Large Information Carrying Capacity Audio Steganography using Sampled MSB

Nensi Rai[1], Prof. Amarjeet Ghosh[2]

[1]M.Tech Scholar, [2]Research Guide

Department of Electronics and Communication Engg., VITS Bhopal

Abstract – Due to the advancement in the technology, sharing of information has also been increased, which is causing the breach in the information being shared among people. So security of information is in demand and keeps on increasing every day. So here in this work some information security methods are being developed which hide sensitive information with an audio piece. The experimental algorithm is enough robust to not to reveal the existence of information hidden with audio to the listener. The experimental outcomes were performed on two different audio lengths and length of the text is larger than the text used in the previous work. So this parameter clearly makes this work stand out among previous works. The figure of merit is PSNR and MSE which shows numerical significance of the work over other previous algorithms.

Keywords – Samples MSB, Steganography, Audio, Large Information Capacity, Security.

I. INTRODUCTION

Data security has gained more attention recently due to the rise in cyber espionage, and the massive increase in data transfer rate over the internet which resulted in more documents being exchanged in digital form. Security of data requires protecting data from access, modification, sharing or even viewing by unauthorized users, allowing only authorized users for such access. Data hiding is an approach that aims to protect data through concealing its existence from adversaries, but this approach needs strengthening to prevent an attacker from access to data in case the existence of hidden data is detected by analytical means.

There are many areas of security technology that deals with the protection of secret data; the most important of these techniques are cryptography and Steganography.

The first technique is cryptography which is referred to as “the study of secret”. It includes encryption and decryption processes, Encryption is the process of converting normal text to unreadable form, where the sender uses an encryption key to encrypt the message to transmit it through the insecure public channel. Decryption is the process of converting encrypted text to normal text in the readable form, thus the reconstruction of the original message is possible only if the receiver has the decryption key.

The second technique is Steganography which is defined as a method of security that hides data among the bits of a cover file, where the secret message is inserted in another medium so that the very existence of the secret message is not detectable. The cover file can be image, audio or video; the most commonly used being the image files, in which unused or insignificant bits are replaced with the secret data.

The Steganography approach relies on hiding secret messages inside innocent- looking messages or documents in order to dissuade the enemy from attempting to find the secret message. However, what if the enemy discovered the secret message and decided on a deception act by changing the secret message in some ways so that to feed the intended recipient with disinformation (disinformation is intentionally false or inaccurate information that is spread deliberately).

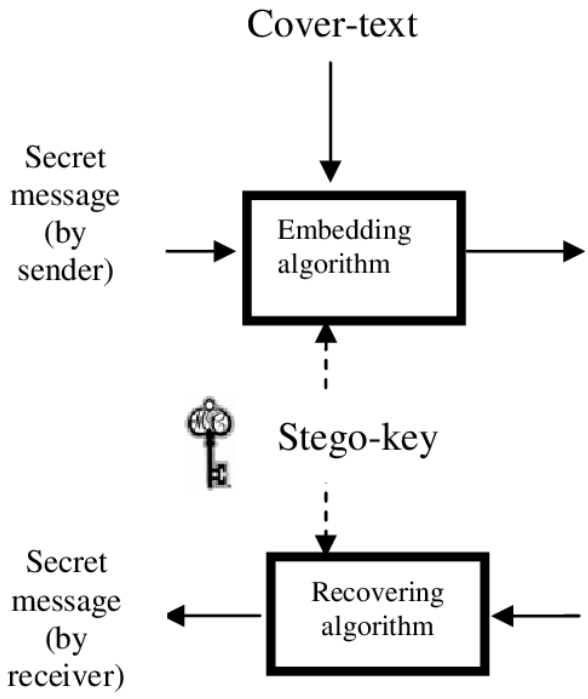

Fig.1.1 Steganographic system mechanism

The aim of this work is to enhance the integrity and security of the hidden secret message. To realize this aim, integrity verification data will be added to the secret data,

so that any alteration to the secret message during transmission between sender and receiver are detected. The added integrity verification data will serve in strengthening of the secret message's secrecy, in case the existence of the secret message is detected.

