Efficient Reversible MP3 Steganography with Zero Error LSB Method

Madhuri Kumari[1], Prof. Komal Tahiliani [2]
[1]*M.tech. Scholar,* [2]*Guide*
Department of Computer Science & Engineering, School of Research & Technology, People's University, Bhopal (M.P.)

Abstract - recently, the need for digital communication has increased dramatically and accordingly, the Internet has turned out to be basically implies increasingly effective and faster communication to digital communication. In the meantime, data on the Internet has turned out to be susceptible to piracy, copyright infringement and espionage etc., which thusly requires secret communication. Accordingly, another domain dedicated to data security has evolved and is known as data hiding. Steganography is a generally novel addition to the domain of data hiding but traces its origin to sometime in the past in history. Invisible ink has been used for quite a long time for the sake of entertainment by children and students and for genuine undercover work by government agents and terrorists. The security of the data is above all else need while transmitting starting with one place then onto the other place or stored some place. Steganography is the capacity of hiding messages inside an image file/Audio file or a Video file with the end goal that the very presence of the message is hidden to third party. Cryptography is used to encode the data with the goal that it is unreadable by a third party. Such procedures will encourage different secret data sharing techniques. From the outcomes it is also clear proposed technique has no effect on audio quality even after information hiding.

Keywords - Audio, LSB, Reversible, Steganography, Secret Information.

I. INTRODUCTION

With advancements in digital communication technology and the growth of computer power and storage, the difficulties in ensuring individuals' privacy become increasingly challenging. The degrees to which individuals appreciate privacy differ from one person to another. Various methods have been investigated and developed to protect personal privacy. Encryption is probably the most obvious one, and then comes steganography. Encryption lends itself to noise and is generally observed while steganography is not observable.

Interest from the scientific community has escalated in the past few years in relation to steganography. This exhibits itself in the establishment of new dedicated conferences and books, increased funding from defence ministries, and the birth of various commercial companies. Needless to say that in a few countries, the burgeoning concern that leads to this generosity is as a result of the widespread paranoia of criminals and terrorists who may or may not use this method to communicate. Therefore, funding in those countries was biased towards counter-attacking steganography and paid little concern to enhancing the privacy of individuals.

Steganography is the art and science of hiding communication by embedding secret data in public cover media without raising suspicion. Due to the availability of the Internet, lack of trust, and the demand for secret communication, people try to secure their private messages using more advanced steganography techniques rather than traditional cryptographic methods. The idea of hiding secret messages in multimedia files like images and video gives an opportunity to a variety of application areas beyond steganography, collectively known as information hiding. Any digital media with some redundancy in their representation could be used by steganographers for embedding secret messages. Hence, digital images became one of the most common cover media used for this purpose. Also, the most widely used method of steganography is least significant bit (LSB) replacement in digital images, due to its extremely easy implementation, imperceptibility, and reasonable capacity. However, LSB steganography is very easy to attack and there are many methods in the literature that can accurately detect them.

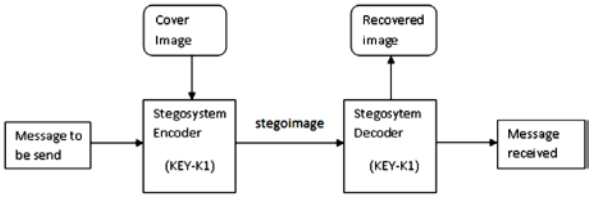


Fig.1.1 Basic block diagram of steganographic system.

A basic block diagram of steganographic model is depicted in Fig. 1.1. The information is inserted in a cover image by the stegonographic encoder, which may employs a key or password. Here the concept of symmetric key steganography having both side the same key(K1) is used. Now the produced stego image is transmitted to the receiver and it is decoded by using the same key to get back the original message. As the stego image is carried over channel, it may be viewed by unintended persons but stego image will behave like an innocent medium without showing the hidden message inside it.

The hard truth for steganographers is that LSB method is reliably detectable by current steganalysis methods with a very accurate estimation of the length and the embedding locations of the secret message. Thus, an efficient reversible mp3 steganography with zero error LSB method has reported in this examination.

One of the most realistic applications of steganalysis methods is its usability as a detection tool for hidden contents by digital forensics analysts, especially for cases that related to cybercrime and terrorist activities. In this case, as the embedding methods are continuously improved, the digital forensics analyst also needs better detection methods to reduce the probability of false alerts in their investigation process.

