Robust and Efficient Reversible Audio Steganography using MSB Scheme with Higher Length of Secret Message

Vinita Bhimte[1], Prof. Jeetendra Singh Yadav[2]

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

Department of Computer Science and Engg. Bhabha Engineering and Research Institute, Bhopal

Abstract - Communication of secret data is a basic factor in the field of information technology that keeps on making challenges with expanding levels of complexity. At the point when communication establish between parties that are situated on the same secure network, these difficulties can be considered as sensible. The security of the information is first and foremost need while transmitting from one place to another place or stored somewhere. Though, in the cutting edge generation desires are that one can travel across the world and get secret information in the meantime without imperiling the confidentiality of secret information. In these circumstances where the involved parties are spatially separate, the security of secret information cannot depend all in all on the trend setting innovations of secure networks, and extra security components ought to be incorporated. Steganography empowers to hide messages inside a multimedia file like image/video/Audio document with the end goal that the very existence of the message is unknown to third party. Cryptography is used to encrypt the data so that it is unreadable by a third party. Such techniques will facilitate various secret information sharing strategies. From the outcomes it is also clear proposed technique has no effect on audio quality even after information hiding.

Keywords - Audio, Speech, Reversible, Steganography, Secret Information

I. INTRODUCTION

Information is shared globally through the Internet, in digital form. There are issues and challenges regarding the security of information in transit from senders to receivers. The major issue is the protection of digital data against any form of intrusion, penetration, and theft. The major challenge is developing a solution to protect information and ensure their security during transmission. Three components of information security are confidentiality, integrity, and availability. Confidentiality ensures that information is kept secret from any unauthorized access. This could be done through information hiding techniques, namely cryptography and steganography.

Cryptography involves the act of encryption and decryption of a digital data. The major weaknesses of such techniques are that even though the message has been encrypted, it still exists. Steganography dwells on concealing any digital data in an innocuous digital carrier, the word steganography is derived from an old Greek word which means covered writing.

The term Steganography is adapted from the Greek word steganographia, meaning “covered writing” and is taken in its modern form to mean the hiding of information inside other information. Naturally these techniques date back throughout history, the main applications being in couriering information during times of war.

With the invention of digital audio and images files this has taken on a whole new meaning; creating new methods for performing “reversible data hiding” as it is often dubbed. This has many possible applications including the copyright watermarking of audio, video and still image data. In digital media, Steganography is mainly oriented around the undetectable transmission of one form of information within another. In order for a data hiding technique to be successful it must adhere to two rules:

- The embedded data must be undetectable within its carrier medium (the audio or image file used). The carrier should display no properties that flag it as suspicious, whether it is to the human visual/auditory system or in increased file size for the carrier file.
- The embedded data must maintain its integrity within the carrier and should be easily removable, under the right circumstances, by the receiving party.

The existing system of Audio Steganography poses more restrictions on the choosing of audio files. User can select only wav files to encode. Further embedding information into sound files is generally considered more difficult than images; according to the human ear is extremely sensitive to perturbations in sound and can in fact detect such turbulence as low as one part in 10 million. The four methods discussed further provide users with a large amount of choice and makes the technology more accessible to everyone.

II. AUDIO STEGANOGRAPHY

As audio techniques have been developed for audio streaming on the Internet for radio stations for example but then incorporated into social networking and communication applications such as Skype. Online gaming is also big user of audio channels on the Internet. Using the TCP/IP protocol, audio files can be uploaded, downloaded, and transmitted through the Internet. This benefit of transmission makes “the interest in using audio data as cover object in steganography” become much stronger. There are many types of audio formats differentiated by encoding algorithms, proprietary design, compression algorithms, and standardized formats. Each type of audio format makes data embedding and steganalysis with different requirements.

