A REVIEW ON AUDIO STEGANOGRAPHY

[1]C. H. Kamesh Rao, [2]Mrs. Jaspal Bagga

Department of Electronics and Telecommunication Engineering
Sri Sankaracharya Tecnical Campus Bhilai Chhattisgarh India

Abstract- A **technique, in which readable form of secret message is converted to an unreadable form to keep the secret message undetectable easily by the any unauthorised access or adversary, is known as cryptography. Cryptography means simply jumbling sequence of original message or altered the sequence of message. Cryptanalysis is the technique at which the secret message is converted from unreadable format to readable format without knowing the techniques how they were converted from readable format to unreadable format. Audio steganography, where the audio file (.wav) file is used for the secret data embedding. Audio signal bits are modified with the secret bits as imperceptible manner.**

Keywords**: Steganography, Identification, Audio, Rotational**

I. INTRODUCTION

Audio steganogaphy are correct medium provide for high data rate transmission & high level of redundancy (Abdulaleem, Azizah, Akram, 2012). A text steganography is considered as a difficult type of steganography because of having low degree of redundancy in text compared to the image, audio & video. Redundancy means the bits which can be easily altered whit out modified the quality of original signal.

II. LITERATURE REVIEW

Aarti Mehndiratta, 2015 presents a paper for different steganographic techniques and the basic knowledge of the encryption and decryption techniques based on symmetric and asymmetric cryptography. The steganography techniques are DCT, DWT & the encryption techniques are RSA and DES .DCT transform a cover signal from spatial domain to frequency domain[1]. The one of the disadvantage of DCT is it works only with the JPEG format for cover image file. DWT transform the special domain information to the frequency domain information's. The DWT divides the signal into high frequency coefficient and the low frequency coefficient. Cryptography techniques RSA & DES are used for the data encryption which provides high level of security and robustness.

Mahmood Maher Salih, Mudhafar Al-Jarrah, 2015 proposes new Bi-LSB techniques over the traditional LSB technique. The technique is tested with AWGN attack before extraction of secret data. The PSNR value decrease due to the attack of AWGN noise. PSNR & MSE value is calculated here for the data checking the quality for the different different cover file. The result shows obvious degradation in the PSNR values is directly related to the noise increase value.

Satish Singh Verma, Ravindra Gupta, Gaurav Shrivastava, 2014 presents a new type of technique for data hiding in audio carrier .taking the secret data and encrypted this data by simple techniques and XORing. This XORed bits are now embedded into the detailed coefficient of audio carrier. This technique gives the overall SNR 25% & stego signal output SNR 35% .the author uses the DWT technique for high data embedding capacity and the improved SNR ratio over the conventional DWT technique. This technique is little bit complex then traditional techniques.

Nishu Gupta, Mrs.Shailja, 2014 shows a new technique at which the data is firstly encrypted and then after it is encrypted by using DES algorithm. After the encryption process the encrypted data is embedded into the cover media. This enhances the security of secret message. But this technique till have some attack from unauthorised access. Hashing function is used maintain the confidentiality of information

Uma Mehta, Mr.Daulat Sihag, 2014 presents technique over the traditional LSB techniques. At this technique data must be encrypted by using blowfish algorithm which is much better than DES and RSA algorithms. The techniques provide the level of security of encrypted message form adversary. Blowfish algorithm takes lots of time to trying to reconstruct the original message & provides level of security. By using the audio file & image some part of message is hidden into the audio and some part is hidden into the image & also hashing function is applied. The receiver has to do decryption of message and applied hashing function too. The only problem with this technique is the several attacks which can affect the original message.

Rohit Tanwar, Bhasker Sharma, Sona Malhotra, 2014 presents a new robust substitution technique over the traditional substitution technique. The traditional technique having the disadvantage and having some attack of adversary problems. First problem is Low robustness against intentional attacks which try to reconstruct the hidden message & the second one is Low robustness against distortions with high average power (unintentional attacks). The new approach presented here is the data of secret message is hidden into the 3rd & 4th LSB of the cover signal. In proposed method currently uses 2 bits per byte of audio sample. The technique uses the deeper layer of cover signal to hide the secret message. The proposed techniques use the reveal of traditional substitution techniques.

