

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320-088X



IJCSMC, Vol. 2, Issue. 8, August 2013, pg.54 – 62

RESEARCH ARTICLE

Steganographic Method for Data Hiding in Audio Signals with LSB & DCT

Linu Babu¹, Jais John S², Parameshchhari B D³, Muruganantham C⁴, H S Divakaramurthy⁵

1M.Tech Student, Department of ECE, Nehru College of Engineering and Research Centre, Pampady, Thiruvilawamala, Kerala, India

2Assistant Professor, Department of ECE, Nehru College of Engineering and Research Centre, Pampady, Thiruvilawamala, Kerala, India

3Associate Professor, Department of ECE, Nehru College of Engineering and Research Centre, Pampady, Thiruvilawamala, Kerala, India

(Research Scholar, Dept. of ECE, Jain University, Bangalore, Karnataka, India)

4Assistant Professor, Department of ECE, Nehru College of Engineering and Research Centre, Pampady, Thiruvilawamala, Kerala, India

5Dean and HOD, Department of ECE, Nehru College of Engineering and Research Centre, Pampady, Thiruvilawamala, Kerala, India

¹linubabup@gmail.com

³parameshbkit@gmail.com

Abstract-Data hiding, a form of steganography, is one of the emerging techniques that embeds secret data into a digital media and thus ensures secured data transfer. In this paper, the steganographic method used, is based on audio steganography which is concerned with embedding secret data in an audio file. The basic idea of proposed method is that the host signal (the sound wave cover media) undergoes preprocessing, and then the results takes the shape of an image in which the data can be securely hidden in the image layers. The secret data is then hidden in a preprocessed sound wave using a traditional steganographic technique. The least significant-bit (LSB) based technique are very popular for steganography in spatial domain. The simplest LSB technique simply replaces the LSB in the cover image with the bits from secret information. Further advanced techniques use some criteria to identify the pixels in which LSB(s) can be replaced with the bits of secret information. In DCT based technique insertion of secret information in carrier depends on the DCT coefficients. Any DCT coefficient value above proper threshold is a potential place for insertion of secret information. The proposed methods offers high quality of steganography process in terms of Peak Signal-to-Noise Ratio (PSNR). Only minor changes in the contents of the audio file occur, which are indiscernible to human ears. In addition, several attacks on the sound wave were performed; the results showed that the hidden secret data can be retrieved with minimal distortion. An implementation of both these methods and their performance analysis has been done in this paper.

Keywords: steganography; data hiding; attacks; PSNR; LSB; DCT

I. INTRODUCTION

Security of information is one of the most important factors of information technology and communication. Security of information often lies in the secrecy of its existence and/or the secrecy of how to decode it. Mainly there are two ways of concealing information: cryptography and steganography. Cryptography's main aspect is that the information is somehow distorted, scrambled by the sender using normally an encryption key also known only by the intended receiver who decrypts the message. The problem with cryptography is that a user intercepting the message, although he cannot decrypt it, he might detect that there is encrypted, secret information.

Steganography is an art of embedding information in a cover image without causing statistically significant variations to the cover image. Audio steganography is one of the popular data hiding techniques that embeds secret data in audio signals. On the other hand in steganography The secret data is hidden in a way that unauthorized persons are not aware of the existence of the embedded data and without altering the quality of the cover audio. In addition, the security of classical steganography system relies on secrecy of the data encoding system. Once the encoding system is known, the steganography system is defeated. Data hiding in audio signals has numerous applications such as protection of copyrighted audio signals, covert communication, hiding data that may influence the security and safety of governments and personnel. An effective audio steganography should have the following characteristics for successful embedding and extracting data: perceptual transparency (i.e. the cover and the stego objects must be imperceptible), high data rate and robustness of the embedded data.