Audio steganography as it is said is a form of technology that uses audio files as cover media to hide secret information for communication purpose. The key function in audio steganography is funding a proper method to embed information either a text file or another audio file into the cover media. The major assessment criteria of embedding methods are the trade-off between payload and visibility.

a. Embedding Methods in Audio Steganography

There are huge challenges for data hiding in technical applications. For example, any embedded data in the host signal are likely to be removed or modify by compression algorithms. The key of successfully embedding data in audio steganography is to find the holes that are not possible for exploitation by compression algorithms. Consequently, the experts in steganography use embedding methods that are commonly found in everyday logic algorithms.

b. Least Significant bit Encoding

The simplest embedding method in audio steganography is low bit encoding, commonly known as the least significant bit encoding. In image steganography the LSB of grey value of each cover image pixel is replaced with corresponding message bit to generate the stego image.

c. Phase Encoding

Phase encoding embedding algorithm is based on the phase encoding technique which embeds data in the phase spectrum of the frequency domain signal of the audio media.

d. Echo Encoding

Echo encoding is a steganography embedding technology to hide information in audio media. Unlike least significant bit encoding that could give 100% recovery; echo encoding algorithms usually had lower recovery rat forensic investigations.

III. PROPOSED METHODOLOGY

In this work a robust and efficient reversible audio steganography using MSB scheme with higher length of secret message has been implemented and simulated in MATLAB. Least significant bit coding is the easiest method empowers to encode data inside a digital audio file. A huge amount of information can be considered to embed in LSB technique by substituting least significant bit of each sampling point of information with a binary message similarly for MSB information is encoded by substituting most significant bit of each sampling point of information with a binary message.

It performs bit level control to encode the message. The accompanying advances are

a. Receives the digital audio file as bytes and changed over in to bit pattern.

b. Each character in the message is changed over in bit pattern.

c. Replaces the MSB bit from audio with MSB bit from character in the message

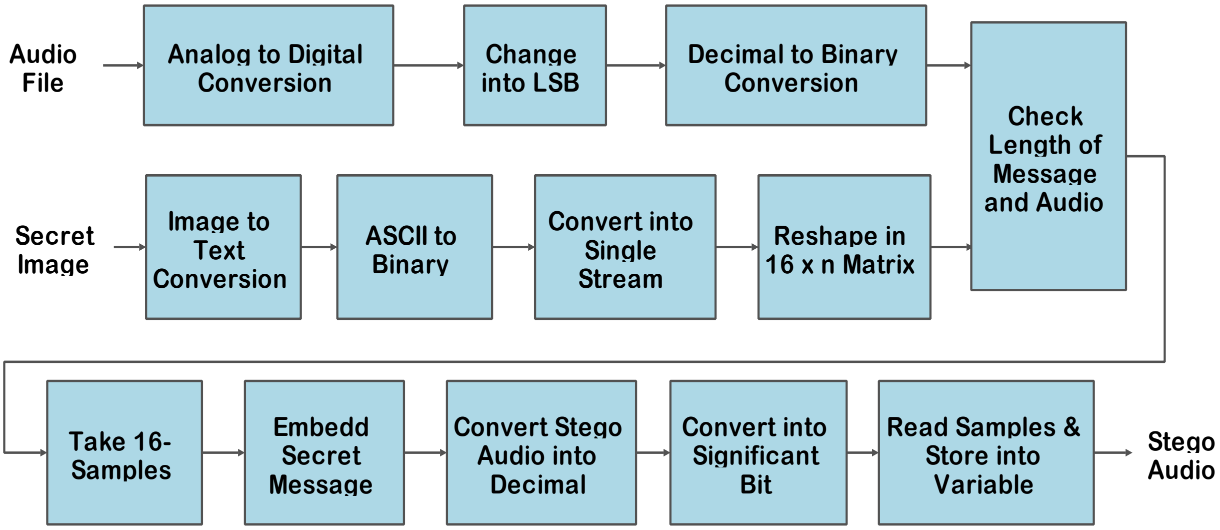

Audio File
Analog to Digital Conversion
Change into LSB
Decimal to Binary Conversion
Check Length of Message and Audio
Secret Image
Image to Text Conversion
ASCII to Binary
Convert into Single Stream
Reshape in 16 x n Matrix
Take 16-Samples
Embedd Secret Message
Convert Stego Audio into Decimal
Convert into Significant Bit
Read Samples & Store into Variable
Stego Audio

Fig. 3.1 Block Diagram of Embedding Process.

