of variable length codes (VLC)

that represent various video segments. For video stream usually being offered in compressed form, steganography algorithms that are not applicable in compressed bit-stream would require complete or at least partial decompression [1-4]. This is an unnecessary burden best avoided. If the requirement of strict compressed domain steganography is to be met, the steganography needs to be embedded in the compressed domain .Nowadays, there are large amount of video watermarking algorithms been proposed. And some of them are applied for compressed video [5-9]. To be useful, a steganographic technique should not be easily detectable. If the existence of secret message can be detected with a probability higher than random guessing, the corresponding steganographic technique is considered to be invalid. Similar to cryptography steganography may suffer from the attack method (steganalysis). Much of the research work in the field of steganalysis has been carried out on images. One approach is based solely on the first order statistics and is applicable only to idempotent embedding another major stream is based on the concept of blind steganalysis, which is formed by blind classifiers. The classifier should be trained to learn the differences between cover and stego-image features at first.

II. LITERATURE REVIEW & RELATED WORK

For studying the concepts of video steganography and watermarking technique we have surveyed many latest papers. Biswajita Datta, Debnath Bhattacharyya, Samir Kumar Bandyopadhay and Kil-hwan Shin, "High Capacity Signature Hiding Technique in Higher Depth of LSB Layer" [21], It gaves basic idea of stegnography. In this papar writers proposed method. They says that ,As target data we consider a very important biometric authentication data –signature. In our proposed technique we consider that the signature image is basically a binary image and we try to hide this binary image within a 24 bit Color image. In our proposed technique we try to adjust the bits of the original string after embedding the data in the 5th LSB layer to reduce difference .Technique for bit adjustment to minimize the change in pixel value due to replacement of 5th LSB layer.

In our method first we have replaced the 5th bit (from the LSB) of each of the R, G and B component of the cover image with the pixel value of the target image. See the 5 position from LSB ,change that 5th bit if there is 1 than make it 0 and vise versa and reduce difference by flipping i.e. make all previous bit (from LSBside)1 of LSB and vise versa ,So that after hiding data on image not so much changes occurd in it. In below papars videos were used to Hide data.

Arup Kumar Bhaumik, Minkyu Choi, Rosslin J. Robles, and Maricel O. Balitanas [2], the main requirements of any data hiding system are security, capacity and robustness. It is very difficult to archive all these factors together because these are inversely proportional to each other. Authors have focuses on maximizing security and capacity factor of data hiding. The data hiding method uses high resolution digital video as a cover signal. It provides the ability to hide a significant quality of information making it different from typical data hiding mechanisms. They have used the large payloads like video in video and picture in video as a cover image.

Ahmed Ch. Shakir [1], the confidential communications over public networks can be done using digital media like text, images, audio and video on the internet. Simply hiding the contents of a message using cryptography was not adequate. Hiding of message should provide an additional layer of security. To provide the more security the author suggested the new procedures in steganography for hiding ciphered Information inside a digital colour bitmap image. He has used quadratic method depending on the locations concluded by the binary image, beside of public key cryptography. He had concluded that the conjunction between cryptography and steganography produce immune information.

Andreas Westfeld and Gritta Wolf [3], in this work author have described a steganographic system which embeds secret messages into a video stream. Normally the compression methods are used in video conferences for securing acceptable quality. But usually, compression methods are lossy because reconstructed image may not be identical with the original. There are some drawback of compression and data embedding method. Signal noise and irrelevance are common examples of data embedding. But compression methods try to remove signal noise and irrelevance. If signal is compressed more, then there are fewer possibilities of data embedding. The author have solved this problem, they have investigated a typical signal path for data embedding. In this algorithm security is established by indeterminism within the signal path.

