DOI: http://dx.doi.org/10.26483/ijarcs.v10i4.6454

ISSN No. 0976-5697

Volume 10, No. 4, July – August 2019

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

SECURE DATA TRANSMISSION IN MP3 FILE USING LSB AND ECHO HIDING

Shwe Sin Myat Than
Dept. of IT Support and Maintenance
Computer University (Hpa-an)
Myanmar

Abstract: Steganography is the hiding secret message in the various media and very popular in today network transmission and information security. Although many of the secure transmission have been done in digital image, a little work has been done in audio mp3 file. Hiding data in mp3 file is the most researchable area and preferable way to carry secret data. Therefore this paper proposes a way of hiding secret message into mp3 file by using LSB, Least Significant Bit technique and Echo Hiding. LSB is the most popular steganographic technique but there is a weak point in including noise, compression technique and extraction process. To compensate that weakness, the combination of Echo Hiding in time spectrum is proposed. The integration is used in serial. To test the effectives of the methods, various types of genres is prepared in different compression rates. The experimental results are carried out for different size of the secret message files.

Keywords: Audio, Echo Hiding, Information Security, Least Significant Bit (LSB), MP3, Secure Data Transmission, Steganography

I. INTRODUCTION

The development of various types of digital technology is growing so fast and communication technology is one of them. Many messages are delivered in digital media and digital communication technology is a computer-based electrical communication technique using the binary number system. Binary numbers will form the codes that represent certain information by digitization. Digital messages can be in various form of text, images, audio or video. The security of digital messaging, especially secure digital messaging, is necessary [1].

Steganography is the study of techniques for hiding the existence of important information in the presence of primary cover information without effects on the size nor results in perceptual distortion and the message needs to be understood by the receiver. The important information is referred to as concealed message, concealed file or concealed information while cover information is known as transporter or embedded stego signal. Digital steganography can be classified [2] as described in figure 1.