In this paper, we proposed a data hiding method where the host signal (the sound wave cover media) undergoes preprocessing and mapping, then the results takes the shape of a colored image in which the data can be securely hidden in the image layers. A number of ways exist to hide information in audio signals. We have concentrated on some techniques and methods which are divided into two types: Spatial Domain in LSB coding and Frequency Domain in DCT technique. That is The secret data is then embedded in the colored image using the LSB coding and DCT steganographic technique. The colored image, in which the secret data embedded, will be converted back to sound wave before transmission.

The paper is organized as follows: Section 2 discusses the brief overview of audio steganographic method Section 3 describes the proposed method. Section 4 shows experimental setup and result. Finally in Section 5 the conclusion and future scope is described.

II. BACKGROUND OF AUDIO STEGANOGRAPHY

A lot of Research has been carried out on Steganography which concentrate on hiding secret data in audio because it is important to know how much data can be concealed without image distortion. Their description is as follows:

Kriti and Pradeep proposed a scheme where a secret gray scale image file is to be embedded in an audio cover file. In their scheme, a comparison is made between secret image bits and the audio samples (1st MSB -Most Significant Bit- to the 7th MSB positions). If a match is found the three LSB of the audio sample is replaced with the binary equivalent of the MSB position. As a result, the image is hidden without affecting the size of the cover audio file. The SNR is calculated, which shows less noise in the audio file compared with other novel techniques. Debnath, Poulami and Tai-hoon used a method called the zigzag LSB method where the binary value of the of the secret message is inserted into the last bit of the audio in a zigzag fashion. On the average, only half of the bits are altered in the audio file. So there are no noticeable sound variations of the audio file before and after hiding the data. Ajay also presented a new 4th bit rate LSB audio steganography method where the message is embedded in 4th LSB layer. This gives an increased robustness against noise addition.

Spatial-based schemes embed the data into the pixels of the cover image directly, While transform-based schemes embed the data into the cover image by modifying the Coefficients in a transform domain, such as the Discrete-Cosine Transform (DCT). In this paper, we will focus upon data hiding in the DCT domain as well as spatial domain. Ken Cabeln and Peter Gent have discussed the mathematical equations of Discrete Cosine Transform (DCT) and its uses in image compression. Andrew B. Watson has discussed Discrete Cosine Transform (DCT) technique for converting a signal into elementary frequency component. He developed simple function to compute DCT and show how it is used for image compression. Hao-tian Wu, Ji-wu Huang in steganographic algorithm is proposed for JPEG Image by modifying the block DCT coefficients. Firstly, an embedding algorithm called LSB+ matching is generated to approximately preserve the marginal distribution of DC coefficients. We further divide the DCT coefficients into four frequency bands, including the direct current (DC), low frequency, middle-frequency, and high-frequency. Via matrix encoding, low data hiding rate and high embedding efficiency are achieved in high-frequency band, while the hiding rate is increased in the middle-frequency and DC bands, and highest in the low-frequency band. In addition, a coefficient selection strategy is employed to make the hidden message less detectable. The proposed work is mainly focused on steganographic data hiding method in audio signal and

evaluate the performance analysis for the same.

III. PROPOSED METHOD

The human auditory system is sensitive to small amplitude variations in audio files, we developed a hiding technique where it is possible to hide secret data in an audio file and ends up with a sound that is indistinguishable from the original.

Sound samples are stored as 8, 16 or 24 bit values. In order to hide secret data, we used 24 bit CD quality wave audio file at 48 kHz as a cover file to hide a secret gray scale image. Our technique can be applied on samples of 8 or 16 values by scaling the sample values into 24 bit.

In the proposed technique, the sound is divided into samples where each sample is 24 bit, 8 bits are to be hidden in each sample by distributing the bit pattern that corresponds to the secret gray scale image across the LSBs of the preprocessed sound samples (i.e. the preprocessed sound waves take the shape of a RGB colored image). So the embedding capacity is 8 bits per audio sample which results in large embedding capacity. Additionally, hiding the secret bit pattern by distributing it in the layers of the colored image, add more secrecy to the hidden data.

