Audio Steganography using Two Layered Encryptions

Dr. U B Mahadevaswamy
Professor
Dept. of Electronics & Communication
Sri Jayachamarajendra College of Engineering
JSS Science and Technology University
Mysuru, India

Megha K M
Assistant Professor
Dept. of Electronics and Communication
JSS Science and Technology University
Mysuru, India

Abhijith B S
Dept. of Electronics & Communication
JSS Science and Technology University
Mysuru, India

Adarsh
Dept. of Electronics & Communication
JSS Science and Technology University
Mysuru, India

Akash M K
Dept. of Electronics & Communication
JSS Science and Technology University
Mysuru, India

***Abstract*—Steganography is proposed as a new opportunity method to enhance mystery data communication in the most secured manner. Lately, precise and bendy audio steganographic methods are proposed. An ideal or perfect audio Steganographic technique aims at embedding information in an indistinguishable, sturdy and comfy manner after which extracting is done with the aid of legal human beings, without statistics loss throughout transmission. Recent hobbies toward designing a system that ensures high ability or robustness and security of embedded facts has brought about extraordinary diversification inside the present steganographic techniques. New algorithms with various embedding techniques have been designed. Multi-layered steganographic techniques are extremely popular in recent times. Using multiple layered embedding strategies not only enhances the data capacity, but also enhances the security of the overall machine. In this paper, we present LSB based totally audio steganographic strategies with double layered protection, every layer with distinctive embedding and deciphering method. We discover their potentials and performance to make sure at ease verbal exchange.**

Keywords—Steganography, Cover audio, encryption, decryption, intermediatory file, bytearray.

I. INTRODUCTION

Digital verbal exchange has ended up as a critical part of infrastructure nowadays and almost all the day-to-day activities are becoming internet based. As internet is becoming a major part of public life, people need to be extremely careful about the data. Privacy is an important aspect in day-to-day communications. So, the communication made must be secret. Steganography is the latest method of offering statistics transmission in secured way.

The term steganography comes from Greek words, “stegano” and “graphy” means “secret” and “writing” respectively. So, steganography is the art of hiding name of the game message in a cover medium in order that its presence is not detected. Audio Steganography encapsulates the private message in an audio signal, such as songs called cover audio. Secret message may be in the form of text, image or even audio. Once the important message is implanted in the cover audio, the resulting message is named stego message or public message. Public message is transmitted to the receiver. Any audio steganographic approach is expected to fulfil three conditions: Capacity means the size of mystery facts that may be implanted inside the host message Transparency estimates how well a message is incorporated within the cowl audio Robustness estimates the strength of mystery message to withstand against all odds.

The primary block diagram of a steganographic device is shown in Fig.1. The mystery message to be transmitted is implanted within a cover file. Embedding and extraction may be done using different algorithms.

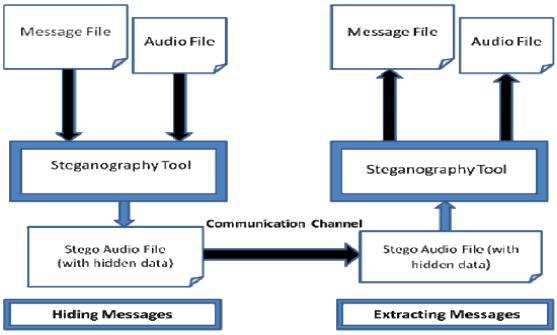

Fig1. Block diagram of steganographic system

II. MOTIVATION

Secret communication has become a great necessity in today’s world. Everyone is looking for secured way in

communication. Due to vulnerability in existing steganographic system, lot of people cannot transfer their information with full trust. Some of the information transferred are breached by the third person and this causes lot of havoc in the life of the user. In order to secure the data from a third party or a hacker, people are looking for an effective method of data hiding which motivates us to provide a secured platform for the required task effectively.