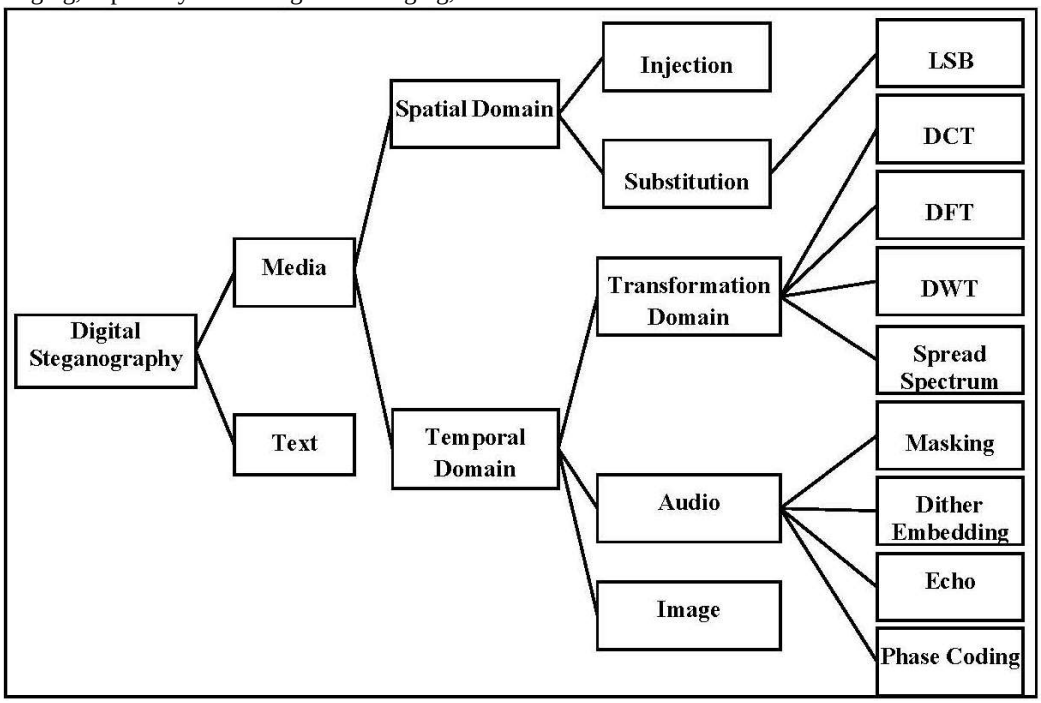

Figure 1: Classification of Digital Steganography

Therefore the MP3 is becoming a kind of universal carrier in today steganographic world, because it is precise suitable to share audio in various popular platform such as WeChat and YouTube. Various types of steganographic algorithms have been done in the audio compressed domain in long term ago. However, most of them generally get low performance in embedding capacity and very poor security. Conventional steganographic methods cannot satisfy security requirements; therefore hybrid MP3 steganography is inevitable tendency in modern steganography [3].

Although, MP3 audio files are very widespread used media file over the world, there has been a little work by applying Stenographic techniques to MP3 audio files in comparing with digital images [4]. Therefore, this paper looks at ways to embed information inside MP3 audio files.

II. MP3 FILE FORMAT

The audio MP3 files are digitally encoded using MPEG-1 Audio Layer III format, third audio format of the MPEG-1 standard. The next versions are MPEG-2 and MPEG-2.5. For all version of MPEG encoded MP3 files, the same steganographic methods can be applied but the newest versions can be done in simplest ways and the oldest version is the hardest. This paper focus on MPEG-1 Audio Layer III, the oldest standard file format.

An MP3 file is made up of with a series of frames by the combination of a header and data frames. The number of frames means the duration of the audio file. The frames are not autonomous items and cannot be mined in arbitrary manner for frame boundaries. Each header frame take 4 bytes, but in some file takes only 2-byte for Cyclic Redundancy Check, CRC, side information uses 32 bytes for stereo and 17-byte for mono file, and the left frames are for main data and can be in different lengths. The structure of MP3 file is shown in the above figure 2 [2, 5].

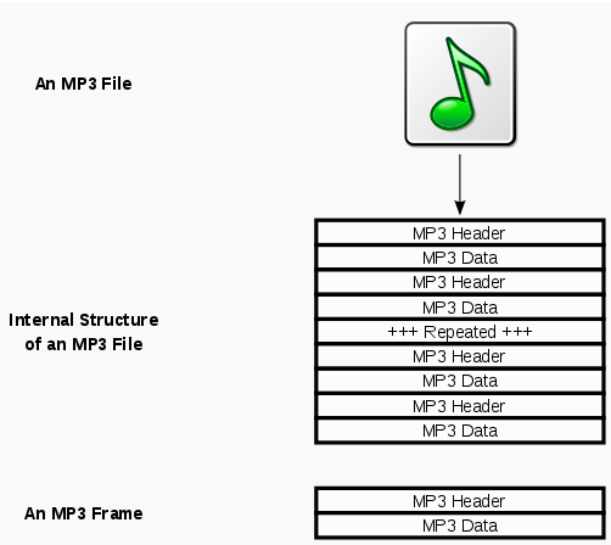

Figure 2: An mp3 file structure

The research works for embedding MP3 audio file after compression techniques can be seen in very little amount. The weakness of the MP3 steganography techniques for expansion in information hiding may result from the small compression rate of audio file. Because the MP3 file is a type of compression file and the size is less than other audio file types, the hiding data in it may not be flexible as other types. There may be the existence of the audio corruption if the secret message is embedded with compression file like mp3. To embed secret message text after compression, there may be two methods: embedding in header frames and embedding in audio data [6].

.

III. LITERATURE REVIEWS

The researchers in [7] compare strength and weakness of the audio steganography techniques as follow in Table 1:

Table 1: Comparison Between different Audio Steganography Techniques.