Sherly A P and Amritha P P [14], in this paper author have proposed a new compressed video Steganographic scheme. In this scheme the data is hided in compressed domain. The novel embedding technique Triway Pixel Value Differencing (TPVD) is used to increase the capacity of the hidden secret information and for to providing an imperceptible stego-image for human vision. This algorithm can be applied on compressed videos without degradation in visual quality.

Saurabh Singh and Gaurav Agarwal [13] have presented a novel approach of hiding image in a video. In this approach, one LSB of each pixel is replaced by the one bit of secrete message. So it is very difficult to find that image is hidden in the video of 30 frames per second. The analysis is very difficult because each row of image pixels is hidden in multiple frames of the video. The intruder requires full video to unhide image. Authors have

described the LSB algorithm in this paper. The proposed algorithm is very useful in sending sensitive information securely.

S.Suma Christal Mary [12] have proposed new Real time Compressed video secure Steganography (CVSS) algorithm using video bit stream. In this, embedding and detection operations are both executed entirely in the compressed. The proposed algorithm increases the security because the statistical invisibility of contiguous frames is used to adjust the embedding strategy and capacity. At present we are hiding the data in video format, so in the future implementation of uncompressed formats may possible as well, so it may support MPEG4 format [15]. Multiple frames embedding are possible. Now we are embedding single frame at a time, but in future multiple frames embedding is also possible.

Yusuf Perwej, Firoj Parwej, Asif Perwej [16] in their work describes An Adaptive Watermarking Technique for the copyright of digital images and Digital Image Protection. Authors proposing edge detection from Gabor Filter method, using data hiding by the simple LSB substitution method. In the method a set of pixels that constitute a block jointly share the bits from the watermark .The values for the mean square error (MSE) and peak signal to noise ratio (PSNR) are measured. The results indicate the method introduces low noise and hence ensures lesser visible distortions.

Abdullah Bamatraf, Rosziati Ibrahim and Mohd.NajibMohd. Salleh[17] in their work authors describes A New Digital Watermarking Algorithm Using Combination of Least Significant Bit (LSB) and Inverse Bit. Author proposed a new LSB based digital watermarking scheme with the combination of LSB and inverse bit. The experimental result shows that the proposed algorithm maintains the quality of the watermarked image. When combining different positions of LSB such as the second LSB and the third LSB and fourth LSB and the combination between them. The proposed algorithm is also tested using Peak signal-to noise ratio (PSNR).

Varsha patil[22] place her read , she says that Image process techniques primarily focus upon Enhancing the standard of a picture or a group of pictures and to Derive the most info from them. Image fusion is such a method of manufacturing a superior quality image from a group of obtainable pictures. It's the method of mixing Relevant info from 2 or a lot of pictures into one Image whereby the ensuing image are going to be a lot of informative And complete than any of the input pictures. Lots of analysis Is being tired this field encompassing areas of pc Vision, automatic object detection, image process, parallel And distributed process, AI and remote sensing. During this paper, we've delineate the varied eleven fusion strategies (pyramid technique, moving ridge remodel etc.) and therefore the totally different quality assessment parameter (PSNR, MSE, Average Distinction, NAE etc.) wont to assess the standard of the consolidated Image. The varied application areas of image fusion are enclosed during this paper.

Xu Shuzheng , Zhang Peng , Wang Pengjun , Yang Huazhong [23]says A high capacity data hiding technique was developed for compressed digital audio. As perceptual audio coding has become the accepted technology for storage andtransmission of audio signals, compressed audio information hiding enables robust, imperceptible transmission of data within audio signals, thus allowing valuable information to be attached to the content, such as the song title, lyrics, composer's name, and artist or property rights related data. This paper describes simultaneous low bit rate encoding and information hiding for highly compressed audio signals. The information hiding is implemented in the quantization process of the audio content which improves robustness, signal quality, and security. The imperceptibility of the embedded data is ensured based on the masking property of the human auditory system (HAS). The robustness and security are evaluated by various attacking algorithms. Tests with an extended MPEG4 advanced audio coding (AAC) encoder confirm that the method is robust to the regular and singular group's method (RS) and sample pair analysis (SPA) attacks as well as other statistical steganalysis method attacks.