II. AUDIO STEGANOGRAPHY

Data hiding in audio signals is especially challenging as compared to data hiding in digital images because the human auditory system (HAS) operates over a wide dynamic range in comparison with human visual system (HVS). Sensitivity to additive random noise is also acute. On the other hand, opposite to its large dynamic range, HAS contains a fairly small differential range, i.e., loud sounds generally tend to mask our weaker sounds. Additionally, the HAS is unable to perceive absolute phase, only relative phase finally, there are some environmental distortions so common as to be ignored by the listener in most of the cases. Such are the weaknesses of HAS that can be exploited for hiding data in audio signals.

The effects of human auditory system (HAS) relative to Steganography are temporal masking and frequency masking. In temporal masking, a weaker audible signal on either side (pre and post) of a strong masker becomes imperceptible. Similarly, in frequency masking, if two signals occurring simultaneously are close together in frequency, the stronger masking signal may make the weaker signal inaudible.

In the past few years, several algorithms for the embedding and extraction of messages in audio sequences have been proposed. All of the developed algorithms take advantage of the perceptual properties (characteristics) of the human auditory system (HAS) in order to hide data into the host signal in a perceptually transparent manner. Some commonly used methods are:

- Least Significant Bit (LSB) Coding
- Parity Coding
- Phase Coding
- Spread Spectrum
- Echo Data Hiding

One of the earliest techniques studied in the information hiding of digital audio (as well as other media types) is LSB coding. In this technique, LSB of binary sequence of each sample of digitized audio file is replaced with binary equivalent of secret message.

For example the letter "A" (binary equivalent 1000001) is to be hidden into a digitized audio file where each sample is represented with 16 bits, then LSB of 7 consecutive samples (each of 16 bit size) is replaced with each bit of binary equivalent of the letter "A"

The number of LSB‟s for data hiding can be increased, but it also increases the amount of resulting noise in the audio file as well. Thus, one should consider the signal content before deciding on the LSB operation to use. For example, a sound file that was recorded in a bustling subway station would mask low-bit encoding noise. On the other hand, the same noise would be audible in a sound file containing a piano solo. To extract a secret message from an LSB encoded sound file, the receiver needs access to the sequence of sample indices used in the embedding process.

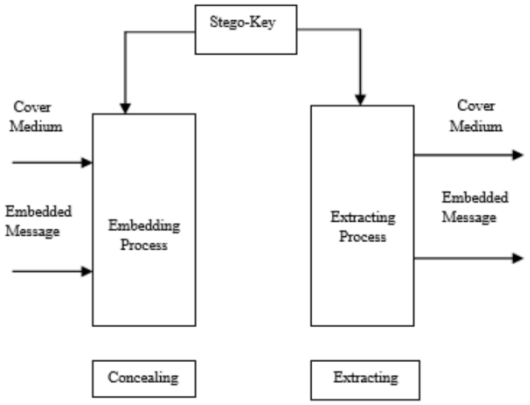


Fig.2.1 Steganography Process.

III. PROPOSED METHODOLOGY

There is a continuous challenge in securing digital transmission between network nodes against any form of penetration and intrusion. MP3 file is divided into header frames and audio data frames to ensure data security requires considering three primary segments as integrity, confidentially, and availability. Methods utilizing header frames to embed secret message are described, MP3 file structure is explained. To address impediments of embedding algorithms after compression, this work introduces another procedure in LSB. The algorithm is described as zero error LSB Least Significant Bit (ZLSB) procedure, which is developed to build the security of secret message, and improves the method of embedding the secret message in the host file. Steganography audio is the development of science from setagnography. The audio file can be used to hide data or secret messages. Audio Steganography methods can embed any messages in MP3

sound files. The steganography of audio, secret messages are embed into digital audio signal which results into changing binary sequence of corresponding audio files. The essential model of steganography on audio comprises of transporter (Audio file), message and password. Carrier or usual called a cover file, which stores confidential information. Fig. 3.1 shows the embedding process and flow of embedding is shown in Fig. 3.3. Extraction process of proposed work has shown in Fig. 3.2 block diagram of proposed extraction process in and 3.4 shows the process flow of proposed extraction process.