III. LITERATURE SURVEY

Recently, audio steganography has emerged as a crucial stenographic technique, wherein information is implanted within an audio file using various properties of voice signal. In time domain mostly used audio steganography is the Least Significant Bit method (LSB). The LSB method provides higher probability of un-detectability as the data change is minimum but suffers from Low robustness and low embedding fee. Some of the techniques, primarily based on LSB embedding scheme are discussed in the section below.

In paper [1], author suggested a new replacement method of audio steganography with improved protection where each data bit of secret message is inserted into the chosen position of a cowl audio. The choice of the location of encryption is based on upper 3MSB bits of cover media. Additional backup is provided with the usage of secret key.

In [2], writer proposed a technique wherein mystery message is encapsulated in different LSBs which is based on the MSBs of the samples of the carrier audio. In comparison with standard LSB technique MSBs of the samples of carrier audio file are checked in this method. The benefit of this technique is that it enhances the percentage of mystery message that can be added to the cover audio file without effecting the quality of the host audio.

In [3], author suggested a brand-new approach called “Robust Multi-Layer Audio Steganography", where data is embedded in different sections to enhance the strength, and the capacity is also enhanced by adding two data bits in the cover audio file. In this technique bitwise operation is implemented for extraction.

In [4], author presented the alteration of LSB method of audio steganography. The proposed method consists of two forms of LSB. First the modification of LSB is completed in 6th layer. Secondly the uniformity of specimen of cowl audio is compared together with confidential message bit accordingly. The method comes with various advantages like LSB at upper layer makes it very difficult for detection and suspicion. Also, the capacity is enhanced as the data is embedded in higher layer. The parity method makes the algorithm more efficient as it reduces the distortion and makes the secret information undetectable.

In LSB alteration technique, some bit(s) in specimen of a cowl message is/are modified with data bits of the mystery message [5]. However, normally unique bit is being used. The improvements within the method have shown that modifying many bits in a sample has no considerable change in the properties of the host message [6]. This enhances the potential of the approach but may additionally decorate the share of noise in the public record [7].

IV. OBJECTIVES

The objectives for this in th layer. are as follows:

- To hide the secret data during transmission of message.
- To ensure that no data is lost during transmission and receiver can access complete data.
- To provide a two layered security system which is very much difficult to breach for any third-party user or hacker.
- To ensure that the file sent during transmission is clean without any noise and disturbance.

V. PROPOSED METHOD

In the proposed work, a new technique is presented where the security is enhanced using a two layered encoding and decoding methods. The secret information to be transmitted is in the form of text or image. We need two audio files, with second file being at least five times the size of first file, which are used as cover files. Secret information is embedded in the first audio file and a new intermediatory audio file is generated. This intermediatory file is embedded in second audio file during second layer encoding technique. Decoding is done by extracting the data portion in the file, opposite to the encryption algorithm.

A. Layer 1 Encoding Algorithm

The input consists of cover audio file and secret information in the form of text or image file. Audio file is converted into byte-array and text and image files are converted into string array and NumPy array respectively. Size of the bytearray is at least eight times the size of string or NumPy array. The size of bytearray and string or NumPy array are made same by adding a dummy character like ‘#’ to string or NumPy array for the similarity of pattern for modification. One bit from each byte in byte array is replaced with one bit from string or NumPy array in sequential order. The bits replaced in byte array vary from LSB in first byte to MSB in eighth byte and the pattern repeats. First the LSB of each byte in byte array is replaced with one bit from string or NumPy array. Then the data bits are shifted to the required position. Pseudo code to shift the data bits is given below.

```
def modify_given_Bit (number, position, bit):
        mask = 1 << position
        return (number & ~mask) | ((bit << position) & mask)
```

where number, position and bit represent the count of byte array, position of bit to which data is to be replaced and data bit respectively. The flowchart of Layer 1 encoding algorithm is shown in Fig. 2.