V.Lokaswara Reddy, A.Subramanyam, P.Cheena Reddy, 2013 uses the both the means of cryptography and steganography. Here the RSA algorithm is used for data encryption & after the traditional LSB technique is used for data embedding into cover medium. The cover medium can be an image, audio & video .by using the technique, security level of message and the embedding capacity into the cover signal also increase. But in here the problem is to when sharing a key this must be shared by the protecting means.

Deepthi S.1, Renuka A.2 and Hemalatha S., 2013 propose a wavelet domain technique for hiding the secret message. The secret message is embedded into the coefficient of the audio cover file. Here the wavelet uses the advantage of the lifting wavelet scheme. The technique gives good SNR & MSE values but the technique have drawback of taking lots of time for the embedding & the extraction process.

Ronak Doshi, Pratik Jain, Lalit Gupta, 2012 presents discussion about the text steganography, image steganography, audio steganography & video steganography .Described each medium & the applications of steganography. The author shows here that the steganography is an easy use function & the secured data is difficult to detect. But here the steganography technique still has some steganalysis techniques to reveal the original message.

Swati Malviya, Krishna Kant Nayak, Manish Saxena, Anubhuti Khare, 2012 presents a literature of different digital steganographic techniques & their methods. Steganography is used for imperceptibility of data .Those techniques are discussed by author & among all techniques LSB technique has more payload, robust & provides transparency then others techniques. The other techniques having some disadvantages like low capacity, increased bandwidth & low robustness.

Masoud Nosrati, Ronak Karimi, Mehdi Harir, 2012 presents a survey on the latest approaches for audio steganography. Modifying Quantized Spectrum Values of MPEG/Audio Layer III techniques involves modification of some quantized spectrum values of audio layer III to embed secret information into audios is done & having the capacity 6 times larger than other. Embedding data between frames in MP3 file method uses the space between frames of mp3 file & along with some cryptography technique is used for data encryption for increased security. Quantized frequency domain embedding and reversible integer transforms domain uses these classical unitary transforms with quantization in the transform domain to embed the secure data and other In the integer domain they look at the binary representation of the integer coefficients and embed the secure information as an extra bit. Integer Transform based Secure Audio Steganography (ITSAS), uses a reversible integer transform to obtain the transform domain coefficients. The QSAS algorithm has low embedding capacity but much better SNR values. The ITSAS algorithm is taken as it is reversible, simple and efficient with acceptable SNR values.

Preety Jain,Vijay Kumar Trivedi, 2012 they taking a reference of the paper (Haider Ismael Shahadi,2011) having the embedding capacity of up to 42% of cover audio and SNR 50 db. They proposed a technique based on wavelet packet transform for hiding the data using HAAR wavelet for decomposition of cover signal with the traditional LSB. They represent techniques for data hiding in the real time scenario and expected that these techniques uses to secure the secret data from others.

S.S. divya, m. Ram Mohan Reddy, 2012 presented two novel methods of substitution technique of audio steganography which improves the capacity of cover audio for embedding additional data. By checking the MSB's of the samples, and then number of LSB's for data hiding is decided. This method can utilize up to 7 LSB's for embedding data or for encryption and decryption the RSA algorithm is used here. This technique was tested with the sampling frequency of 44,100 hz audio file represented 16 bit per sample. This method calculated the PSNR, increase capacity & the MSE valencues. By using this technique the data embedded capacity were increased. These are very simple techniques and embedded text into audio & hidden text recovered without any error.

Prof. Samir Kumar Bandyopadhyay1 and Barnali Gupta Banik2, 2012 represented a multilevel steganography by sending two secret messages on a single cover object. In this paper two level securities were presented by using the techniques LSB modification and parity encoding. At first level the text message embedded into the audio cover file & generates a stego file. After first encryption this stego file used as a cover file for next secret message & generates another stego file. This final stego file contains both the secret message. The advantage of this method is provides the two level security of message & output stego object is decoded with difficulties which makes this method successful to hide data from adversary

S.S. divya, m. Ram Mohan Reddy, 2012 presented two novel methods of substitution technique of audio steganography which improves the capacity of cover audio for embedding additional data. By checking the MSB's of the samples, and then number of LSB's for data hiding is decided. This method can utilize up to 7 LSB's for embedding data or for encryption and decryption the RSA algorithm is used here. This technique was tested with the sampling frequency of 44,100 hz audio file represented 16 bit per sample. This method calculated the PSNR, increase capacity & the MSE valencues. By using this technique the data embedded capacity were increased. These are very simple techniques and embedded text into audio & hidden text recovered without any error.