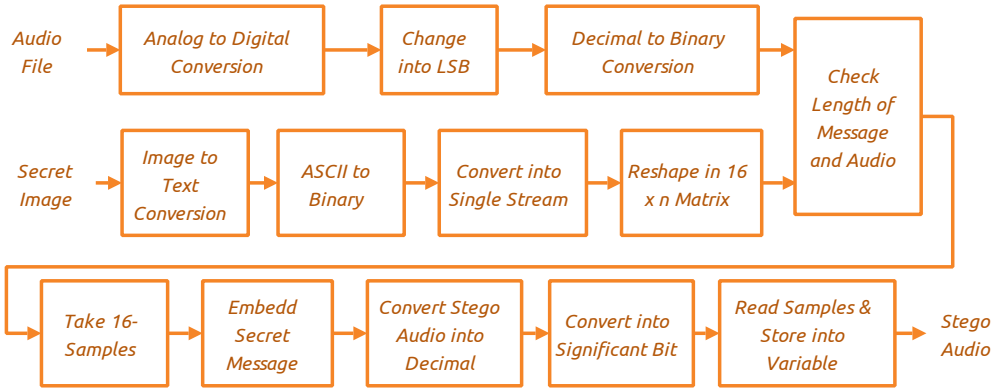


Fig.3.1 Block Diagram of Embedding Process.

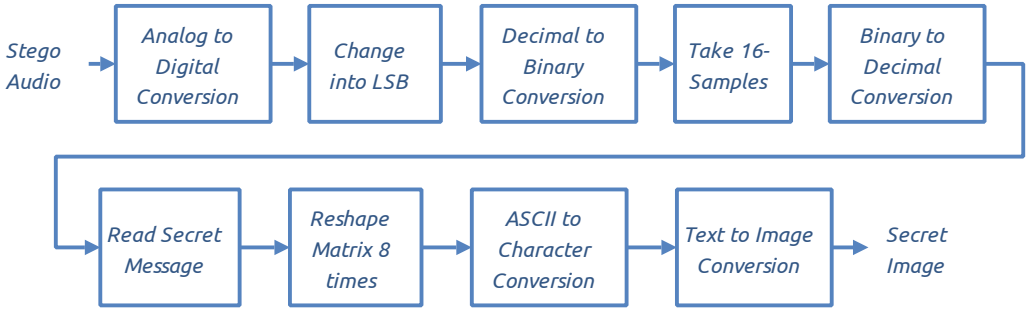


Fig.3.2 Block Diagram of Extraction Process

A. Embedding Process

The implementation of proposed algorithm has carried out in MATLAB as shown in Fig. 3.3. First load audio file in MATLAB. Convert analog audio file into digital audio file and convert it into significant bit. Apply decimal to binary conversion on significant bit. Convert sample secret image into text. Load the converted text massage and convert into binary and convert it to Matrix of 16Xn. Now start hiding message into audio stream. Convert binary to decimal and sample it. Again convert into decimal and save stego audio file now the embeding process of secret image has completed end embedding process.

B. Extraction Process

From the previous process a secure embedded file has achieved at the receiver end it is need to decode to extract actual information. To extract original information stego audio file is loaded into MATLAB read using MATLAB default read function. Convert analog stego file to digital file format. Read significant bits and convert from decimal to binary format. Read secret message from stego file. Reshape it into 8Xn matrix. Convert binary data from its equivalent ASCII values and further ASCII to character. Convert text to image. Display recovered secret image.