Technique	Strong point	Week point
Least Significant Bit	1-Simple 2-High bit rate 3-Easier implementation	1. Easy to extract 2. Addition of noise 3.Compression can destroy the data
Parity coding	1. More robust than LSB 2. More choices in encoding the secret bit	1-Easy to extract and destroy
Echo hiding	1-Avoids problem with additive noise 2-Compression of audio will not destroy the data 3-All parameters are set below threshold value of human hearing so echo is not easily resolved	1-Low embedding capacity and security
Phase coding	1. High Robust 2. Effective technique in terms of signal to perceived noise ratio	1-Low Capacity
Spread spectrum	1-Increases transparency 2-Highly Robust	1-Occupies more bandwidth 2-Unprotected to time scale modification
Wavelet Domain	1-High hiding capacity and transparency	1-Extracted data may be loss

Although the various researchers propose the above techniques in their way at mp3 stego techniques, many system continue to find the best way of hidden messages in audio file.

The authors in [8] proposed a work for audio steganographic embedding by using Least Significant Bit, LSB coding analysis. Their main goal is to find an approach for an audio file to be used as a cover channel to embed text information without corrupting the file structure and audio content of the carrier file. They achieved the two principles in successful techniques for steganography; the resulting stego signal from their embedding process is normally the

same with the original audio signal, and the recovered message is correctly decrypted at the side of the receiver.

In [9], the authors proposed a way to achieve robustness, high security and high data rate for embedding text in audio file. The different correspondence method is used for encryption of text and text embedding is applied at the layer of higher LSB. The get with low complexity and the secret message is recovered without an error.

The authors in [10] determine the maximum limit of adding bits and its effects on audio quality based on modified LSB method consisting of LSB+l, LSB+2 and LSB+3. Then, they evaluated by counting steganography capacity, Peak Signal to Noise Ratio, PSNR and Bit Error Rate, BER values. The stated that the size of MP3 cover and secret message absolutely influence of modified LSB method. The bigger MP3 cover size and the smaller secret message size, the less noise will be produced. And vice versa, the smaller the MP3 cover size and the bigger message size, the more noises will be generated.

The work in [11] presented a scheme for hiding data in audio using echo modulation. The information is embedded in an audio sound file by adding an echo into the discrete audio signal. The experiment shows that their method is more security while still remains the inaudibility of stego audio file and appropriate to embed data in audio.

The previous work of [12] proposes a robust steganographic system that embeds high-capacity data in phase spectrum. Their approach is based on the assumption that little changing of selected frequency bins in the phase spectrum can get a smooth transition in the process of preserving phase continuity. They showed that when phase coding can be used, it gives better signal to noise ratio.

The combination of a spread spectrum hiding technique and Shamir's Secret Sharing technique is used for hiding data in audio Mp3 file format is proposed in paper [13]. They described audio quality of stego file after hiding and sharing the data is nearly the same as the original MP3 file with the average value of MSE, i.e., 0.023, and PSNR us 129.426 db.

The authors in [14] proposed embedding encrypted text in cover audio file by using lifting wavelet transform. The number of bits is selected based on the coefficients values to hold the secret data. In this method, text is encrypted based on the size of the message and then concealed in shelter audio file. They stated that acceptable SNR and MSE values are obtained even they made encryption of text and adding of noise.

IV. PROPOSED SYSTEM

The proposed system is based on the combination of Least Significant Bit with the Echo Hiding method in time spectrum. Most of the researches worked only on the Least Significant Bit, LSB or Echo Hiding only and every technique has various strength and weakness. So, an integration technique is proposed and that intends to take the effectiveness of the two techniques and overcome some weakness to enhance the efficiency of MP3 audio file steganography.