Spatial domain technique Spatial steganography mainly includes LSB(Least Significant Bit) steganography Least significant bit (LSB) insertion is a common, simple approach to embedding information in a cover image. The least significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message.

Stage 1: Scaling the wave samples and mapping it into a colored cover image

1. Read the audio data samples in the cover audio file.
2. The values of the audio data samples will be in the range $[+8,388,607, -8,388,608]$
3. To make the technique more secure and to decrease the possibility of distortion in the retrieved secret data select a subset of the data samples that are enough to embed the secret data either by taking a set of sequential samples of numbers equivalent to the number of pixels in the secret data, or taking the odd or even samples of numbers equivalent to the number of pixels in the secret data.
4. Scale the selected sample values to values from 0 to $16777215 (2^{24}-1)$ using eqs (1) and (2) :

$$\text{new_samples} = \text{sample_values} + \text{abs}(\min(\text{sample_values})). \quad (1)$$

$$\text{Scaled_Samples} = \text{round}(\text{New_samples} . * ((2^{24}-1) / \max(\text{New_samples}))). \quad (2)$$

Due to the scaling process, the scaled values are similar to the image values (each value is stored in 24 bits)

5. Map and reshape these values to produce a colored cover image (the colored image is consisted of three layers Red, Green and Blue). This image will be used to hide the secret data.

The mapping process can be achieved by using the following two ways:

- Color mapping: Map each scaled value to a specific color (Red, Green or Blue) using a color table.
- Split each scaled value (24 bits) into three groups of 8 bits (i.e. the RGB color components)

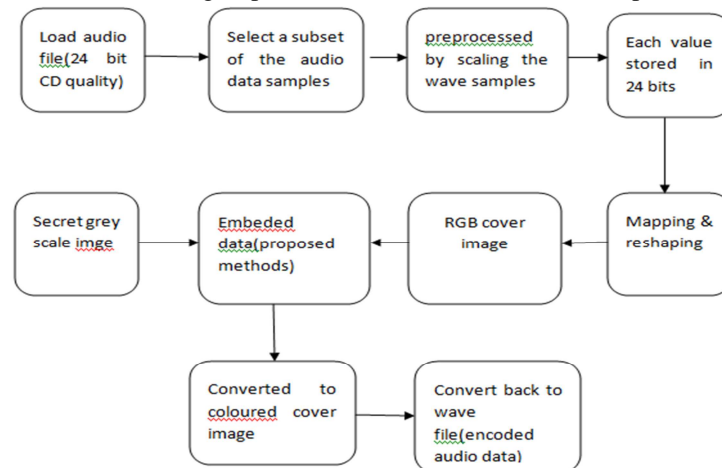


Figure3.1: General block diagram of proposed method

Stage 2: Embedding the secret gray image in the colored cover image:

a) LSB technique

1. Using the LSB technique, embed each pixel (8 bits) of the secret gray image in the corresponding pixel of the colored cover image (24 bits) by doing the following:

- a) Divide the pixel in the secret gray image into 2 groups of 3 bits and 1 group of 2 bits.
- b) Embed the resulted groups of bits in the corresponding pixel in the colored cover image (embed the first group of 3 bits in the Red layer, the second group of 3 bits in the Green layer and the last group of 2 bits in the Blue layer)

Repeat the steps a and b until you embed all the pixels of the secret image in the colored cover image.

b) LSB extracting technique

The data extraction at the receiver's side follows the same logic as the embedding technique. The first step is to read the wave data samples in the cover audio file then scale the sample values to values from 0 to 16777215 ($2^{24} - 1$) as discussed before. After that, map and reshape these values to produce a colored cover image, finally, retrieve the secret image by:

- a) Each pixel in the secret image will be constructed by retrieving the first three bits from the Red Layer to be the least three bits in the secret image pixel, the first three bits from the Green Layer to be the fourth, fifth and sixth bits in the secret image pixel and the first two bits from the Blue Layer to be the seventh and eighth bits in the secret image pixel.
- b) Retrieve the image size from the cover image to reconstruct the secret image.

c) DCT based steganography

The audio data samples are converted to gray image is same as that of lsb technique. data embedded in the cover image will be different from lsb.