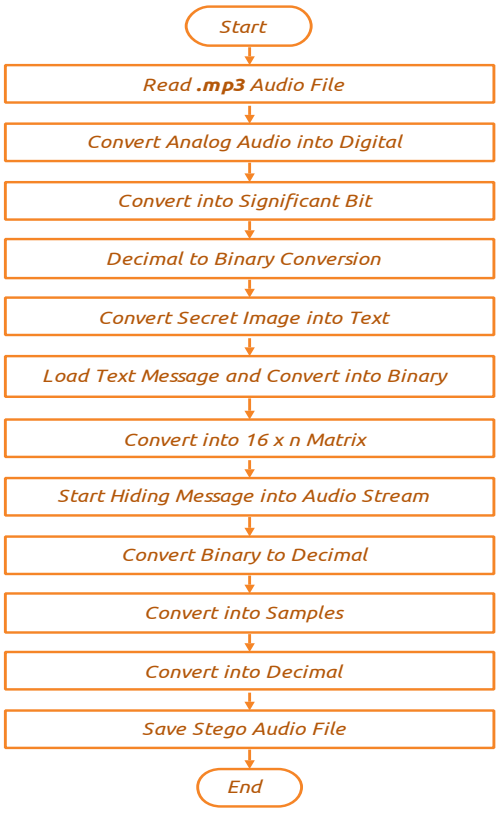


Fig.3.3 Flow Chart of Embedding Process

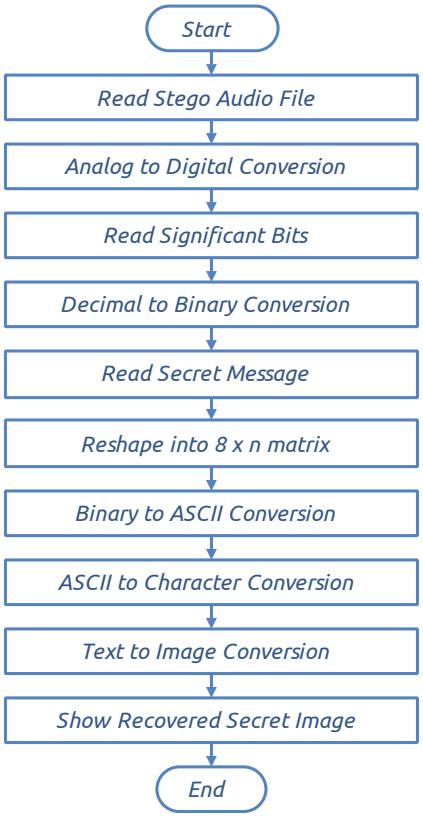
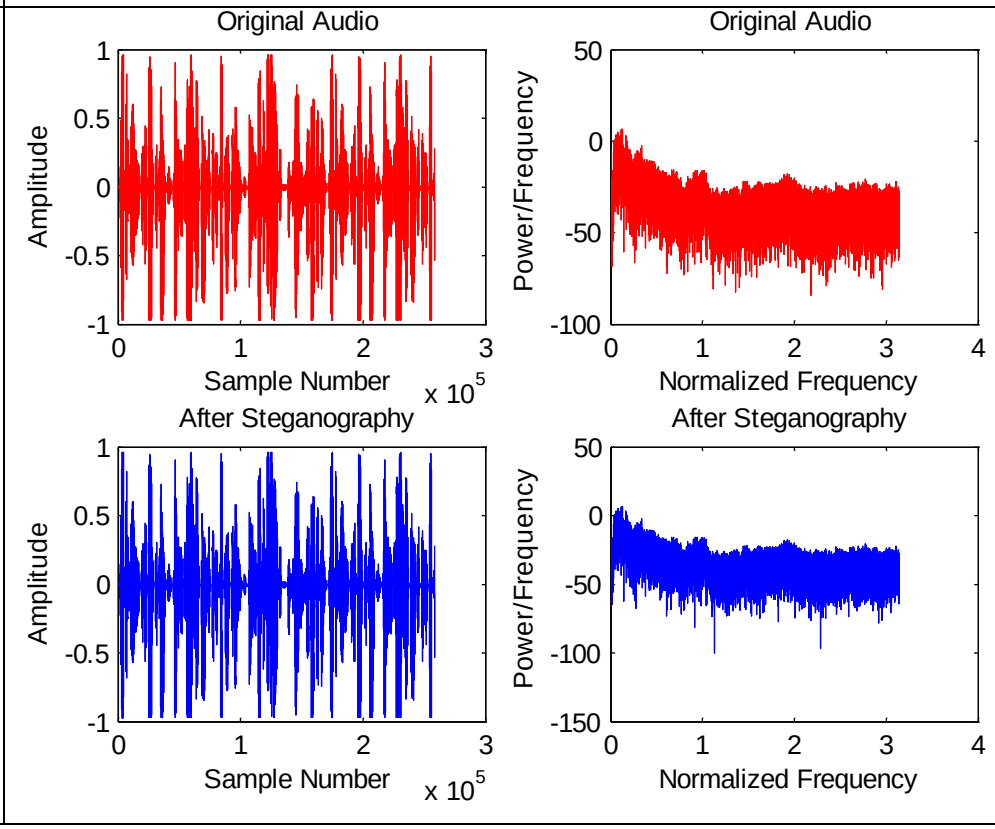