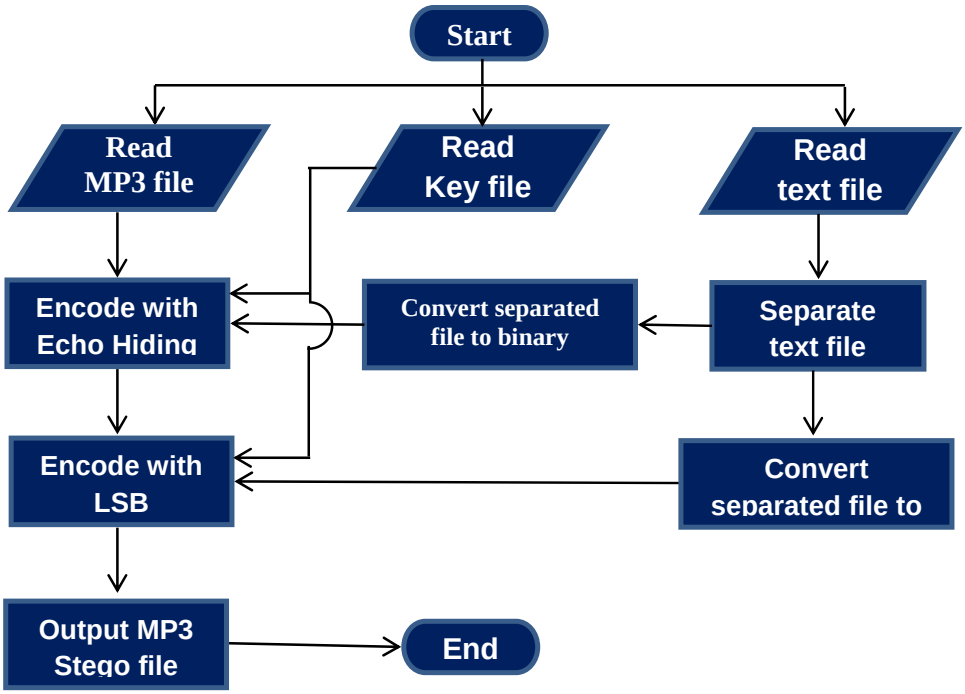

Figure 3: Process Flow Diagram for embedding Text to MP3 file

A. *Least significant bit (LSB)*

Least significant bit, LSB coding can be used to embed secret information in a digital media file. The least significant bit is substituted in each binary message in LSB coding; a large amount of data can be encoded in different ways [15].

B. *Echo Hiding*

Echo hiding is a method of hiding secret message in audio signal, with the binary format without much

dropping in the sound quality at the data rate of about 16bps. The data is embedded in an audio file by adding an echo into the discrete digital signal [15].

C. *Combine Techniques*

The proposed method contains two phase: Embedding and Extracting phase.

1). Embedding Phase

To encrypt the text message into audio file, the mp3 file to use as a cover media, the secret message file and the key file are loaded into the system. Firstly the input secret message is separated into two pieces. As the capacity of the echo hiding is very low and it depends on the time frame, the length of the message for this method is shorter than for the LSB coding method. The shorter message is encoded to the mp3 file using Echo Hiding method firstly in combination with the key file. The stego audio file is again encoded by using the LSB method with the rest message part and key file. Finally the encrypted stego mp3 file is ready for transmission. The detail process for encryption is shown in the figure 3.

2). Extraction Phase

At the extraction process, the stego file is firstly decoded by using LSB method with the help of key file. The encoded message is stored and the stego file is decoded again by using Echo Hiding method. The resulted message is combined with the stored encrypted message to produce the original secret message. The detail process for decryption is shown in the following figure 4.