DCT coefficients are used for compression technique. It separates the image into parts of differing importance. It transforms a signal or image from the spatial domain to the frequency domain. It can separate the image into high, middle and low frequency components.

In dct domain technique first Read audio data select a portion of wave samples and convert it into corresponding RGB cover image by proper scaling mapping & reshaping. Read secret message then convert it in binary. The cover image is broken into 8×8 block of pixels. Working from left to right, top to bottom subtract 128 in each block of pixels. DCT is applied to each block. Each block is compressed through quantization table. Then Calculate LSB of each DC coefficient and replace with each bit of secret message. hence obtained the stego image. The image of size $M \times N$ is divided into 8×8 blocks and two dimensional (2-D) DCT is performed on each block. The DCT is calculated using equation 1:

$$F(u,v) = \frac{1}{4} C(u)C(v) \sum_{x=0}^7 \sum_{y=0}^7 f(x,y) \cos \left[\frac{\pi(2x+1)u}{16} \right] \cos \left[\frac{\pi(2y+1)v}{16} \right] \quad (1)$$

$$\text{where } C(k) = \begin{cases} 1/\sqrt{2} & \text{for } k = 0 \\ 1 & \text{otherwise} \end{cases}$$

for $x=0, \dots, 7$ and $y=0, \dots, 7$

Here, $C(u,v)$ is the DCT coefficient in row u and column v of the DCT matrix. Signal energy lies at low frequency in image; it appears in the upper left corner of the DCT and high frequency coefficients are lower right positions. Compression can be achieved since the lower right values represent higher frequencies, and generally small enough to be neglected with little visible distortion

d) DCT extracting technique

The extracting method for dct is the reversal of the hiding method. first read the stego wave file, then by preprocessed scaling convert the audio file into stego cover image of RGB color. This Stego image is broken into 8×8 block of pixels. Working from left to right, top to bottom subtract 128 in each block of pixels. DCT is applied to each block. Each block is compressed through quantization table. Calculate LSB of each DC coefficient. : Retrieve and convert each 8 bit into character




Stage 3: Converting the colored cover image back into sound wave

Convert the colored cover image back to a wave file by rescaling the values to be in the range $[+8,388,607, -8,388,608]$ and sending the cover wave to the receiver side.

IV. EXPERIMENTAL SETUP AND RESULT

The proposed perceptual video encryption is implemented with MATLAB 7.10.0(R2010a) using windows 7 operating system. The experiments are carried out on an image(lena.jpeg)hiding in an audio signal. Performance evaluation factors like PSNR and MSE values for encoded audio for proposed methodwith and without AWGN and comparison method, is tabularized in table4.1.

Table 4.1: simulation results for LSB & DCT Method

	LSB METHOD			DCT METHOD			SIZE OF THE COVER IMAGE
	PSNR(without AWGN)	PSNR(with AWGN)	MSE	PSNR(without AWGN)	PSNR with AWGN)	MSE	
	49.032	48.13	0.4078	42.764	40.312	5.56	256*256
	51.08	50.25	0.4124	41.231	39.078	7.4678	256*256
	53.541	51.325	0.3078	39.986	37.641	8.85	256*256

The comparison table depicting the differences between both the methods is given below in Table 4.2. Here invisibility, robustness against attacks, payload capacity,PSNR, MSE are compared.

Features	LSB	DCT
Invisibility	Low	High
Payload capacity	High	Medium
Robustness against statistical attacks	Low	High
Robustness against image manipulation	Low	Medium
Independent of file format	Low	Medium
PSNR	High	Medium
MSE	Less	Medium

TABLE 4.2: Parameters analysis of both steganographic method

Two of the output results on LSB technique and DCT technique are shown in figure2 and 3 respectively.