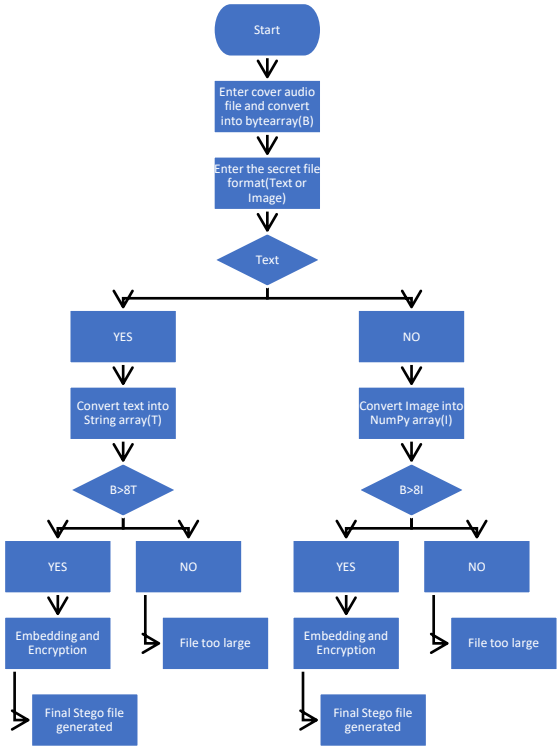

Fig. 2. Data Encoding in Layer 1

B. Layer 2 encoding algorithm.

Input consists of intermediatory stego file and cover audio file of larger size. Both the audio files are converted to byte array. Unlike layer 1 encryption, byte to byte replacement is used in layer 2 encryption. The first 25 bytes are reserved to store some information that are necessary for the receiver side decryption method and the encryption starts from 31st byte in cover file. Size of byte array of cover audio file reduced by 30 is divided with that of intermediatory stego

C. Decryption 1

Once the stego file is received by the receiver he needs to decode the file to get the secret information. Since encryption is double layered, receiver should perform two layered decryptions to get the original information. Input in decryption 1 consists of final stego file and cover file used in layer 1 encryption. Both audio files are converted to byte array. The information stored in first 25 bytes are read. This information provides the position of the bytes in stego file which consists of the data to be decoded. Decryption is done by extracting the data bytes and replacing the byte arrays of file. The integer value obtained is stored in first byte of cover file. The data is embedded in cover file from 31st byte, with multiples of the value of first byte of cover file added to 31. Number of integers in size of byte array of intermediatory stego file is stored in second byte of cover file. Value of these integers are stored from 5th to 25th byte with gap of five bytes in cover file. A new audio file will be generated which contains the original data and this is sent to the receiver. The flowchart of the procedure is shown in Fig. 3.

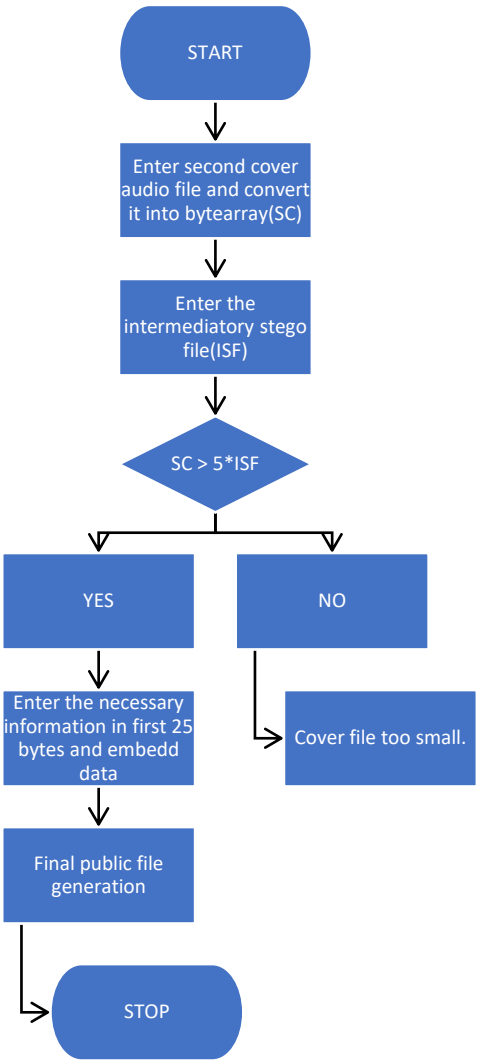

Fig. 3. Data Encoding in Layer 2

cover file of layer 1 encryption with these data bytes. The flowchart of the procedure is shown in Fig. 4.