Sneha A. Deshmukh [24] proposed data is hidden in RGB component of Pixels with LSB 5 bit Replacement method. In this an Authentication of Secretly Encrypted Message Using Half-Tone Pixel Swapping from Carrier Stego Image. This paper used a secured LSB (5 bit) for image steganography has been presented. In this the proposed method not only has an acceptable image quality but also can provide a large embedded secrete data capacity.

Rasika Ghom [25] in this paper, Position Based Pixel Swapping Standard Method has been proposed, which includes the secret data that must be encrypted using key and hiding secret data in image using Data Hiding Algorithm. Higher group LSB method is applied on image to hide the secret data. Therefore, the proposed algorithm is a combination of encryption of any form of data or information first then hiding the any form of data or information into the cover image which provides double security. The results of the proposed algorithm is increase the data hiding capacity as compare to existing system and provide security to secret data. The result of the proposed system is analyzed and discussed using entropy, mean intensity, data hiding capacity and PSNR.

III. PROPOSED METHODOLOGY

Data Hiding

We hide secure data in image and Audio of compressed/uncompressed Video channel. In this section we see how data is hiding in this. Below Algorithm is nothing but a flowchart. Algorithm (Data Hiding in image and sound)

1. Select Video (Compressed / Uncompressed)
2. Extract Frames and sound.
3. Choose Carrier Media (Either Frame or Sound)
4. Convert Carrier Media to binary Format (Sampling of Data)
5. Input Secrete Data
6. Convert Secrete Data to Binary format (Sampling of Data)
7. Replace secrete Data bit with 6th LSB Position bit of carrier media and do flipping or other relevant bits.
8. Recreate carrier media after data hiding.

Data Hiding in Frame

In below Sixth bit LSB replacement Algorithm. By using this we hide data in frame.

```
if host sample a>0
        if bit 0 is to be embedded
        if a_{i-1} =0 then a_{i-1} a_{i-2} .... a_0 = 11...1
        if a_{i-1} =1 then a_{i-1} a_{i-2} .... a_0 = 00...0 and
            if a_{i+1}=0 then a_{i+1} = 1
              else if a_{i+2}=0 then a_{i+2}=1
              .....
              else if a_15 =0 then a_15 = 1
        else if bit 1 is to be embedded

          if a_{i-1} =1 then a_{i-1} a_{i-2} .... a_0 = 00...0
          if a_{i-1} =0 then a_{i-1} a_{i-2} .... a_0 = 11...1 and
              if a_{i+1}=1 then a_{i+1} = 0
                else if a_{i+2}=1 then a_{i+2}=0
                .....
                else if a_15 =1 then a_15 = 0
          else if bit 1 is to be embedded

  if host sample a<0
          if bit 0 is to be embedded
          if a_{i-1} =0 then  a_{i-1} a_{i-2} .... a_0 = 11...1
          if a_{i-1} =1 then  a_{i-1} a_{i-2} .... a_0 = 00...0 and
              if a_{i+1}=0 then a_{i+1} = 1
                else if a_{i+2}=0 then a_{i+2}=1
                .....
                else if a_15 =0 then a_15 = 1


              else if bit 1 is to be embedded
          if a_{i-1} =1 then a_{i-1} a_{i-2} .... a_0 = 00...0
          if a_{i-1} =0 then a_{i-1} a_{i-2} .... a_0 = 11...1 and
              if a_{i+1}=1 then a_{i+1} = 0
                else if a_{i+2}=1 then a_{i+2}=0
                .....
                else if a_15 =1 then a_15 = 0
          else if bit 1 is to be embedded
```

Data Hiding in Audio Wave file

For this we use Key generation Algorithm, Key Compression Algorithm and Key Replacement Algorithm mention below, We use following algorithms for watermarking in Audio.