II. STEGANOGRAPHY MODEL

Steganography is a security technique through obscurity. It is used to communicate, but at the same time, to hide the existence of any communication. Just like cryptography, the purpose is to transmit a message, the content of which must remain secret. But unlike cryptography this isn't accomplished by making the message difficult or impossible to decipher. Instead, steganography makes it hard to detect whether any such transmission was made in the first place.

To achieve this, an innocuous-looking cover object is chosen. Then, to accommodate the secret message, the original, also called the cover, is slightly modified by the embedding algorithm. Thus the so-called stego object is obtained. This embedding procedure must result in very little deviation from the original. The receiving party can, with the prior shared knowledge of where to look, decode the hidden embedded message from the stego object. Should it be intercepted, an eavesdropper would be oblivious to any secret communication taking place.

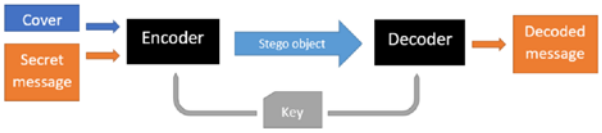

Fig.2.2 A simple model of Steganography

Least Significant Bit Replacement is the most widely used technique for image embedding. This method became very popular due to its easy implementation. It embeds data in a cover image by replacing the least significant bits (LSB) of cover image with most significant bits (MSB) of message image which is represented.

III. PROPOSED SECURITY SYSTEM

In this examination work new approach for secret audio data hiding for an audio file with mp3 and wav format has implemented and simulated in MATLAB. Proposed approach is based on audio Steganography utilizing sampled MSB which enables large data conveying limit and security when contrasted with past base work. Proposed approach avoid embedding data in the consecutive indexes of the audio, which would eventually assist prevent distortion in quality of audio. The input messages taken in text in digital form, and are often treated as bit streams. The location of embedding is chosen based on some numerical calculations that rely upon the data estimation of the digital audio stream. Data embedding is performed by mapping each two-bit of secret message in every one of the seed positions based on the rest of the intensity esteem. The extraction procedure begins with the choice of those seed positions required during embedding. On the receiver end, an alternate reverse operation is performed for extraction of the original data.

Block diagram of the Steganography system with RSA encryption has shown in Fig. 3.1. RSA) encryption method is used to encrypt secret data, transform them into binary sequence bits and hide then in cover audio based on changing the cover audio streams into LSBs.

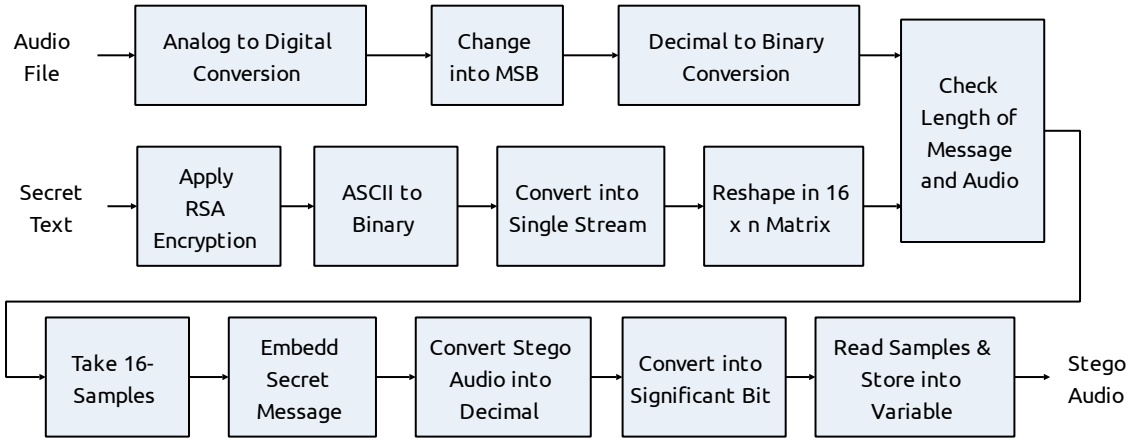

Fig.3.1 Block Diagram of the Steganography System with RSA Encryption.