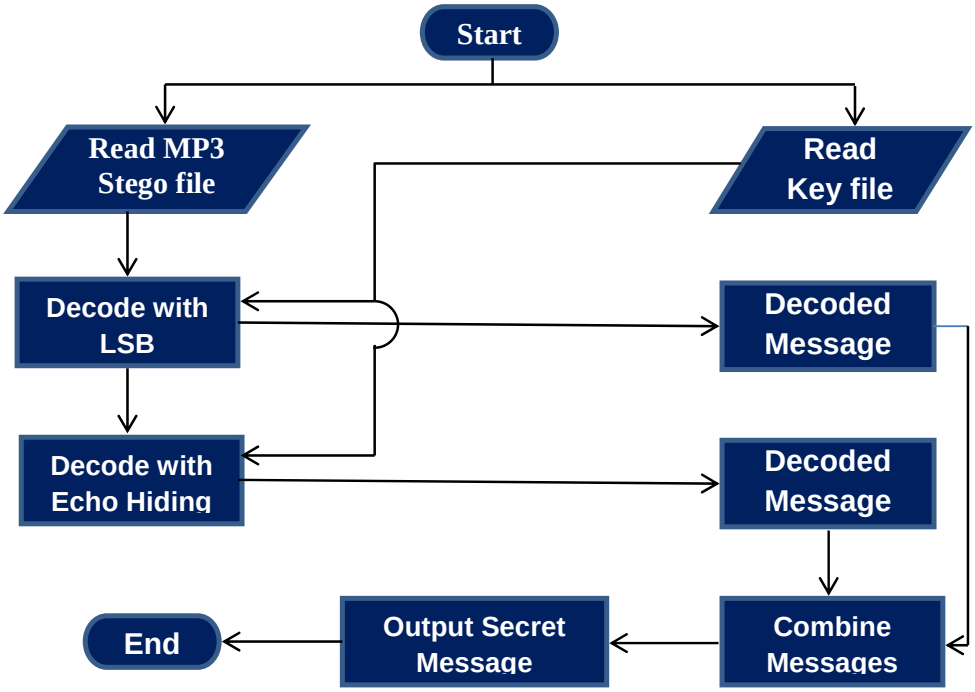

Figure 4: Process Flow Diagram for extracting Text from MP3 file

V. PERFORMANCE MEASURES

A. *MSE*

MSE is defined as the square of error between original audio signal and transmitted audio stego signal. It is used to measure the distortion of the audio signal. It is calculated from the following formula,

$$MSE = \frac{1}{n}\sum_{n=0}^{N}\left(x(n) - y(n)\right)^2$$

Where $x(n)$ denotes cover original audio signal and $y(n)$ represent transmitted stego audio signal.

B. *PSNR*

PSNR is the measurement of the quality of audio signal by comparing original cover audio file with transmitted stego audio file. It can be calculated by using the following formula.

$$PSNR = 10\log_{10}\frac{\sum_{n=0}^{N} x(n)^2}{\sum_{n=0}^{N}[x(n) - y(n)]^2}$$

Where $x(n)$ be the original cover audio signal and $y(n)$ be the transmitted stego audio signal.

C. *CAPACITY*

Capacity is the amount of secret data information that can be embedded within the cover message or cover audio signal.

D. *BER*

BER is the number of decrypted bits of a data stream over a communication channel that has been altered due to noise, interference, distortion or bit synchronization errors.

$$BER(w, w') = \frac{100}{N} \cdot \sum_{n=1}^{N} XOR\left(w(n), w'(n)\right)$$

where *w* is desired bit and w' is retrieved bit [16].

VI. EXPERIMENTAL RESULTS

To carry out the experimental result, different 10 types of genres database is prepared with various bit rates encoding values in MP3 compression: 320 kbps, 128 kbps and 64 kbps. The detail description of the dataset is shown in the following table 2.

The experiments are carried out for LSB method only, for Echo hiding method only and the combination methods by using above dataset. The results for 1kb secret text message under 64kbps are shown in the table 3. In some types of genres, the psnr of combination method is higher than the echo only methods (for example, Classic, Jazz, Country, Reggae and Dancehall). However, the bit error rate is higher.

Table 2: MP3 Test Database

No	Name of Genres	Time (minutes)	Size under 64kbs (mb)	Size under 128kbs (mb)	Size under 320kbs (mb)
1	Classic	1.39	0.495	1.0	1.21
2	Jazz	3.30	1.61	3.23	8.05
3	Country	2.52	1.32	2.65	6.60
4	Reggae	4.27	2.04	4.09	10.21
5	Dancehall	3.30	1.61	3.23	8.06
6	Pop	3.45	1.73	3.46	8.63
7	Rock	3.34	1.64	3.28	8.19
8	R&B	1.37	0.771	1.5	3.74
9	Hip-Hop	3.59	1.83	3.66	9.15
10	DJ Mixes	2.13	1.02	2.04	5.10

The experimental is again tested for different capacity of the proposed method for different genres and the results are shown in the following figures 5, 6 and 7.