a). Algorithm of Key Generation

1: Start
2: Read Sound
3: Read Master Component
4: convert Mpc to Binary
5: Input Bd
6: for i=1 to length(Bd)

for Bd(i)==Msc(j)
Add j to Key file
end
end
7: Save Key file
8: Stop
Where, Msc – Master sample component
Bd - Binary data

b). Algorithm of Key Compression

1: Start
2: Read Key file K
3:for i=10 to 2
Read cluster C(i,10)
Find C(i,10) in Key
if Frequency(C(i,10)>2
Replace C(i,10)with replace character in Key
End
End
4: Save Key file
5: Stop
Where, C – Compressed Key

c). Algorithm of Generation of Key Replacement table

1: Start
2: Read Compress Key Ck
3: load Key Replacement table
4: for i=length (Krt) to 1
Read S= Krt(i)
Replace Rc with Key from compress Key
End
5:Save uncompressed Key
6: Stop
Where, Ck – Compressed Key
Krt – Key replacement table
S – String
Rc – Replace component

Data Extraction

In this section we extract data which is hidden in frame and audio

a). Algorithm (Data Extraction for image)

1. Start
2. Input Video (Compressed / Uncompressed)
3. Extract Frames & Sound.
4. Choose Carrier Media (Either Frame or Sound)
5. Extract 6th Position LSB
6. Converts all collected bits into ASCII Format.
7. Stop

b). Algorithm (Data Extraction for Audio)

1: Start
2: Read Uncompressed Key Uck
3: Read Master Component Mc
4: for i= 1 to length (Uck)
Data=Data+Mc(Uck(i))
End
5: Convert Data to ASCII
6: Stop
Where, Uck – Uncompress key
Mc – Master sample componant

By using above Algorithms we Extract secure Data at destination in Image and Audio of Video.

IV. RESULT ANALYSIS

During this project we tend to hide secure knowledge in image and audio of video. Here we discover results of this activity action.

A. For Image

Histogram Result for original and resultant Image Here we find RGB Histogram of original and resultant Image

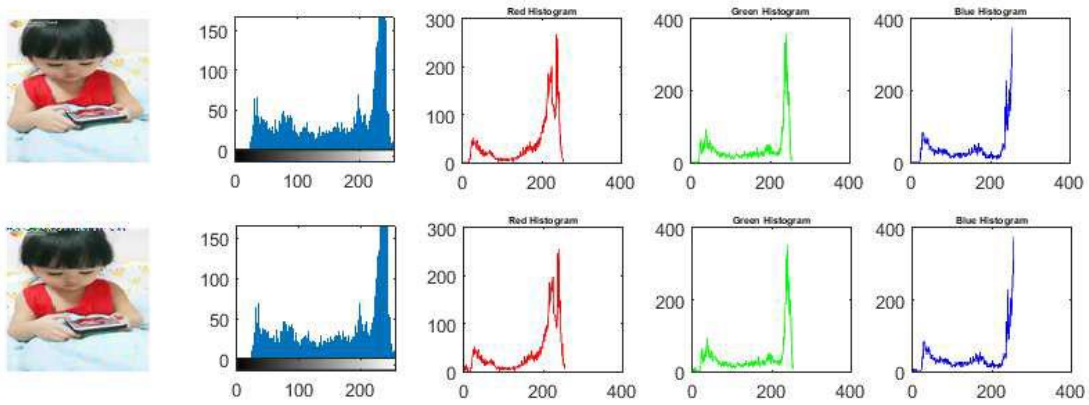


Fig. 1 Histogram Result for original and resultant Image

Parameters for Image Analysis

By comparing Original and Resultant Image we calculate MSE, PSNR, NCC, AD,SC, MD, and NAF on which we define Image Quality [22].