The text file is encrypted by utilization of RSA algorithm so as to expand the undisclosed secret message security. Encrypted data is filled in the primary frame. It also embeds text file to audio file such as .MP3 file or .wav file. Data is encrypted in bits format by utilization of RSA algorithm to give additional protection to that hid secret messages.

Frame headers of the MP3 are comprised of fields like the copyright bit, private bit, emphasis bit and original bit. However, their utilization is usually precluded in various MP3 players. Such fields are the significant part of frame, which helps the interpretation of data that is concealed in sound signal. They can be appropriately applied to embed

secret massage where they replace the secret message bit stream through the bits in the field.

As shown in Fig.3.1 encryption of audio file in RSA first it converted in to digital format using an analog to digital converter. Than it is changed to most significant bit MSB. Now this bit streams are converted in to binary. Parallaly secret text has taken to embed in audio RSA encryption is applied on it. Then encrypted ASCII text is converted in to binary and again in to single streams. Reshape these streams in to Matrix form of 16 X n. Now both audio and text are prepared to embed. Check length of both audio and text. 16 samples are taken to embed secret message and converted stego audio in to decimal. Convert the stego file in to significant bits. Read sample and store in to variable to get stego output from proposed system.

The extraction system is just reverse to embedding process as shown in Fig. 3.2. Take a stego audio to extract original information and convert analog stego in to digital. Change it in to most significant bits. Apply decimal to binary conversion to convert it into binary. Take 16 samples and convert ito decimal. Read secret message extracted from stego. Reshape matrix 8 times convert ASCII into character using ASCII to character conversion. Apply SRA decryption to decrypt message. Finally secret text has extracted from stego.

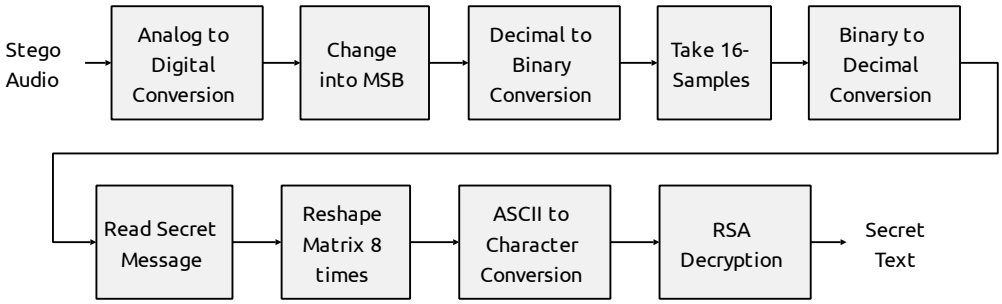

Fig.3.2 Block Diagram of the Extraction System with RSA Decryption

Process flow of both encryption and decryption process has shown in Fig. 3.3 and 3.4 respectively. Fig. 3.3 shows the Fig. flow chart of the Steganography process with RSA encryption and Fig 3.4 shows the flow chart of the extraction process with RSA decryption.