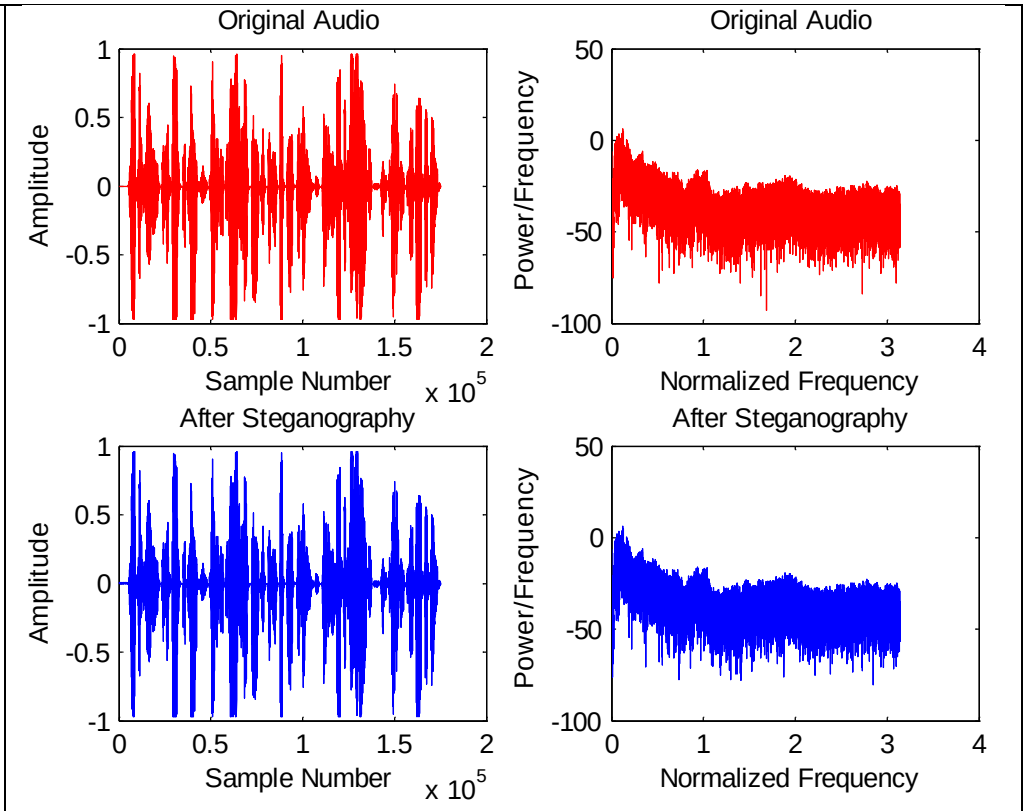
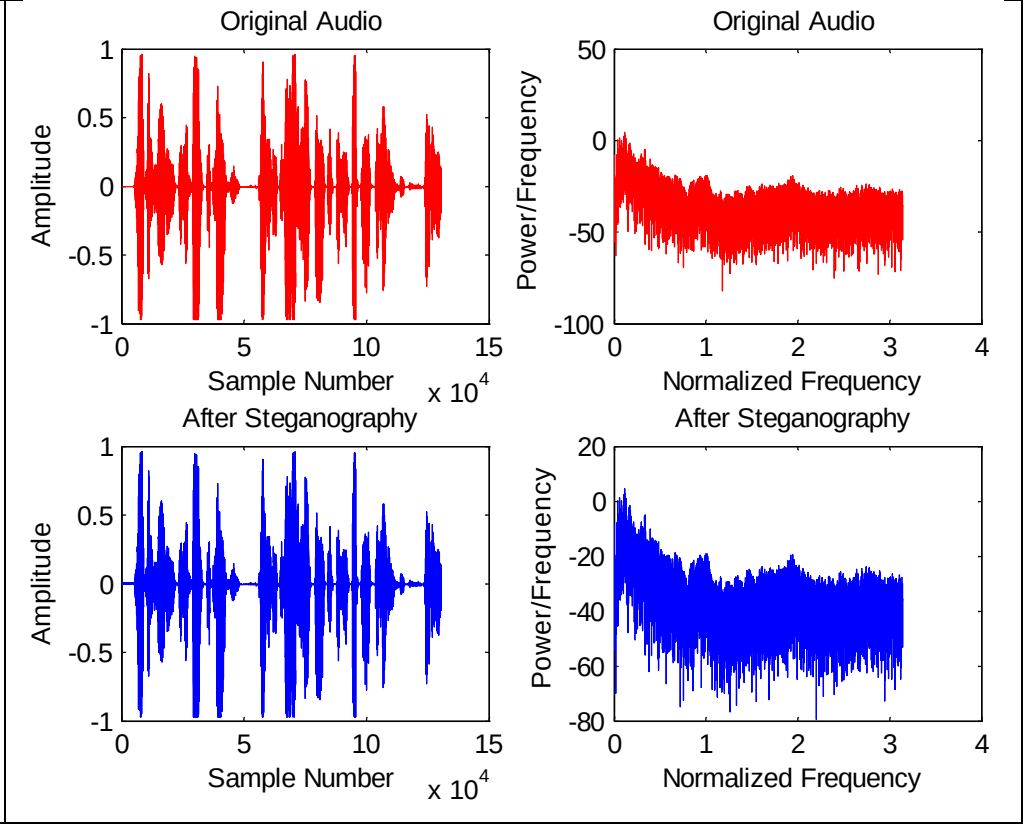
Fig.3.4 Flow Chart of Extraction Process