The data transmission rate in LSB coding is 1 kbps per 1 kHz in a few experimental examination of LSB coding. However, the two LSB of an example are supplanted with two message bits. This expands the measure of information that can be encoded yet additionally builds the measure of coming about clamor in the sound document also. Therefore, one ought to consider the signal content before settling on the LSB task to utilize. For instance, a sound document that was recorded in a clamoring metro station would cover low-bit encoding commotion.

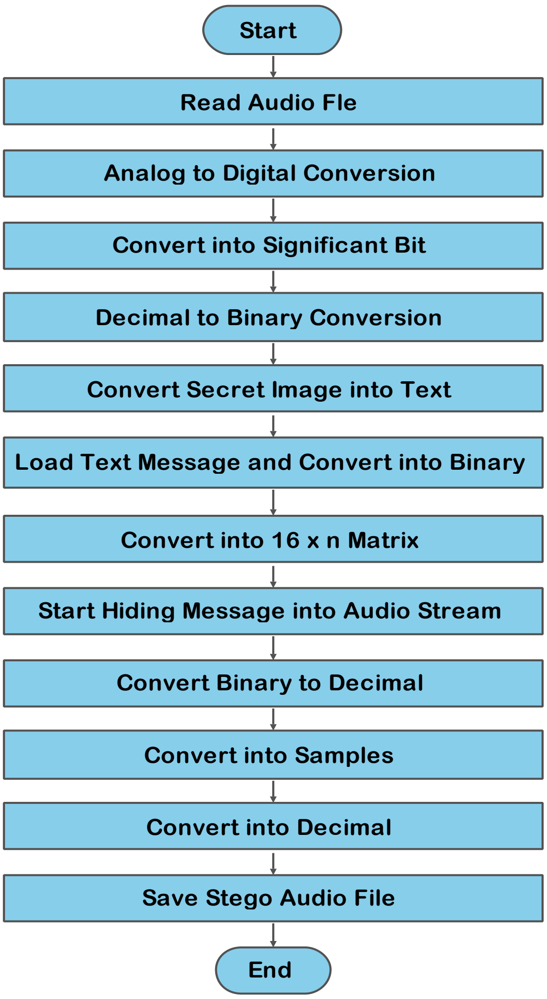

Start
Read Audio Fle
Analog to Digital Conversion
Convert into Significant Bit
Decimal to Binary Conversion
Convert Secret Image into Text
Load Text Message and Convert into Binary
Convert into 16 x n Matrix
Start Hiding Message into Audio Stream
Convert Binary to Decimal
Convert into Samples
Convert into Decimal
Save Stego Audio File
End

Fig. 3.2 Flow Chart of Embedding Process.

Both the input cover and the Message are MP3 files. In this work, the secret message is validated and preprocessed based on implementing. In the embedding process, both the audio file and secret image files are processed to offer a Stego Object (SO). After that, the reversible LSB method is used to embed the secret message in the cover. In the process of extracting, the stego object is then prepared to separate the message file. Figure 3.1 demonstrates the block outline of embedding procedure of proposed algorithm and comparing stream of proposed inserting process is appeared in Fig. 3.2.

To get stego audio data embedding of data has completed in two diverse ways simultaneously, as shown in Fig. 3.1 audio file is provided in proposed algorithm, the audio file is converted in digital format using ADC converter. Change it into LSB. Further decimal digital information is coded into the form of binary data. Along with the audio data secret image is processed in Matlab the secret image is converted in the form of text and in binary equivalent of ASCII text. Then binary transformed texts are converted to single stream. Reshape in $16 \times n$ matrix check length of message and audio. Take 16 samples to embedded secret message. Convert stego audio into decimal. Convert into significant bit and read its samples and store into variable. End of the day embedded stego audio has achieved.