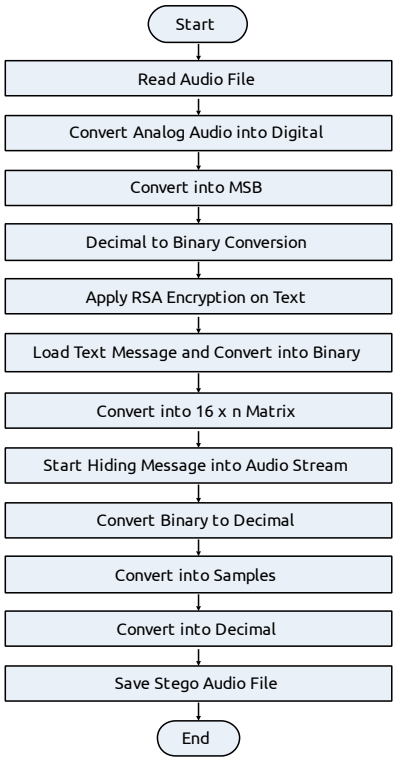

Fig.3.3 Flow Chart of the Steganography Process with RSA Encryption

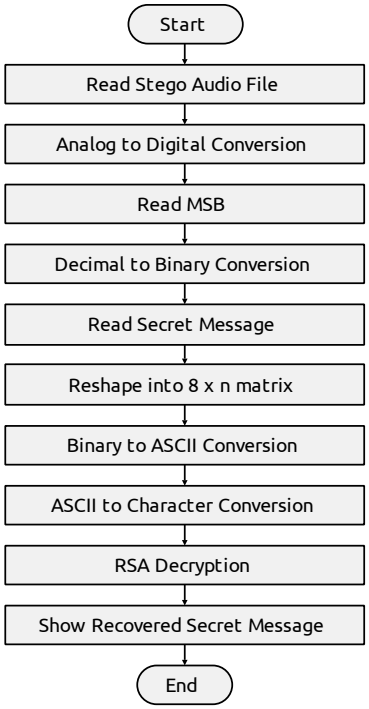

Fig.3.4 Flow Chart of the Extraction Process with RSA Decryption

IV. EXPERIMENTAL OUTCOMES

To analyze the performance of proposed algorithm and verification. Simulation of proposed work has done in MATLAB simulation environment. Fig.4.1 shows the GUI of proposed audio Steganography system with input audio audio1.wav (~12 KB).

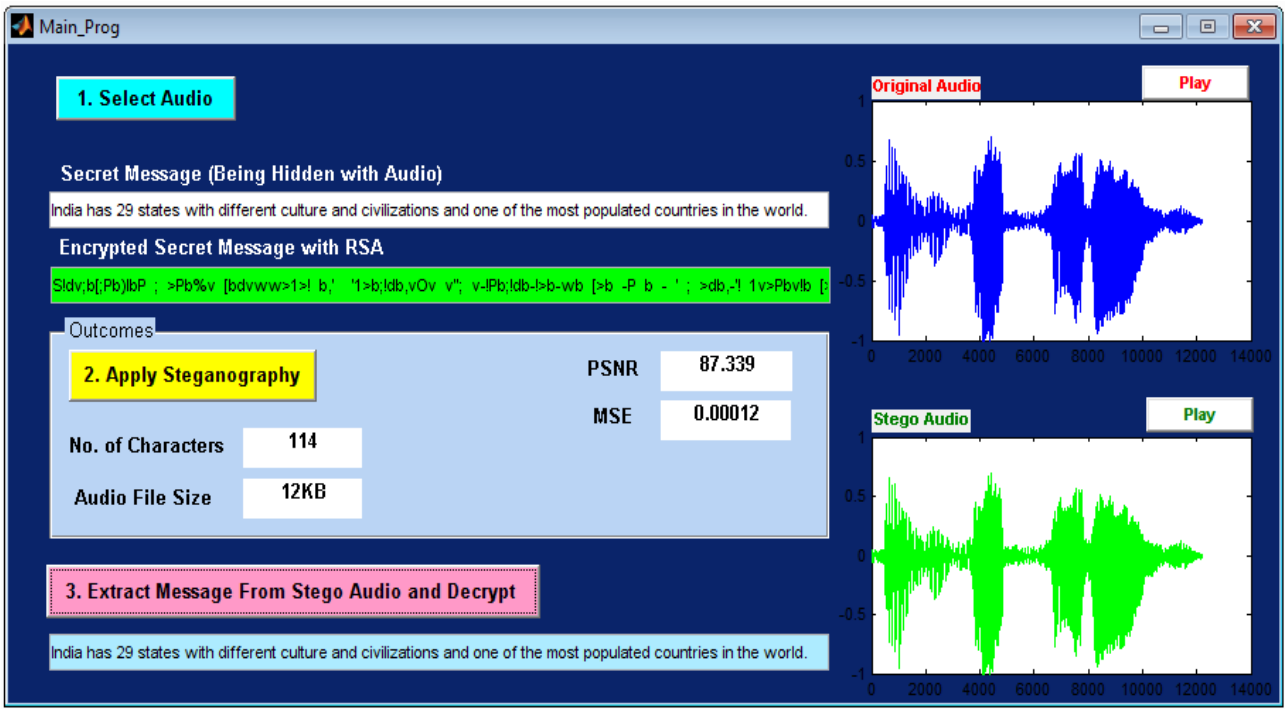

Fig.4.1 GUI of Proposed Audio Steganography System with input audio ***Audio1.wav (~12 KB).***

Fig.4.2 shows the GUI of proposed audio Steganography system with input audio audio2.wav (~82 KB). The performance of proposed algorithm has been validated based on its PSNR (dB), MSE calculation. Table 1 shows the comparison of parameter (PSNR and MSE) for two different audio files Audio1 MP3 and Audio2 wav file. from the comparative analysis of proposed work with existing work it is examined that proposed work has better performance it terms of PSNR and MSE as compared to previous work.