Table 3: Steganography Results under 64kbps for 1kb text file

No	LSB Only			Echo Only			Combine ECh+LSB		
	BER	MSE	PSNR	BER	MSE	PSNR	BER	MSE	PSNR
1	0.061035	0.15529	112.5068	0	0.19711	110.4352	3.0041	0.1923	110.6499
2	0.061035	0.37378	104.8771	1.5278	0.55506	101.4426	10.3223	0.5356	101.7527
3	0.061035	0.27609	107.5084	0.62057	0.34775	105.5041	8.5207	0.38457	104.6299
4	0.061035	0.44549	103.3526	0.98315	0.63104	100.3283	5.9339	0.61759	100.5154
5	0.061035	0.39499	104.3978	0.53191	0.67057	99.8005	8.5358	0.60826	100.6477
6	0.061035	0.21491	109.6845	0.53879	0.12842	114.157	7.1989	0.26351	107.9135
7	0.061035	0.27239	107.6256	0.31056	0.39974	104.2939	9.5309	0.41501	103.9684
8	0.061035	0.34378	105.604	0.57947	0.39741	104.3448	9.1987	0.43696	103.5207
9	0.061035	0.35878	105.2328	0.43403	0.34959	105.4583	8.6364	0.45795	103.1131
10	0.061035	0.1708	111.6797	1.9231	0.091073	117.1417	4.4511	0.19833	110.3815