Table 1 Comparison between Existing System and Proposed System

 Original Image	MSE	95.88
	PSNR	28.31
	NCC	0.99
	AD	-0.20
 Resultant Image	SC	0.99
	MD	212
	NAF	0.0061

Data hiding capacity of an Image

We hide data in image so there is need to find hiding capacity of image. We hide one bit in each RGB component of pixel [24].

Table 2 Data Hiding Capacity in Percentage

No. of Bits	hiding capacity in%
1 bit	12.50
2 bit	25
3 bit	37.50
4 bit	50
5 bit	62.50
6 bit	75

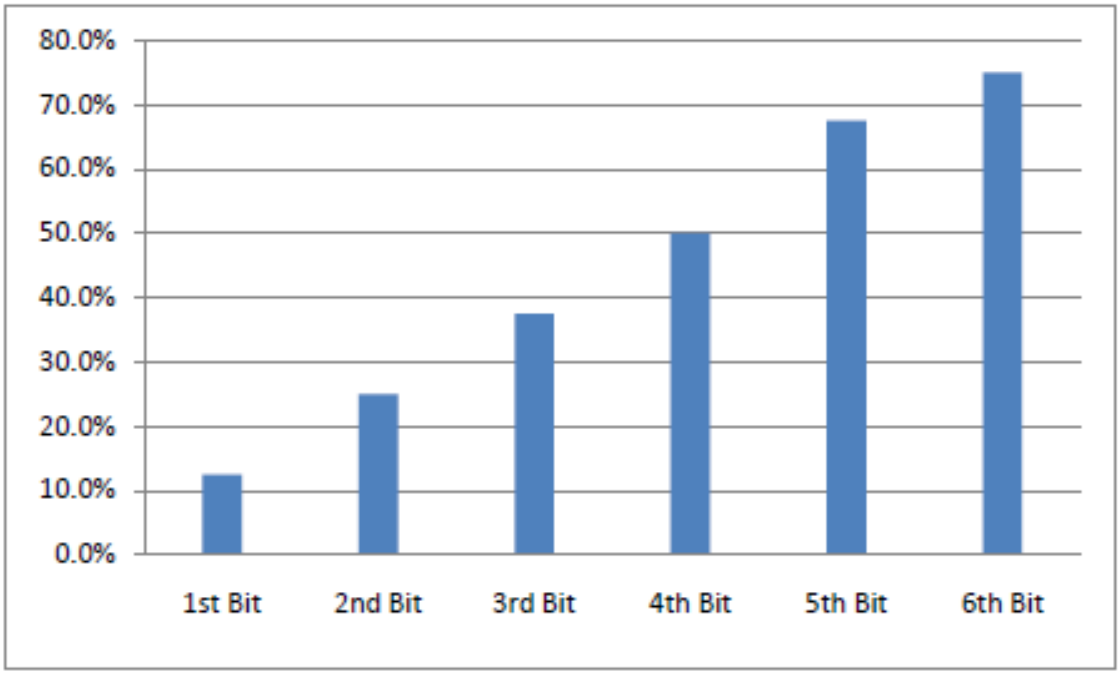


Fig. 2 Graph shows Data Hiding Capacity in Percentage

B. For Audio

Hiding capacity of audio

The aim of this project is hide data in video, so there is need to study about hiding capacity of carrier. The hiding capacity of audio is given below.

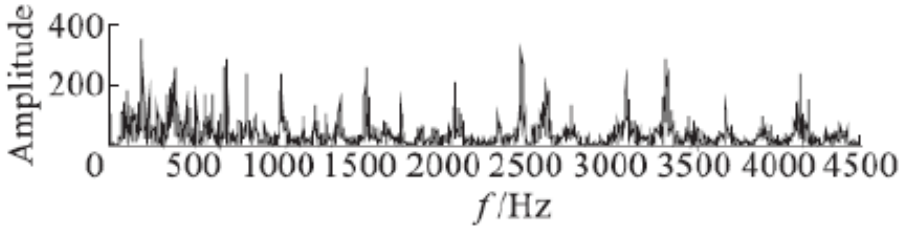
The hiding capacity of audio is greater than Size of audio sample

i.e. ADH > Size (As)