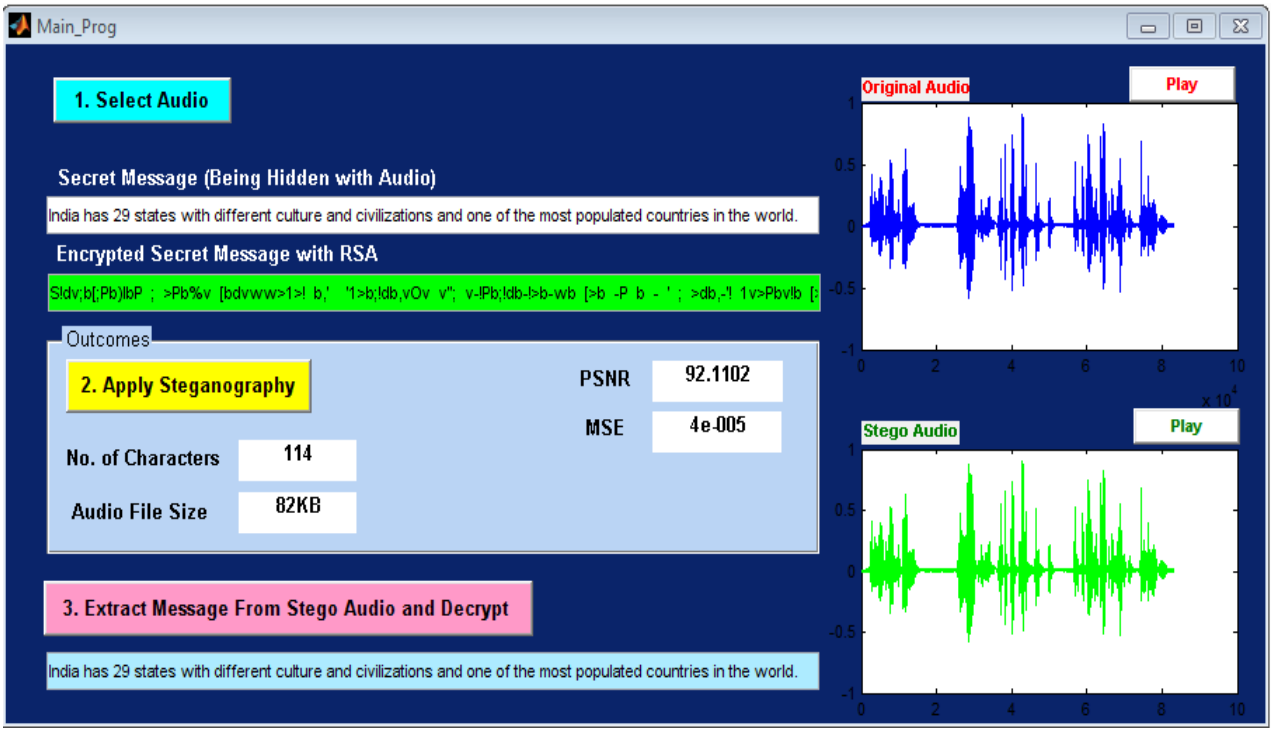

Fig.4.2 GUI of Proposed Audio Steganography System with input audio ***Audio2.wav (~82 KB)***

Table 1: Comparison of Parameter (PSNR and MSE)

Name of Audio File	*Audio File Size*	*Text Information Characters Length*		*PSNR (dB)*		*MSE*	
		Previous	*Our*	*Previous*	*Our*	*Previous*	*Our*
Audio1.wav	12 KB	14	114	61.051	87.339	7×10^{-3}	1.2×10^{-4}
Audio2.wav	82 KB	14	114	70.766	92.110	2.7×10^{-3}	4.0×10^{-5}

Graphical representation of results of previous and proposed work has shown in Fig.4.3 and Fig.4.4 in the form of a bar chart. In Fig.4.3 shown graphical comparison of PSNR and in Fig. 4.4 shown graphical comparison of MSE.