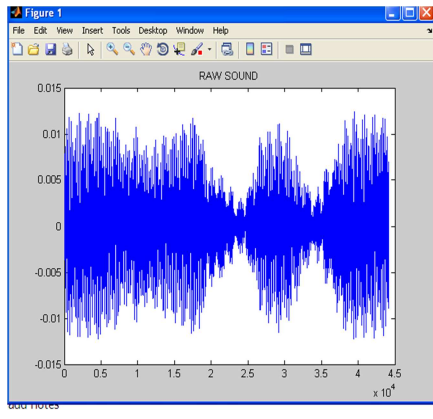


Fig 2 (a)

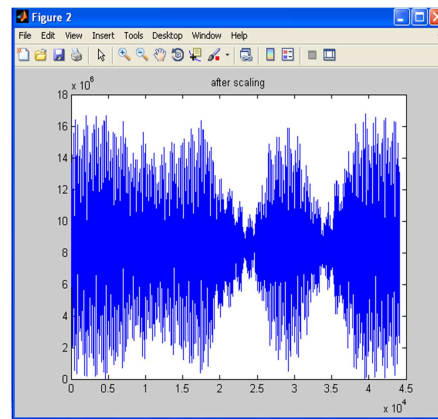


Fig 2 (b)

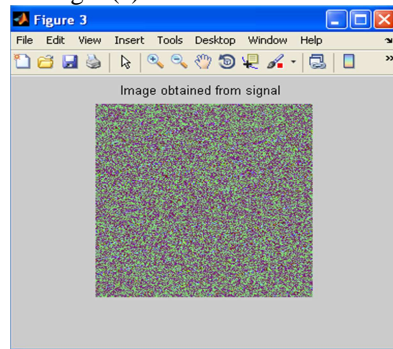


Fig 2 (c)

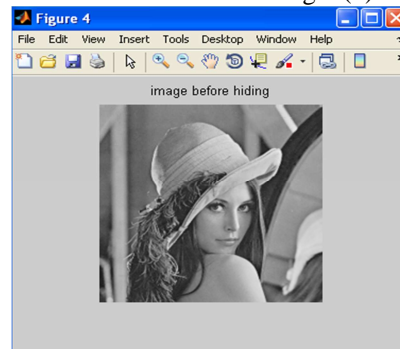


Fig 2 (d)

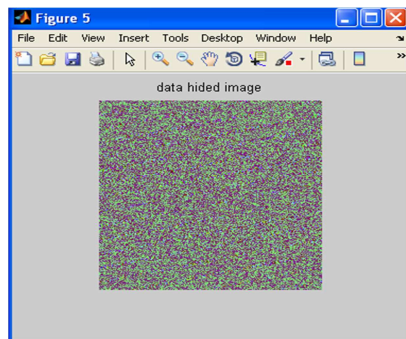


Fig 2 (e)

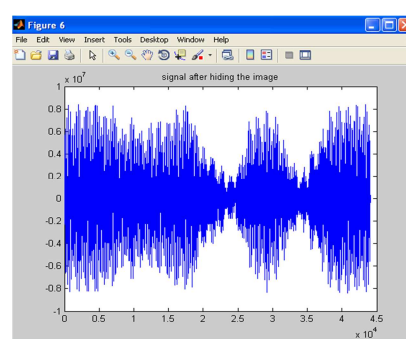


Fig 2 (f)

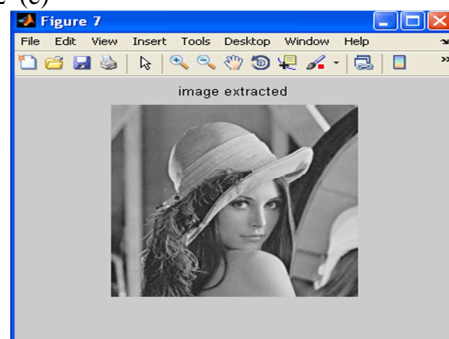


Fig 2 (g)

Fig 2(a): input audio , Fig 2(b): signal after scalling, Fig 2(c): image RGB from the signal, Fig 2(d): selecting image for hiding, Fig 2(e): data hided with cover image using LSB method , Fig 2(f): signal after hiding image, Fig 2(g): image extracted from audio signal.