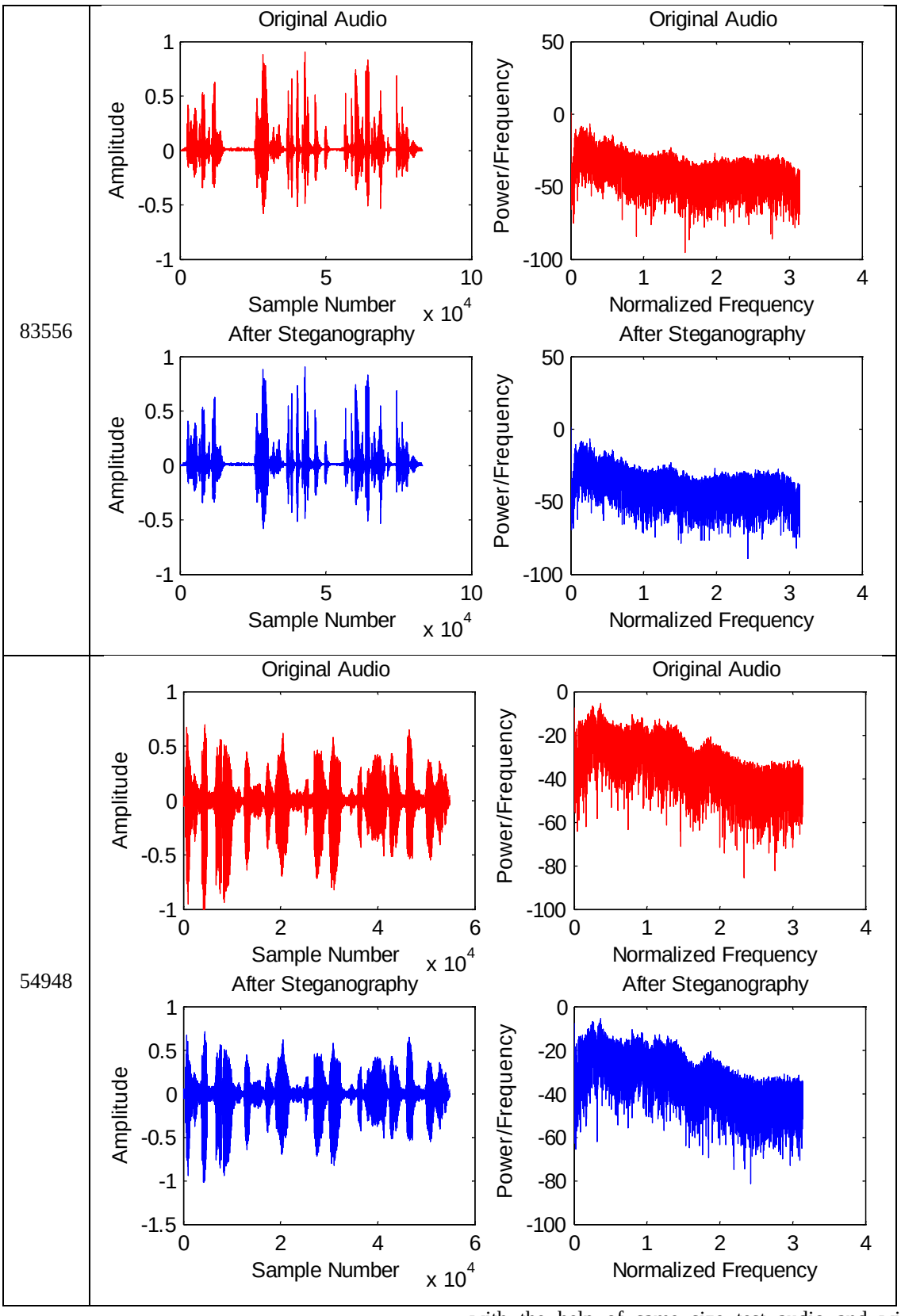
The evaluation and simulation of the proposed Steganography system has completed in MATLAB. The security parts of the proposed method analyzed based on MATLAB simulation. In addition the key affectability and key space should be adequate. To make the test results progressively solid, different arrangements of audio are considered as appeared Table. 3.1 size of audio file taken for experimental analysis and its corresponding waveform and power spectrum. To verify the efficiency of the proposed embedding algorithm, detection methods are considered based on the zero error LSB. In all simulation based experimental analysis, pseudo-random bits streams are considered as a secret message of 100bit due to the way that it will have every statistical property of an encrypted version of the secret message. The detection results of the proposed method showed that the proposed method can effectively improve the embedding efficiency in comparison to previous approach. The most generally used method of image steganography is the LSB embedding. The purpose for the interest in LSB steganography is that it is anything but difficult to execute, has a sensible limit, and is outwardly vague. Be that as it may, it could be effectively detected due to the lopsidedness distortion on the intensity histogram of the image and producing 'Sets of Values'.