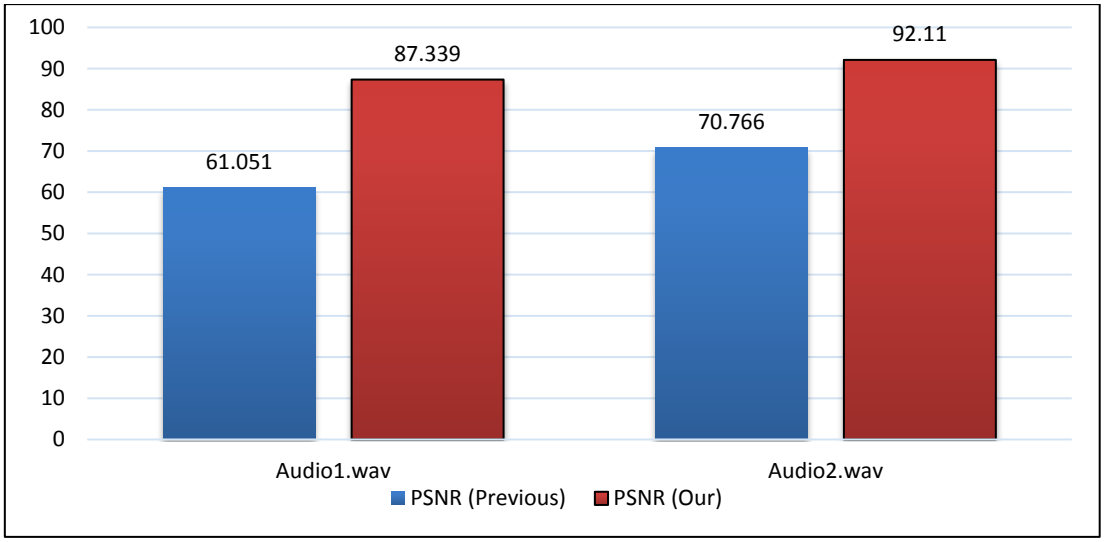

Fig.4.3 Graphical Comparison of PSNR

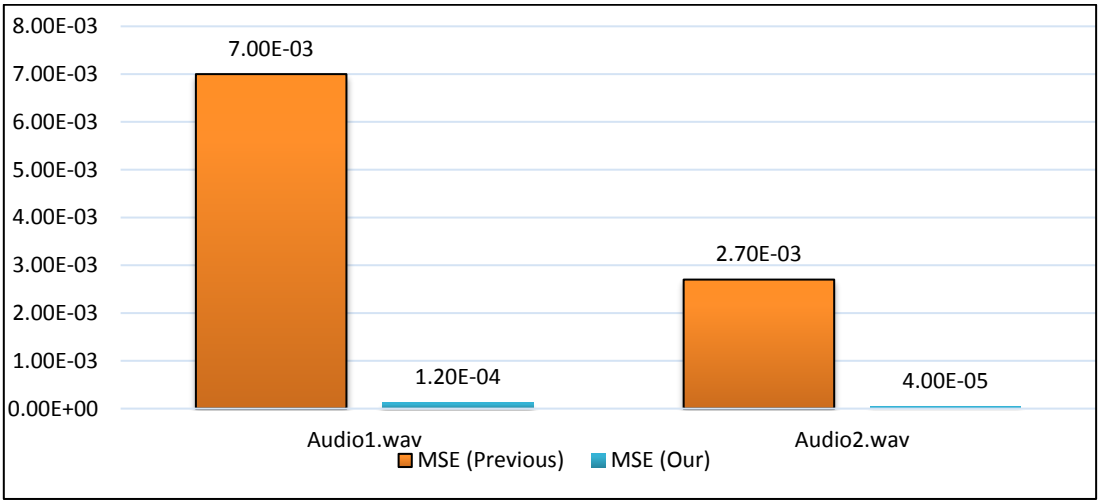

Fig.4.4 Graphical Comparison of MSE

V. CONCLUSION AND FUTURE SCOPES

This work introduces the implementation of large information carrying capacity audio Steganography using sampled MSB algorithm using MATLAB platform to solve the low security and capacity problems of the traditional used LSB techniques, which do not provide a step for encrypting data, and if secret message is sequentially or randomly embedded and attackers know this pattern of embedding the message, they can obtain the message. In proposed algorithm RSA encryption has been used to provide additional security of information. To verify proposed approach a simulation based verification has completed in this work in MATLAB simulation environment. In order to validate two different audio file are taken in mp3 and wav format and a text message is taken to embed in it and also extracted message from stego to verify system. For the comparative analysis of proposed work with existing approach two parameters are taken PSNR and MSE. The comparative analysis of proposed

work with previous work shows that proposed work has better PSNR and MSE performance. Results of the hiding part illustrate that the Peak Signal to Noise Ration results of the proposed method are better than those of the traditional LSB for all genre names and all used secret messages.

This work can be enhanced in the future based on applying it in hiding more secret messages and adding other types of noises. Also proposed approach open a way toward video Steganography and seeking other alternatives of encryption also to study the effect of compression ratio on the performance of PSNR.

REFERENCES

[1]. S. Teotia and P. Srivastava, "Enhancing Audio and Video Steganography Technique Using Hybrid Algorithm," 2018 International Conference on Communication and Signal Processing (ICCSP), Chennai, 2018, pp. 1059-1063.

[2]. R. S. Phadte and R. Dhanaraj, "Enhanced blend of image steganography and cryptography," 2017 International Conference on Computing Methodologies and Communication (ICCMC), Erode, 2017, pp. 230-235.