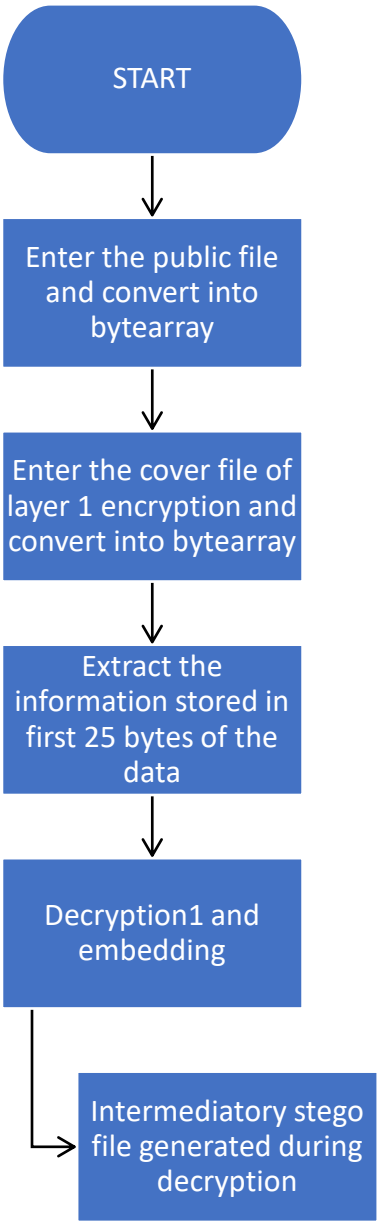

Fig. 4. Decryption 1

D. Decryption 2

This is the final procedure to get the original data. Input consists of intermediatory stego file generated during decryption 1. This is converted to byte array and all the data bits present in the different bit position are shifted to LSB. The dummy character '#' which was inserted during layer 1 encryption for string array is removed for text file. Finally, output is obtained as text file or as image file based on the input provided. The flowchart of the process is shown in Fig. 5.