IV. SIMULATION OUTCOMES

Table 4.1 Test Audio Characteristics

Audio File Size	***Audio Waveforms and Power Spectrum***
259664	

175154	
130770	



In this proposed scheme, when substituting LSBs of each edge pixel, by the secret message on cover audio mp3, not only is the PSNR high, but the stego image quality is also good. To prove that this scheme provide better stego image quality than the normal LSB steganography methodology, with the help of same size test audio and with same payload ratio, the performance of classic LSB steganography is compared with proposed scheme. The comparative analysis of proposed scheme with previous approach tabulated in Table 3.2 in terms of PSNR in dB

and its graphical representation is shown in Fig.4.1 PSNR comparison chart.

Table 4.2: Comparison of Performance between Previous [1] and Proposed Work (Our)

Audio File Size	*Previous [1]*		*Proposed(Our)*	
	Secret Message Size(bytes)	*PSNR (dB)*	*Secret Message Size(bytes)*	*PSNR(dB)*
259664	100	50.67	941	60.24
175154	100	39.43	941	58.69
128770	100	68.25	941	57.42
83556	100	40.31	941	54.75
54948	100	42.60	941	44.83

Table 4.3: BER Evaluation between Previous [1] and Proposed Work (Our)

BER (%)	
Previous [1]	*Proposed (Our)*
0.00441	*0.0000%*

BER performance of proposed algorithm evaluated and analyzed as shown in table 4.3 BER Evaluation between Previous [1] and Proposed Work (Our). It is clear that proposed algorithm has better BER performance as compared to previous work. In proposed work based on MATLAB it is found it is very error resistance.