Decoding process looks through the hidden bits of a secret message into the LSB of the pixels inside a cover picture utilizing the arbitrary key. In decoding algorithm the arbitrary key must match i.e. the irregular key which was utilized in encoding should coordinate in light of the fact that the arbitrary key sets the concealing purposes of the message in the event of encoding. At that point recipient can extract the inserted messages precisely utilizing just the stego-key.

In a second phase at the receiver end an information extraction system has been designed to retrieve data from stego audio. Fig. 3.3 shows block diagram of extraction process.

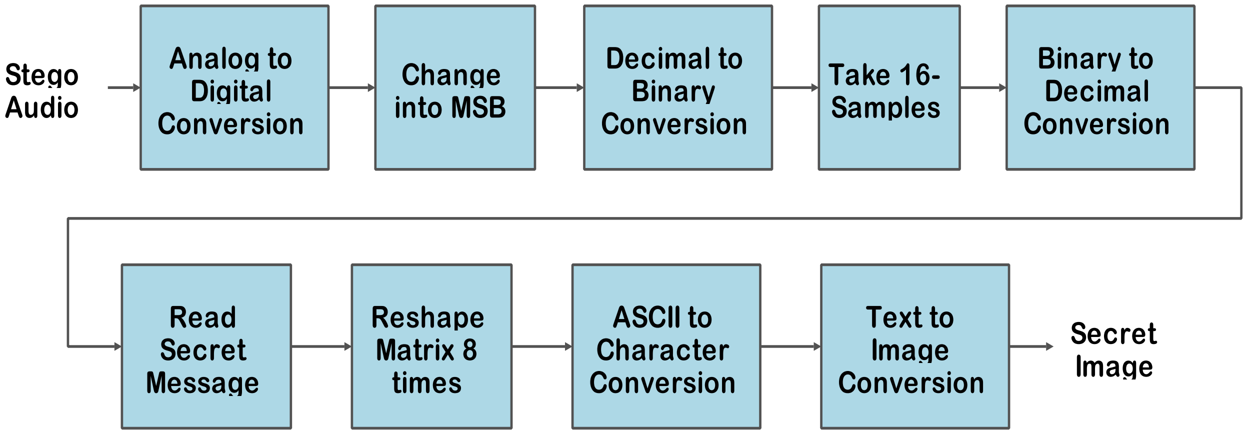


Fig.3.3 Block Diagram of Extraction Process

In extraction process stego audio is processed through the ADC conversion system. Change converted signal into MSB and convert it to its equivalent binary form. Take 16 sample of binary data and convert it into decimal form.

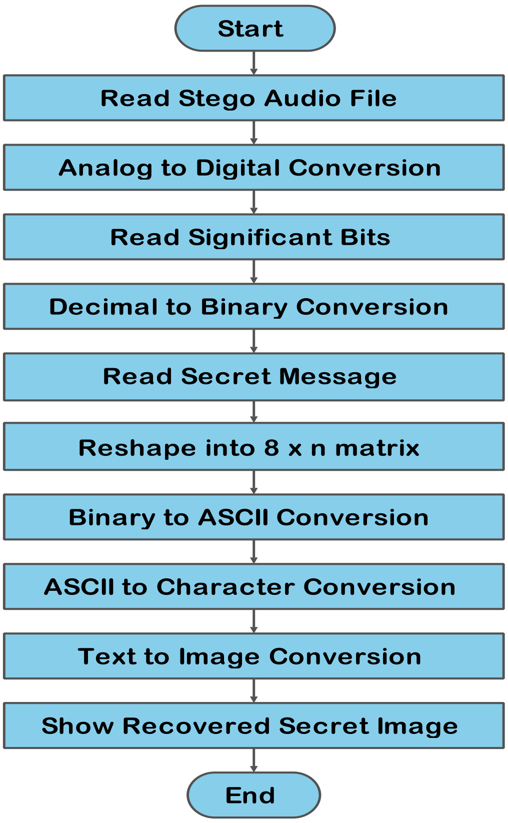

Start
Read Stego Audio File
Analog to Digital Conversion
Read Significant Bits
Decimal to Binary Conversion
Read Secret Message
Reshape into 8 x n matrix
Binary to ASCII Conversion
ASCII to Character Conversion
Text to Image Conversion
Show Recovered Secret Image
End

Fig.3.4 Flow Chart of Extraction Process.