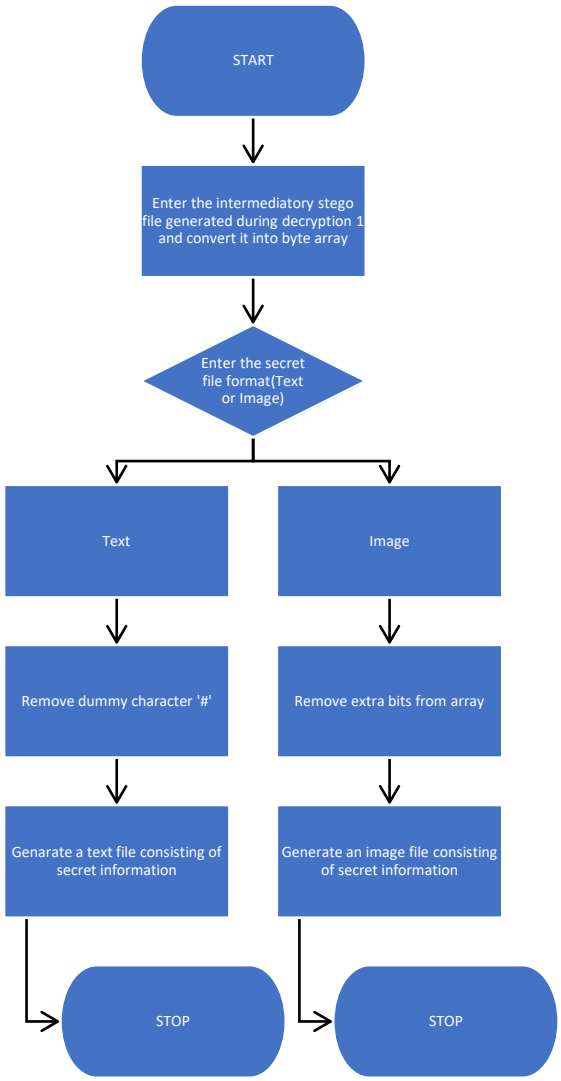

Fig. 5. Decryption 2

VI. RESULTS AND DISCUSSION

Fig.6 and Fig.7 is the screenshots of the secret text file and secret image.

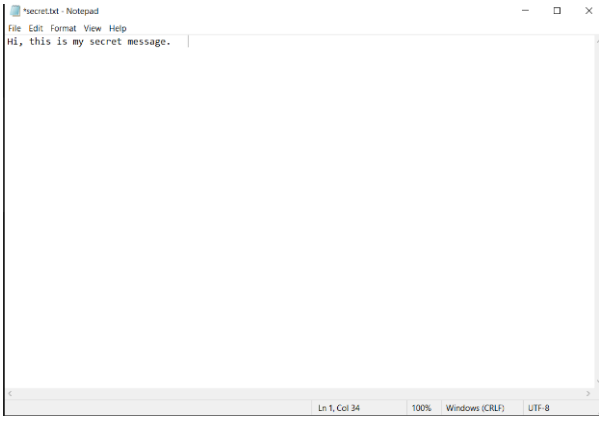

Fig 6 Secret data (Text)

Fig 7 Secret data (Image)

Fig.8 shows the generation of new intermediatory audio file after first layer of encryption for both text and image files.

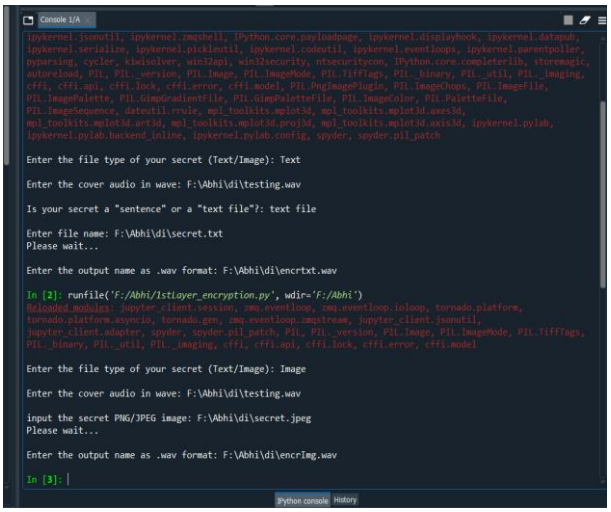

Fig .8. Layer1 Encryption

Fig. 9 shows the generation of final output audio file which is completely encrypted and is ready for transmission.

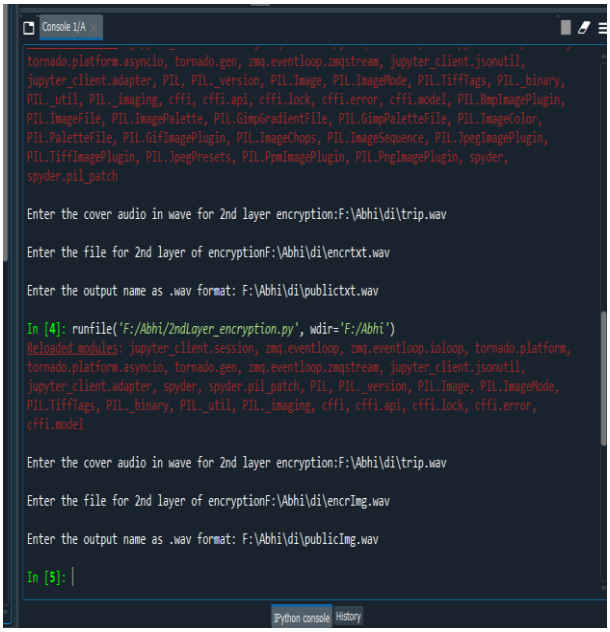

Fig. 9. Layer 2 encryption

Fig. 10 shows the intermediatory file generated after decryption 1. An audio file which contains secret text or image is generated.