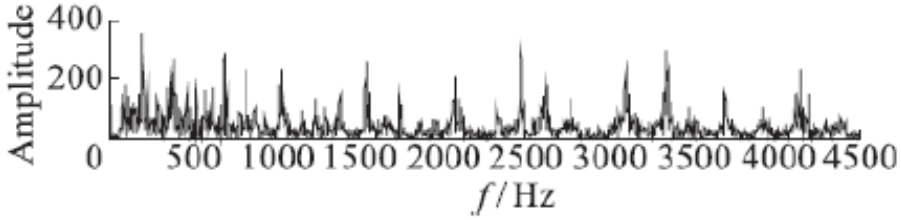
Time and Frequency of existing system and proposed system

Time and Frequency of existing system

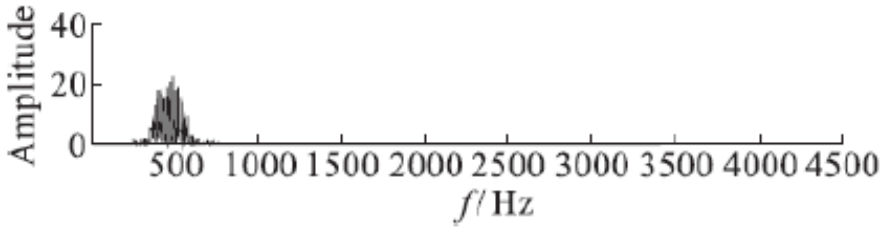
Frequency depend upon time, both the time and frequency analyses do not show any distinguishing differences between the Original Audio and the Resultant Audio with the hidden data[23].see figure a), b) and c)



a) **Original Audio Spectrum**



b) **Resultant Audio Spectrum**



c) **Difference from a) and b)**

Time and Frequency of proposed system

Here we find Spectrum for Original sound and resultant sound by using spectrum analyser. There is no difference between Original sound and resultant sound.