[3]. P. K. Sethy, K. Pradhan and S. K. Behera, "A security enhanced approach for video Steganography using K-Means clustering and direct mapping," 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT), Pune, 2016, pp. 618-622.

[4]. A. Singh and H. Singh, "An improved LSB based image steganography technique for RGB images," 2015 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), Coimbatore, 2015, pp. 1-4.

[5]. C. R. Geetha and C. Puttamadappa, "Enhanced stego-crypto techniques of data hiding through geometrical figures in an image," 2015 2nd International Conference on Electronics and Communication Systems (ICECS), Coimbatore, 2015, pp. 116-122.

[6]. S. Dagar, "Highly randomized image steganography using secret keys," International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014), Jaipur, 2014, pp. 1-5. doi: 10.1109/ICRAIE.2014.6909116].

[7]. P. Yadav, N. Mishra and S. Sharma, "A secure video steganography with encryption based on LSB technique," 2013 IEEE International Conference on Computational Intelligence and Computing Research, Enathi, 2013, pp. 1-5.

[8]. Malviya Swati, Dr Anubhuti Khare, Manish Saxena "Audio Steganography by Different Methods". In proceedings of International Journal for Emerging Technologies, Advanced Engineering ISSN- 2250-2459- Volume 2, Issue- 7 (2012)).

[9]. Khan, Mohammad Kamran "Distributed Least Significant Bit technique for data hiding in images" in proceedings of Multitopic Conference (INMIC) 2011 IEEE 14th International. IEEE, 2011.

[10]. HS. Anupama "Information Hiding uses Audio Steganography- a Survey" in proceedings of International Journal on Multimedia and Its Applications (2011).

[11]. K Sherly A P and Amritha P "A Compressed video Steganography using TPVD",in proceedings of International Journal for Databases Management Systems Vol.2.3 August,2010.

[12]. Dutta Poulami, Debnath Bhattacharya & Tai,hoon Kim- "Data hiding in audio signal-A review." In proceedings of International journal of databases theory and application 2.2 (2009).

[13]. Amr A Hanafy Gouda I Salama and Yahya Z.Mohasseb "A Secure Covert Communication Model Based on Video Steganography,"in proceedings of Military Communications Conference 2008.

[14]. Keio University Yokohama, japan, May 20-22-2009 NSC97-2221-E-468-006 International-conference on computational, intelligence, multimedia application 2007.