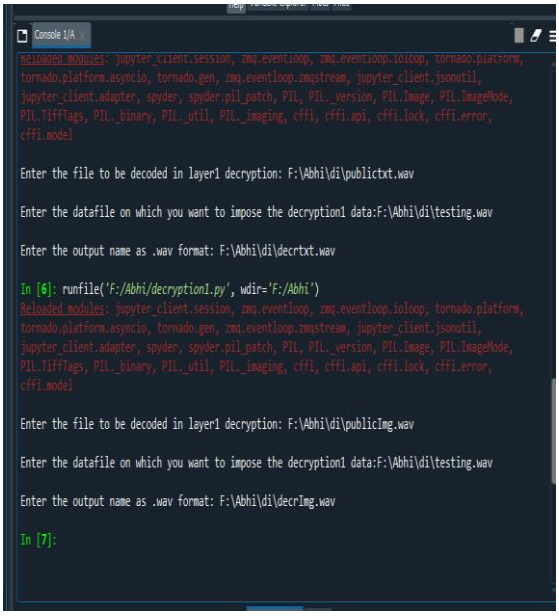

Fig. 10. Decryption1

Fig. 11 and Fig. 12 shows the screenshots of final text and image file that is finally extracted by the receiver. There is no data loss in the final information obtained.

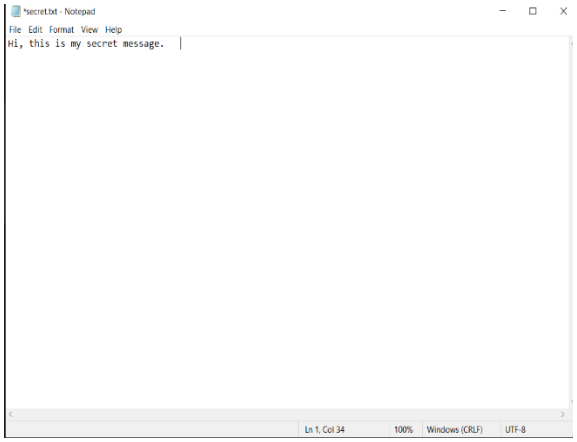

Fig. 11. Final output(text)

Fig. 12 Final output (Image)

Cover audio file of second layer encryption was compared with final stego file obtained after second layer encryption. The similarity between the audio files is 99.99% as shown in Fig. 13. Since the difference between the two audio files is negligible, it is impossible for the hacker or any third user to detect the presence of data in the final stego file.

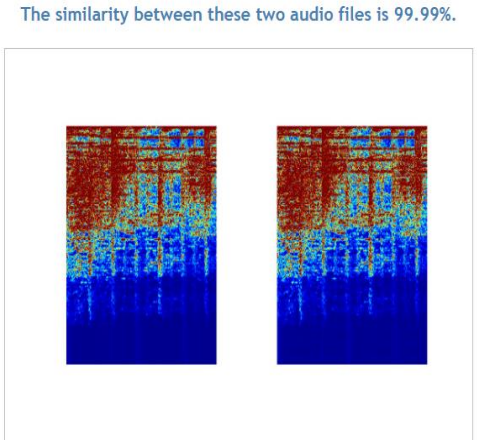

Fig. 13 Comparison of two audio files

VII. CONCLUSION AND FUTURE WORK

The proposed work gives a great insight on how signal processing works and how to implement the same in real life applications. This project has great applications towards privacy/secrecy i.e., defence applications. This technique gives an edge over the classical techniques of cryptography where a hacker might decode the algorithm by just understanding the algorithm of encryption. What this offer is cloaking, hence people are not prone to suspicion.