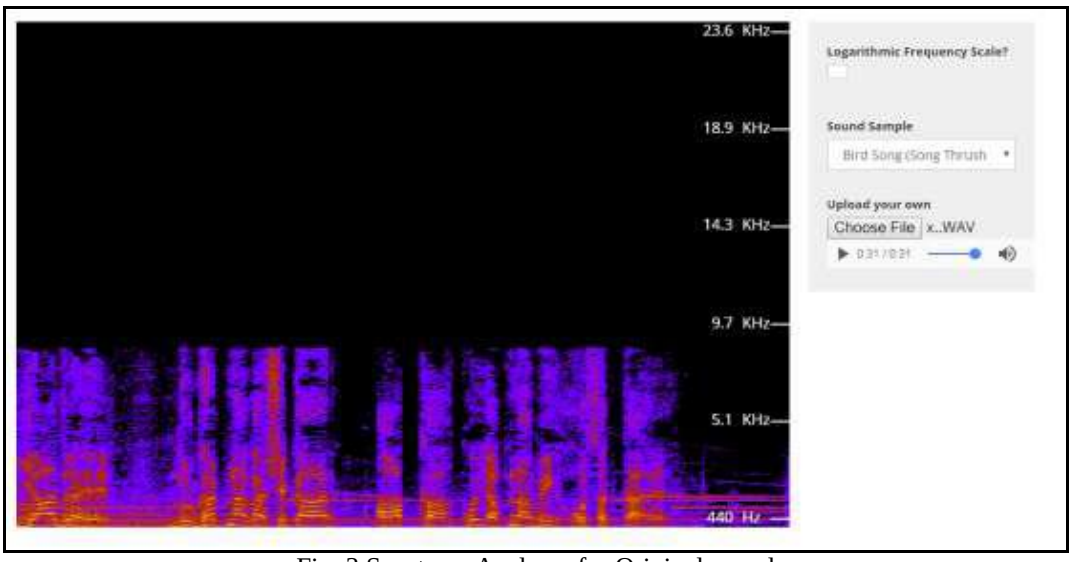


Fig. 3 Spectrum Analyser for Original sound

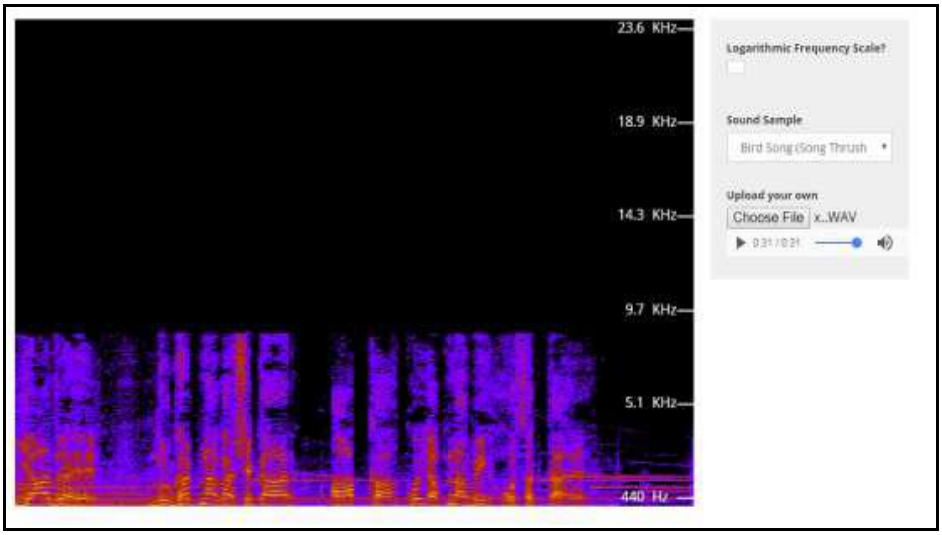


Fig 4. Spectrum analyser for resultant sound

Frequency of Original and Resultant is same and Time required for Completion of Audio of Original Audio and Resultant Audio is same. At last we Conclude that our system is good than Previous.

V. CONCLUSION

Information concealment in Image and Audio of Compressed/Uncompressed Video is difficult task in information Security domain. This projected system provides the simplest result than the previous techniques and work.

REFERENCES

[1] Ahmed Ch. Shakir," Steno Encrypted Message in Any Language for Network Communication Using Quadratic Method", Journal of Computer Science 6 (3): 320-322, 2010 ISSN 1549-3636 © 2010 Science Publications.

[2] Arup Kumar Bhaumik, Minkyu Choi, Rosslin J. Robles, and Maricel O. Balitanas," Data Hiding in Video", International Journal of Database Theory and Application Vol. 2, No. 2, June 2009.

[3] Andreas Westfeld and Gritta Wolf," Steganography in a Video Conferencing System", Information Hiding 1998, LNCS 1525, pp. 32-47, 1998. Springer-Verlag Berlin Heidelberg 1998.

[4] Cheng Cheok Yan, "Introduction on Text Compression Using Lempel, Zip, Welch (LZW) method".

[5] D. P. Gaikwad and Dr. S.J. Wagh, "Color Image Restoration for Effective Steganography", i-manager's Journal on Software Engineering, Vol. 4 l No. 3 l January - March 2010 65, pp.65-71.

[6] D.P. Gaikwad and Dr. S.J. Wagh, "Image Restoration Based LSB Steganography for Color Image", AISA-PACIFIC Regional Conference in ICTM-2010 on Innovations and Technology Management at Mumbai.

[7] Richard E. Woods & Rafael C. Gonzalez "Digital Image Processing" Book.