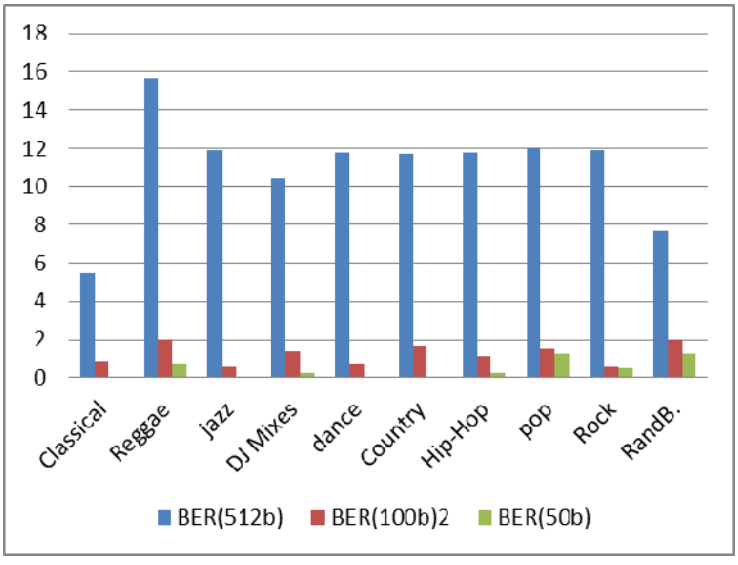

Figure 5: Bit Error Rate for different text size under 64 kbps

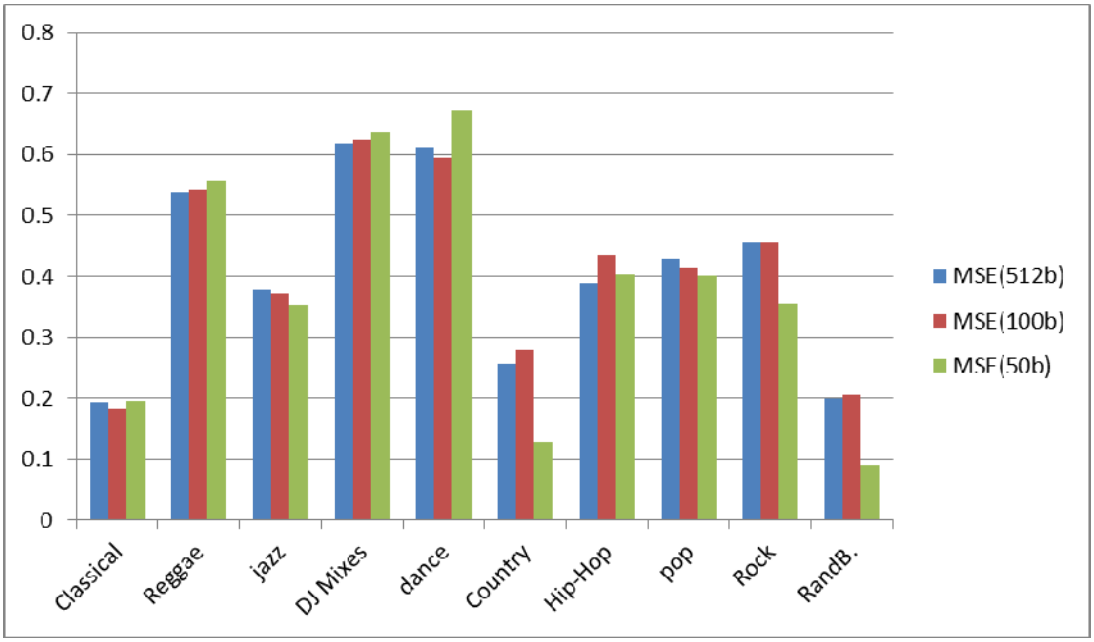

Figure 6: Mean Square Error for different text size under 64 kbps

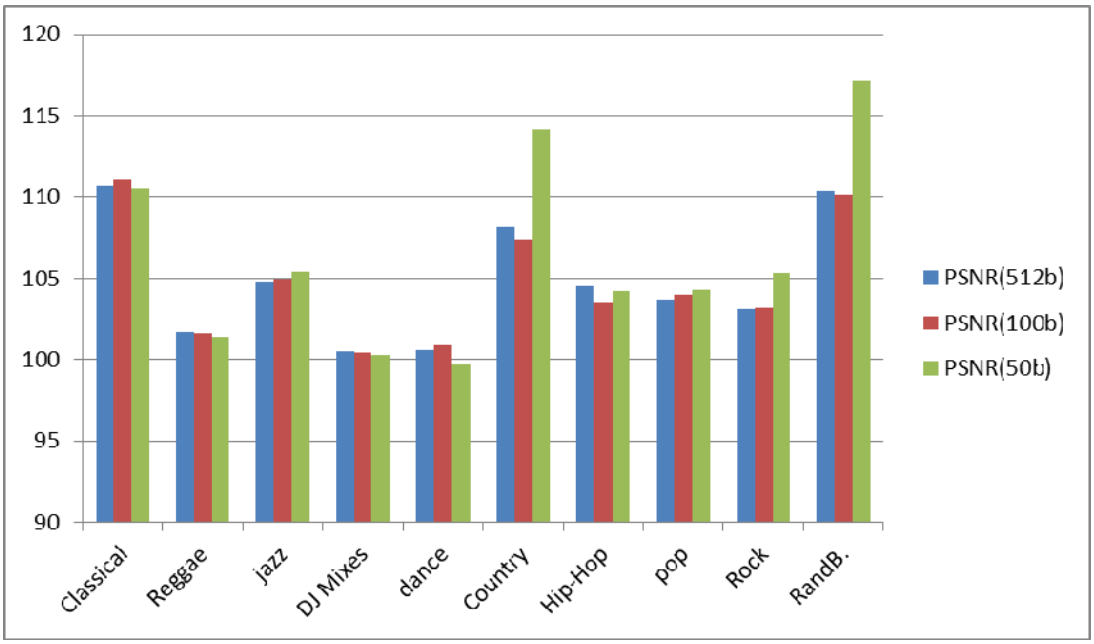

Figure 7: Peak Signal to Noise Ration for different text size under 64 kbps

VII. CONCLUSION

In the proposed technique, the serial integration of LSB and Echo Hiding is developed and extensive results are carried out for different text sizes. The major disadvantage of LSB is cover by the Echo Hiding technique and verse visa the low capacity of echo is overcome by the LSB method. The serial integration can improve the PSNR value in some genre but the consideration of higher BER depend on the integration method and need to be further process to decrease BER rate. The combination method can also increase the capacity of the text file especially in Country and RandB types.