The proposed work is just a prototype. We can achieve more privacy by generating a key so as to lock our secret data, even if the code/app is leaked, so as to retrieve the secret, one must enter a passcode generated while embedding the data into the cover. There is another type of steganography 'Frequency modulation-based steganography', where an audio is embedded in a cover audio to be transmitted. We can mix both of them and come up with an excellent idea.

One can embed a secret data in a cover audio which is an ultrasonic frequency signal which in turn is hidden in a cover audio using frequency modulation-based steganography. This is not only strong but complex as well. The things to be kept in mind in these steganography projects are that these projects are digital and must keep in mind the sampling rate. There must be no mistake in sampling rate of the cover audio, otherwise the data is lost forever. There is an ocean of opportunities and no one way to do this project. One must always look for simpler and stronger alternatives which sometimes contradict each other.

VIII. ACKNOWLDGMENT

The authors thank the principal, the faculty and all the technical staff of electronics and communication engineering department of Sri Jayachamarajendra College of Engineering, JSS Science and Technology University, Mysuru, Karnataka, India

IX. REFERENCES

[1] Shweta Vinayakarao Jadhav, A.M. Rawate, "A New Audio Steganography with Enhanced Security based on Location SelectionScheme", International Journal of Sceintific Enginneering and Research-2016.

[2] Mohsen Bazyar, Rubita Sudhirman, "A New Method to Increase the capacity of Audio Steganography Based on the LSB algorithm", Journal Teknologi Science and Engineering, 74:6 (2015), 49-53.

[3] Biswajita Datta, Prithwish Pal and Samir Kumar Bandyopadhyay, "Robust Multi-Layer Audio Steganography", IEEE-2015.

[4] Jyoti Bahl, Dr. R. Ramakishore, "Audio Steganography using Parity Method at higher LSB layer as a variant of LSB Technique", International Journal of Innovative Research in Computer and Communication Engineering-Vol. 3, Issue 7, July 2015.

[5] Kaliappan Gopalan., "Audio steganography using bit modification", 2003 IEEE International Conference on Acoustics, Speech, and Signal Processing, Page(s): II - 421-4 vol.2.

[6] Nedeljko Cvejic, Tapio Seppanen, "Increasing the capacity of LSBbased audio steganography", 2002 IEEE Workshop on Multimedia Signal Processing, Pages: 336 - 338.

[7] Kaliappan Gopalan, Qidong Shi, "Audio Steganography Using Bit Modification - A Tradeoff on Perceptibility and Data Robustness for Large Payload Audio Embedding", 19th International Conference on Computer Communications and Networks, Pages: 1 - 6

AUTHORS DETAILS

Dr. U B Mahadevaswamy is working as Professor in the department of Electronics and Communication Engineering, JSS Science and Technology University, Mysuru, Karnataka, India. He received his Bachelor of Engineering in Electronics and Communication from University of Mysuru in the year 1988, and obtained his Master's degree in Industrial Electronics from Mangalore University in the year 1995 and Ph.D. in the area of Wireless Sensor Networks from University of Mysore, Mysuru in the year 2013. His areas of interest include Control Systems, Analog and Mixed Mode VLSI Circuits, Linear Integrated Circuits and Signal Processing.

Megha K M is working as Assistant Professor in the department of Electronics and Communication Engineering, JSS Science and Technology University, Mysuru, Karnataka, India. She received her Bachelor of Engineering in Electronics and Communication from GSSS Institute of Engineering and Technology for Women, Mysuru in the year 2015, and obtained her Master's degree in Digital Communication and Networking from CMRIT, Bengaluru in the year 2017.

Abhijith B S is pursuing B.E. in Electronics and Communication Engineering at JSSSTU, Mysuru, Karnataka, India.

Adarsh is pursuing B.E in Electronics and Communication Engineering at JSSSTU, Mysuru, Karnataka, India.

Akash M K is pursuing B.E in Electronics and Communication Engineering at JSSSTU, Mysuru, Karnataka, India.