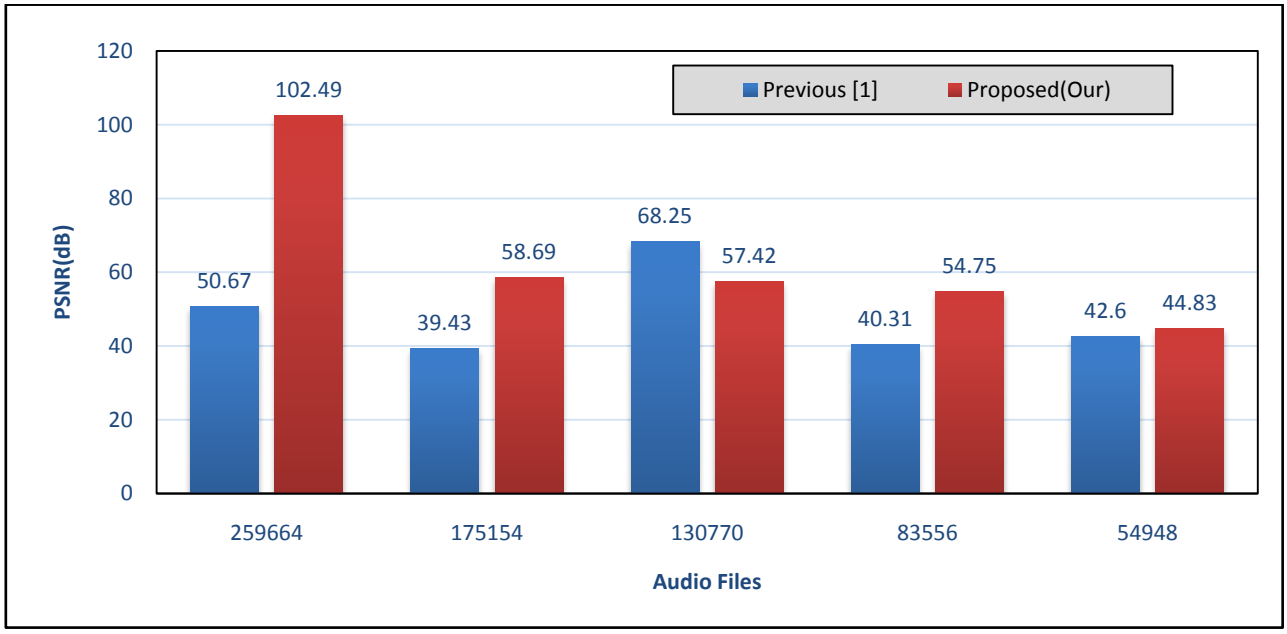


Fig.4.1 PSNR Comparison Chart

V. CONCLUSION AND FUTURE SCOPE

Steganography, the science of secret communication, has received much attention from the scientific community recently. This examination has reported a novel way to deal with audio (mp3) steganography which provided enhancements to the current available steganography algorithms. The primary objective of this examination was not simply on the embedding methodology, similar to the trend in ongoing examination, but at the same time was on the pre-processing stages, for example, payload encryption and embedding region determination. It was observed that the majority of the present algorithms depend intensely on the traditional encryption frameworks which for different outlined reasons. Exploiting the benefits brought by these two algorithms, a new system named Steganoflage was created which used an object-oriented embedding strategy. The results were promising and outperformed relevant methods.

Today's world of digital media is in a constant state of evolution. Steganography is regarded as technology that has major competitive applications. In this regards, future work is set mainly to increase the robustness against digital-analogue-digital distortions which is also known as the print-scan resilience. Additionally, improving the algorithm to be able to withstand severe JPEG/MPEG compression would be a challenge.

REFERENCES

[1] R. Indrayani, H. A. Nugroho and R. Hidayat, "An evaluation of MP3 steganography based on modified LSB method," 2017 International Conference on

Information Technology Systems and Innovation (ICITSI), Bandung, 2017, pp. 257-260.

[2] M. C. Sushmitha, H. N. Suresh and J. Manikandan, "An approach towards novel video steganography for consumer electronics," 2017 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia), Bangalore, 2017, pp. 72-76.

[3] A. Pradhan, A. K. Sahu, G. Swain and K. R. Sekhar, "Performance evaluation parameters of image steganography techniques," 2016 International Conference on Research Advances in Integrated Navigation Systems (RAINS), Bangalore, 2016, pp. 1-8.

[4] S. Bukhari, M. S. Arif, M. R. Anjum and S. Dilbar, "Enhancing security of images by Steganography and Cryptography techniques," 2016 Sixth International Conference on Innovative Computing Technology (INTECH), Dublin, 2016, pp. 531-534.

[5] M. Takahashi and H. Yamamoto, "Photographing-decodable steganography by use of a high-frame-rate LED display," 2015 14th Workshop on Information Optics (WIO), Kyoto, 2015, pp. 1-3.

[6] D. Yadav, M. Agrawal and A. Arora, "Performance evaluation of LSB and LSD in steganography," 2014 5th International Conference - Confluence the Next Generation Information Technology Summit (Confluence), Noida, 2014, pp. 515-520.

[7] D. Majercak, V. Banoci, M. Broda, G. Bugar and D. Levicky, "Performance evaluation of feature-based steganalysis in steganography," 2013 23rd International Conference Radio elektronika (RADIOELEKTRONIKA), Pardubice, 2013, pp. 377-382.

[8] Y. Zheng, F. Liu, C. Yang, X. Luo and K. Zhao, "Identification of Steganography Software Based on Core Instructions Template Matching," 2011 Third International Conference on Multimedia Information Networking and Security, Shanghai, 2011, pp. 494-498.

[9] K. Alla and R. S. R. Prasad, "A New Approach to Hindi Text Steganography Using Matraye, Core Classification and HHK Scheme," 2010 Seventh International Conference on Information Technology: New Generations, Las Vegas, NV, 2010, pp. 1223-1224.

[10] S. Sarreshtedari, M. Ghotbi and S. Ghaemmaghami, "One-third probability embedding: Less detectable LSB steganography," 2009 IEEE International Conference on Multimedia and Expo, New York, NY, 2009, pp. 1002-1005.

[11] Boulis, A. et al. (2003) Aggregation in Sensor Networks: An energy-accuracy trade-off. Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications.

[12] Castelluccia, C., Mykletun, E. and Tsudik, G. (2005) Efficient Aggregation of Encrypted Data Wireless Sensor Network, Proc. ACM/IEEE Mobiquitous, San Diego, CA.