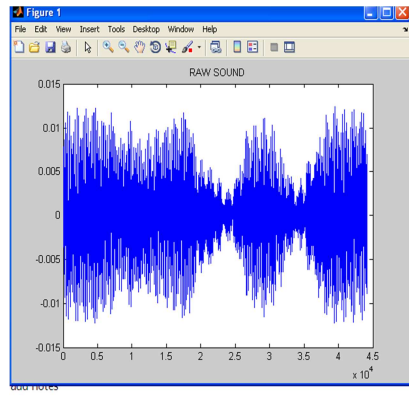


Fig 3 (a)

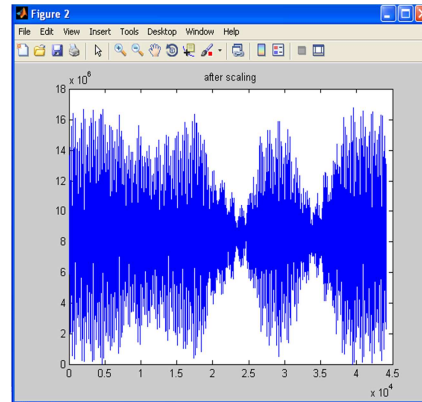


Fig 3 (b)

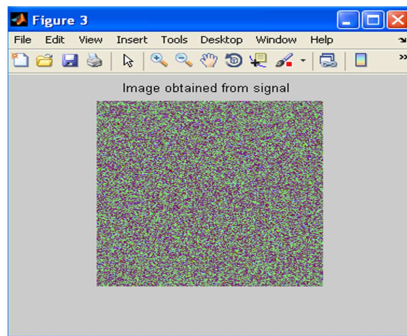


Fig 3(c)

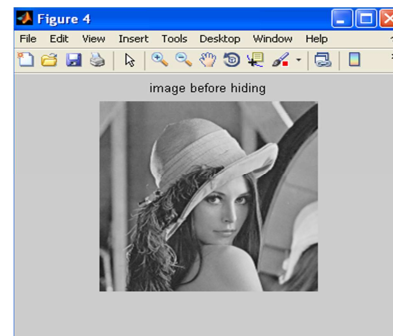


Fig 3 (d)

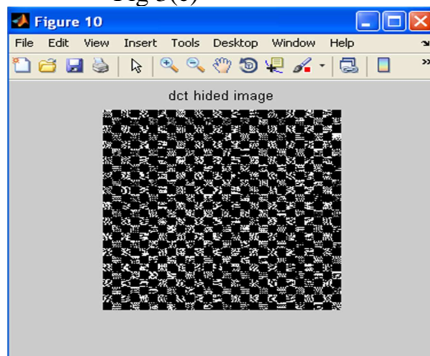


Fig 3 (e)

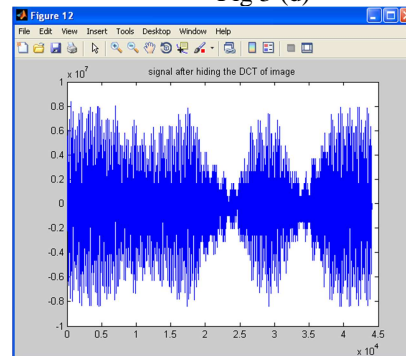


Fig 3 (f)