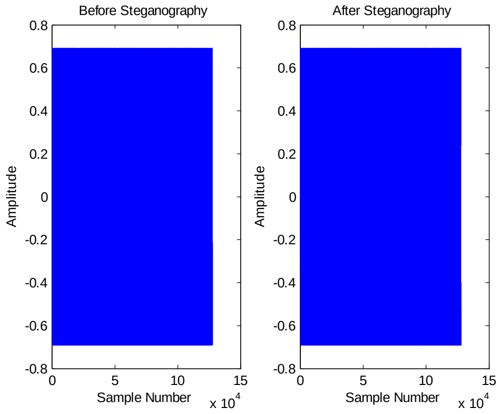
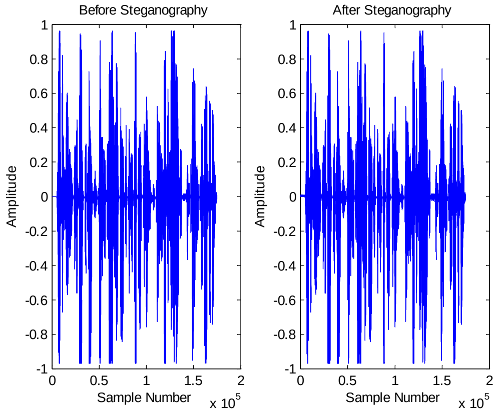
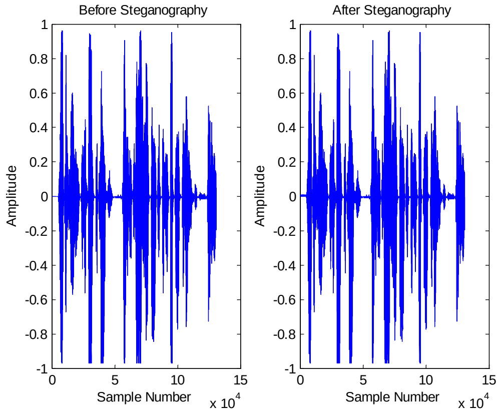
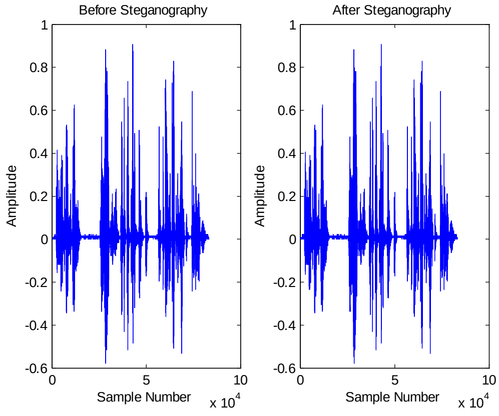
Read secret message embedded in secret audio. Reshape new matrix 8 times. Convert ASCII values to its equivalent character and convert stream of text to image to obtain secret image embedded. Fig. 3.4 shows the flow chart of proposed algorithm.