VIII. REFERENCES

[1] L. U. Hasanah and Tito Waluyo Purboyo and Randy Erfa Saputra, “A Review of MP3 Steganography Methods”, International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, pp. 1128-1133, Number 2 (2018)

[2] M. Zamani, A. Bt A. Manaf and S. M. Abdullah, “An Overview on Audio Steganography Techniques”, International Journal of Digital Content Technology and its Applications(JDCTA), Volume6,Number13,July 2012.

[3] K. Yang, X.i Yi, X. Zhao, and L. Zhou, “Adaptive MP3 Steganography Using Equal Length Entropy Codes Substitution”, IWDW 2017, LNCS 10431, pp. 202–216, 2017

[4] M. Zaturenskiy, “MP3 Files as a Steganography Medium”, RIIT 13 Proceedings of the 2nd annual conference on Research in information

technology, Pages 23-28, Orlando, Florida, USA — October 10 - 12, 2013

[5] http://www.wikipedia.com, last accessed on Oct, 2018.

[6] M. S. Atoum, M. M Alnabhan and A. Habboush, "ADVANCED LSB TECHNIQUE FOR AUDIO STENOGRAPHY", Dhinaharan Nagamalai et al. (Eds) : CoSIT, SIGL, AIAPP, CYBI, CRIS, SEC, DMA , pp. 79–86, 2017

[7] M. Tayel, A. Gamal and H. Shawky, "A Proposed Implementation Method of an Audio Steganography Technique", 18th IEEE International Conference on Advanced Communications Technology, Jan 31, 2016 - Feb 3, 2016.

[8] Dr. Aziz Makandar and Vanishree Pattar, " Least Significant Bit Coding Analysis for Audio Steganography", Journal of Future Generation Computing, Vol. 2, No. 3, Mar. 2018

[9] Bahl and 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

[10] R. Indrayani , H. A. Nugrohoand and R. Hidayat, "An Evaluation of MP3 Steganography Based on Modified LSB Method", 2017 International Conferenc on Information Technology Systems and Innovation (ICITSI), ISBN: 978-1-5386-3100-3, October 23 - 24, 2017

[11] H. B. Dieu, "An Improvement for Hiding Data in Audio Using Echo Modulation", The Second International Conference on Informatics Engineering & Information Science (ICIEIS 2013), Nov. 12-14, 2013.

[12] F. Djebbar and B. Ayad, "Audio Steganograpgy by Phase Modification", SECURWARE 2014 : The Eighth International Conference on Emerging Security Information, Systems and Technologies.

[13] N. M. Yoeseph, F. A. Purnomo, B. K. Riasti, M. A. Safiie, T. N. Hidayat , "Steganography on multiple MP3 files using spread spectrum and Shamir's secret sharing", 8th International Conference on Physics and its Applications (ICOPIA), 2016

[14] Deepthi S ,Renuka A. and Hemalatha S., "DATA HIDING IN AUDIO SIGNALS USING WAVELET TRANSFORM WITH ENHANCED SECURITY", Natarajan Meghanathan et al. (Eds) : ITCSE, ICDIP, ICAIT – 2013, pp. 137–146, 2013

[15] H. Kumarl and Anuradha, "Enhanced LSB technique for Audio Steganography", ICCCNT 12 : Third International Conference on Computing Communication and Networking Technologies 2012 :: Karur, Tamilnadu, India, 26-28 July, 2012

[16] P. P. Balgurgi and Prof. Sonal K. Jagtap, "Intelligent Processing : An Approach of AudioSteganography, 2012 International Conference on Communication, Information & Computing Technology (ICCICT), Mumbai, India, Oct. 19-20, 2012.