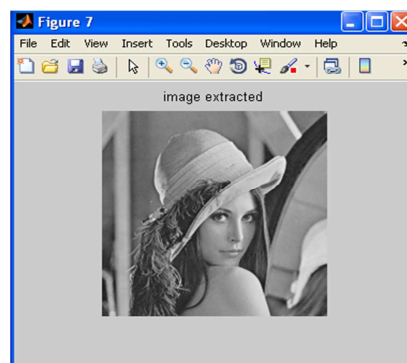


Fig 3 (g)

Fig 3(a): input audio , Fig 3(b): signal after scalling, Fig 3(c): image RGB from the signal, Fig 3(d): selecting image for hiding, Fig 3(e): data hided with cover image using DCT method , Fig 3(f): signal after hiding image, Fig 3(g): image extracted from audio signal.

V. CONCLUSION

Data hiding in audio signals using LSB &DCT method is implemented using MATLAB successfully. Older methods for data hiding are discussed. LSB based steganography embed the text message in LSB of cover image. DCT based steganography embed the text message in LSB of DC coefficients. This paper implements LSB based steganography, DCT based steganography and computes PSNR ratio. PSNR is the peak signal to noise ratio, in decibels, between two images. This ratio is used as a quality measurement between two images. If PSNR ratio is high then images are better of quality. Comparison of LSB based and DCT based stego images using PSNR ratio shows that PSNR ratio of LSB based steganography scheme is high as compared to DCT based steganography scheme for all types of images- (Grayscale as well as Color). DCT based steganography scheme works perfectly with minimal distortion of the image quality as compared to LSB based steganography scheme. Even though the amount of secret data that can be hidden using DCT technique is very small as compared to LSB based steganography scheme still, DCT based steganography scheme is recommended because of the minimum distortion of image quality. As future work, data hiding in audio signal may be extended to other steganographic technique like wavelet transformation for more secure data transmission and the noise attack may be extended to some of salt & pepper noise instead of AWGN.

ACKNOWLEDGEMENT

The work described in this paper is supported by Adv.Dr.P.Krishnadas, Managing Trustee and Dr.P Krishnakumar, CEO & Secretary, Nehru Group of Institutions, Tamil Nadu, Kerala-India. Authors are grateful to Prof. Dr. P.N. Ramachandran, Principal and Dr.N K Shakthivel, Vice Principal, Nehru College of Engineering and Research Centre (NCERC), Pampady, Thiruvilawamala, Kerala, India, for providing us the opportunity to undertake this project.

REFERENCES

- [1] Dalal N. Hmood, Khamael A. Khudhiar and Mohammad S. Altaei (2012). **A New Steganographic Method for Embedded Image In Audio File**. *International Journal of Computer Science and Security(IJCSS)* 6(2): pp.135-141.
- [2] Samir K. Bandyopadhyay and Biswajita Datta (2011). **Higher LSB Layer Based Audio Steganography Technique**. *International Journal of Electronics and Communication Technology (IJECT)* 2(4): pp.129-135.
- [3] Kirti Saroha , Pradeep Kumar Singh (2012). **A Variant of LSB Steganography for Hiding Images in Audio**. *International Journal of Computer Applications(0975-8887)* 11(6): pp.12-16.
- [4] Debnath Bhattacharyya, Poulami Dutta and Tai-hoon Kim (2009). **Secure Data Transfer through Audio Signal**. *Journal of Security Engineering* 6(3): pp.187-194.
- [5] Masoud Nosrati, Ronak Karimi and Mehdi Hariri (2012). **Audio Steganography: A Survey on Recent Approaches**. *World Applied Programming* 2(3): pp.202-205.
- [6] Ajay.B.Gadichal (2011). **Audio Wave Steganography**. *International Journal of Soft Computing and Engineering (IJSCE)* 1(5): pp.174-176.

AUTHORS

Linu Babu P received B.Tech degree in Electronics and Communication Engineering from Sasurie College Of engineering, affiliated to Anna University , Tamil Nadu. Presently she is pursuing her M.Tech in Applied Electronics and Communication Systems from Nehru College of Engineering and Research Centre, Pampady, Kerala, affiliated to University of Calicut. She is having 3 years of teaching experience.