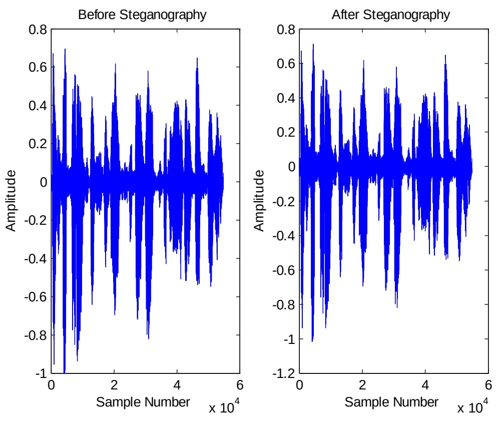
As an execution measure for image distortion because of hidding of message, the outstanding peak-signal-to noise ratio (PSNR), which is sorted under distinction distortion measurements, can be applied to stego images performance evolution of proposed work has been carried out based on PSNR performance of proposed methodology.

IV. SIMULATION OUTCOMES

Implementation and simulation of proposed robust and efficient reversible audio steganography using MSB scheme with higher length of secret message has completed in Matalb Simulation environment. The conducted work in this research aims to design an effective audio steganography technique to find a solution for the security problem previous techniques. In addition, it offers an efficient method to hide audio information in more secured way with the use of the MATLAB program.

Table 1 Audio file and its corresponding waveform.

Audio File Size	*Waveforms*
254954	
172616	
128985	
82756	

54026	

Secret messages are hidden in various cover messages using improved techniques. In this work hiding of secret messages in covers messages to compare the current technique with the previous base work. It can be clearly seen that the PSNR results of the proposed method are better than those of the previous method. The developed technique in this work also outperforms previous methods in terms of PSNR values for embedding the second secret message. The enhancement between the current method and the previous methods for the cover messages are shown in the table 2. Table 1 shows the size of various audio file size and its corresponding waveforms used in this examination.

Table 2 shows the comparative analysis of proposed work with respect to previous base work in terms of secret message size and corresponding PSNR value recorded for a fixed audio file size. Fig. 4.1 shows the comparison chart of proposed work with existing work. It is clearly visible in chart that proposed work has better performance as compared to previous work.

Table 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)*
254954	100	50.67	941	102.49
172616	100	39.43	941	58.69
128985	100	68.25	941	57.42
82756	100	40.31	941	54.75
54026	100	42.60	941	44.83