[8] F5 algorithm implementation: 2009, Fridrich, J.R.Du, M. Long: Steganalysis in Color Images, Binghamton, 2007.

[9] Neil F. Johnson and SushilJajodia, "Exploring Steganography: Seeing the Unseen", George Mason University.

[10] Steganography on new generation of mobile phones with image and video processing abilities, as appeared Computational Cybernetics and Technical Informatics (ICCCCONTI), 2010 International Joint Conference on 27-29 May 2010 in Timisoara, Romania ISBN: 978-1-4244- 7432-5.

[11] Saurabh Singh and Gaurav Agarwal, "Hiding image to video: A new approach of LSB replacement", International Journal of Engineering Science and Technology Vol. 2(12), 2010, 6999-7003.

[12] S. Suma Christal Mary, "Improved Protection In Video Steganopgraphy Used Compressed Video Bitstream ," International Journal on Computer Science and Engineering Vol. 02, No. 03, 2010, 764-766, ISSN: 0975-3397.

[13] Y. J. Dai., L. H. Zhang and Y. X. Yang.: A New Method of MPEG Video Steganographying Technology .International Conference on Communication Technology Proceedings (ICCT), 2003.

[14] D.C. Wu and W.H. Tsai: A steganographic method for images by pixel-value differencing, Pattern Recognition Letters, Vol. 24, pp. 1613–1626, 2003.
[15] F Hartung., B. Girod.: Steganoing of uncompressed and compressed video, Signal Processing, Special Issue on Copyright Protection and Access Control for Multimedia Services, 1998, 66 (3): 283-301.
[16] Sherly A P and Amritha P P,"A Compressed Video Steganography using TPVD", International Journal of Database Management Systems(IJDMS) Vol.2, No.3, August 2010 DOI: 10.5121/ijdms.2010.2307-67.
[17] Abdullah Bamatraf, Rosziati Ibrahim and Mohd. NajibMohd. Salleh in their work authors describes A New Digital Watermarking Algorithm Using Combination of Least Significant Bit (LSB) and Inverse Bit.
[18] G. Paul, I. Davidson, I. Mukherjee and S. S. Ravi, Keyless Steganography in Spatial Domain using Energetic Pixels, In Proceedings of the 8th International Conference on Information Systems Security (ICISS), vol.7671, LNCS, Springer (2012), 134 - 148.
[19] Deepa put paper A steganalysis module, operated in a closed-loop manner to enhance the anti-steganalysis capability of the stegovideo with data embedded.
[20] Yusuf Perwej, Firoj Parwej, Asif Perwej in their work describes An Adaptive Watermarking Technique for the copyright of digital images and Digital Image Protection.
[21] Biswajita Datta, Debnath Bhattacharyya, Samir Kumar Bandyopadhay and Kil-hwan Shin, "High Capacity Signature Hiding Technique in Higher Depth of LSB Layer", Contemporary Engineering Sciences, Vol.7, 2014, no. 15, 731 – 736.
[22] Varsha patil, "Image fusion methods and quality assessment parameters" Asian journal of engineering and applied technology ISSN 2249-068x vol. 2 no. 1, 2013, pp.40-46.
[23] Xu Shuzheng , Zhang Peng , Wang Pengjun , Yang Huazhong , "Performance Analysis Of Data Hiding In MPEG-4 AAC Audio" Tsinghua Science And Technology ISSNnlL1007-021,L07/2, pp55-61,Volume 14, Number 1, February 2009.
[24] Sneha A. Deshmukh, "An Authentication of Secretely Encrypted Message Using Half-Tone Pixel Swapping From Carrier Stego Image", International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 6 (3) , pp. 2409-2014, 2015.
[25] Rasika Ghom "Data Hiding Security Approached with Position Based Pixel Swapping Standard Method", IJCSMC, Vol. 5, Issue. 5, May 2016