Jais John working as an Assistant Professor in Department of Electronics and Communication Engineering, Nehru college of Engineering and Research Centre, Thrissur, Kerala . Before that he worked as a Lecturer in Department of Electronics at College of Applied Science (Govt. of Kerala Undertaking), Thodupuzha, India. He Obtained the Bachelor of Science Degree and the Master of Science Degree in Electronics from Mahatma Gandhi University, Kottayam, Kerala, India and the Master of Technology Degree in Communication System from Vellore Institute of Technology (VIT University), Tamilnadu, India. He done his M.Tech research project in the field of Optical Fiber Technology, specialized in Photonic Crystal Fiber design. His areas of interests are Optical Communication, Optical Sensors and Secure Communication.



Parameshachari B D working as an Associate Professor in the Department of Electronics and Communication Engineering at Nehru College of Engineering and Research Centre, Pampady, Thiruvilawamala, Kerala, India, affiliated to University of Calicut. Worked as a Senior Lecturer and incharge HOD in the Department of Electronics and Communication Engineering at JSS Academy of Technical Education, Mauritius. He worked at JSSATE, Mauritius for Three years and also worked as a Lecturer at Kalpatharu Institute of Technology, Tiptur for Seven years. He obtained his B.E in Electronics and Communication Engineering from Kalpatharu Institute of Technology, Tiptur and M. Tech in Digital communication Engineering from B M S college of Engineering, Bangalore, affiliated to Visveswararajah Technological University, Belgaum. He is pursuing his Ph.D in Electronics and Communication Engineering at Jain University, Bangalore, Karnataka, India under the guidance of Dr. K M Sunjiv Soyjaudah, Professor, University of Mauritius, Reduit, Republic of Mauritius and Co-guidance of Dr. Sumithra Devi K A, Professor and Director, Department of MCA, R V College of Engineering, Bangalore. Parameshachari area of interest and research include image processing, cryptography and Communication. He has published several Research papers in international Journals/conferences. He is a Member of ISTE, IETE, IACSIT, IAEST, IAENG and AIRCC.



Muruganantham.C working as an Assistant Professor in the Department of Electronics and Communication Engineering at Nehru College of Engineering and Research Centre, Kerala, India. He obtained B.E in ECE from Madurai Kamaraj University, Tamilnadu and M.E in Applied Electronics from Anna University, Tamilnadu. Worked as Assistant Professor-II in SEE of SASTRA University. Worked as Lecturer in Electrical & Computer Engg Department of Ethiopian Universities. Published papers in national/international conferences. He is member of ISTE. His areas of interest are High Speed VLSI Networks, Signal Processing.



Divakara Murthy H S has multi faceted experience in Research, Industry and Academic fields, He is working as a Dean and HOD in the Department of Electronics and Communication Engineering at Nehru College of Engineering and Research Centre, Pampady, Thiruvilawamala, Kerala, India, affiliated to University of Calicut and also served as a Principal at JSS Academy of Technical Education, Mauritius for two years. Involved in Administrative & Academic activities in development of infrastructure facilities marketing, mounting new courses and strategic planning. He worked at RGV telecom Ltd Bangalore as Deputy Vice president, for providing optical communication for Indian Railways for nearly two years and also worked nearly 27 years in Telecom in Industry at senior level in various capacities in Telecom Projects and Planning, Production and Marketing. During my initial career involved in Design and development of Instrumentation at NAL Bangalore. He obtained his B.E in Electronics and Communication Engineering from Siddaganga Institute of Technology, Tumkur from University of Mysore and MSc(Engg) in communication system from PSG Institute of technology, Coimbatore , from University of Madras. Divakara Murthy area of interest and research include Micro and Pico Satellite communication, Optical Communication and Wireless communication, GSM and WiMAX technology. He is a Member of ISTE, IETE