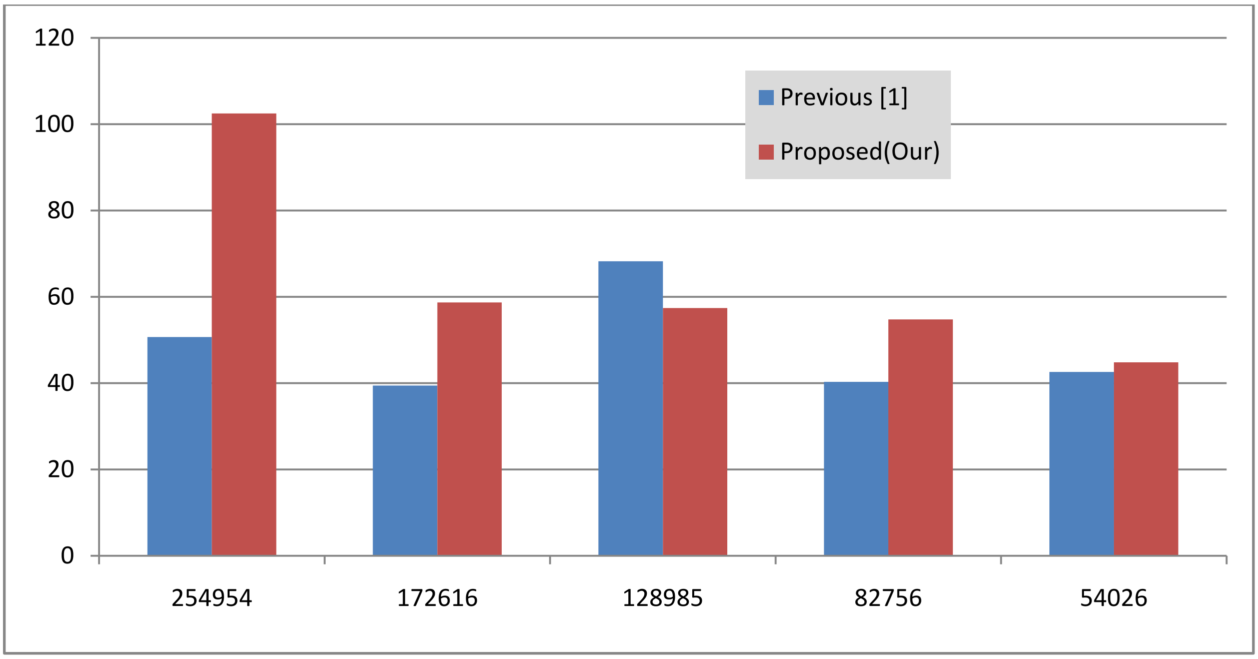


Fig. 4.1 PSNR Comparison Chart.

V. CONCLUSION AND FUTURE SCOPE

This work reported the implantation a robust and efficient reversible audio steganography using MSB Scheme with higher length of secret message to solve the low security and capacity problems of the previous approach, which do not provide a step for encrypting data. In addition, the validation of proposed code is stored in the stego object. Therefore, proposed technique is developed in this work to solve those problems and offer an efficient method to hide audio information in more secured way with the use of the MATLAB environment.

The proposed algorithm includes three main phases; embedding and extracting and message validation. In the first phase, the main purpose is to improve the security of messages to be hidden in an audio file. In the second stage, the proposed algorithm is designed for audio files to solve the security issue of the previous technique and to provide efficient security.

This work can be enhanced in the future based on applying it in hiding more secret messages and adding other types of noises. Different parameters can be added in order to get high PSNR or to improve message integrity.

REFERENCES

[1] H. Lin, R. Xie and L. Wei, "Density, distance and energy based clustering algorithm for data aggregation in wireless sensor networks," 2017 IEEE/CIC International Conference on Communications in China (ICCC), Qingdao, 2017, pp. 1-5.

[2] K. Rajeswari and S. Neduncheliyan, "Genetic algorithm based fault tolerant clustering in wireless sensor network," in IET Communications, vol. 11, no. 12, pp. 1927-1932, 8 24 2017.

[3] Venkatesh, C. S. Sengar, K. R. Venugopal, S. S. Iyengar and L. M. Patnaik, "RRDVCR: Real-time reliable data delivery based on virtual coordinating routing for Wireless Sensor Networks," 2016 2nd IEEE International Conference on Computer and Communications (ICCC), Chengdu, 2016, pp. 2227-2234.

[4] G. C. Vanarotti, U. M. Kulkarni and H. H. Kenchannavar, "Ferry based data gathering in Wireless Sensor Networks," 2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), Bangalore, 2016, pp. 165-170.

[5] D. V. Pushpalatha and P. Nayak, "A Clustering Algorithm for WSN to Optimize the Network Lifetime Using Type-2 Fuzzy Logic Model," 2015 3rd International Conference on Artificial Intelligence, Modelling and Simulation (AIMS), Kota Kinabalu, 2015, pp. 53-58.

[6] H. Tran-Dang, N. Krommenacker and P. Charpentier, "Localization algorithms based on hop counting for Wireless Nano-Sensor networks," 2014 International Conference on Indoor Positioning and Indoor Navigation (IPIN), Busan, 2014, pp. 300-306.

[7] Gurpree Sigh Chhabra and Dipesh Sharma (2011) Cluster-Tree based Data Gathering in Wireless Sensor Network. International Journal of Soft Computing and Engineering, Vol. 1, Issue 1.

[8] Hani Alzaid, Ernest Foo and Juan Gonzalez Neito and DongGook Park (2011) Secure Data Aggregation in Wireless Sensor Networks, Emerging Communications for Wireless Sensor Networks, InTech.

[9] 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.

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

[11] De-Shuang Huang, Kang Li and George William Irwin (2006) International Conference on Intelligent Computing: Computational Intelligence. Germany: Springer-VerlagBerlin, ISBN 3540372741,