Prof. Samir Kumar Bandyopadhyay1 and Barnali Gupta Banik2, 2012 represented a multilevel steganography by sending two secret message on a single cover object. In this paper two level security were presented by using the techniques LSB modification and parity encoding. At first level the text message embedded into the audio cover file & generates a stego file. After first encryption this stego file used as a cover file for next secret message & generates another stego file. This final stego file contains both the secret message. The advantage of this method is provides the two level security of message & output stego object is decoded with difficulties which makes this method successful to hide data from adversary.

Abdulaleem Z. Al-Othmani, Azizah Abdul Manaf and Akram M. Zeki, 2012 represents survey of existing data hiding techniques ,functions ,advantages and disadvantages for real time audio signal. Some common techniques used for data hiding is described here like LSB coding, parity coding ,phase coding ,spread spectrum coding and echo hiding coding. In LSB technique allows more data to be embedded but sometimes when taking some more data at the last two LSB bits it may become quite risky

for security of message. By using parity coding technique the cover signal is breaks into separates areas of sample & at the parity but of its sample the data of message signal is embedded. Only the disadvantage of this technique is its weakness about robustness. Another method like phase coding the message signal is embedded at only the phase of the cover signal so it's having very low capacity. Spread spectrum technique spread the message bits over the entire cover medium at frequency function as the maximum no of bits can be embedded. But only the problem with it is increasing in bandwidth. One of another technique echo hiding is a technique at which the message is embedded as an echo. The technique having a disadvantage of complexity. This paper represents the benefits and limitations for the all given techniques.

Ashwini Mane., Gajanan Galshetwar., Amutha Jeyakumar, 2012 shows a simple and robust technique for speech hiding in audio cover medium by the bit insertion technique. The technique uses the sampling frequency of 3000 sample/second at which each sample have 8 bits. The paper represents a comparison of actual cover file and stego cover file at which the very small amount of difference is shown which can not be heard by the ears. The security is maintained here by using key.

Nagaseshu .K, Srinivasa Rao.V , Hima Deepthi.V, 2011 presented one techniques at which the secret key is shared by the sender and receiver and DES algorithm is used for the data encryption. After the encryption the data is hidden into the lower nits of the cover file. This technique gives the 35% high embedding capacity over the conventional method which gives only 15% of embedding capacity into cover medium. But here the header file are not modified because of it contains some sensitive information. This creates some problem for embedding technique.

Jayaram P, Ranganatha H , Anupama H, 2011 represents many simple steganogrphy techniques and their works & limitations. The techniques which described here is LSB, parity, phase, spread spectrum and echo hiding technique. Parity coding and spread spectrum coding have problem with the HAS and robustness. Phase coding has limitation of low data rate transmission. The paper introduced a robust technique for data hiding in audio at which is adversary cannot get the idea for the secret data within cover file.

Zaidoon Kh. AL-Ani, A.A.Zaidan, B.B.Zaidan and Hamdan.O.Alanazi, 2010 provides the knowledge of the general steganography system, stegnograohy type, characteristics and the classifications .it presents three types of steganography pure, secret key &public key steganography. At where the message is encrypted without any key called pure steganography. When the same key is used for the encryption &decryption the technique is called secret key steganograohy & when the two different key is used for encryption and decryption the technique is called public key steganography. Here described the 6 types of steganography system like substitution, spread spectrum, transform domain, statically, distortions and cover generation techniques. The simple substitutions technique uses data hiding into the LSB part of the cover signal. Transfer domain system refers to hide the secret message into the either frequency domain or time domain system. Spread spectrum technique uses the secret message must be hidden into the frequency domain but its increases the bandwidth of the occupied channel. Statistical technique utilize the fact that when the 1 is embedded into the cover file this must be modified the statistical characteristics of the cover signal can be observed by the receiver .Cover generation technique provides when secret information is added to a specific cover by applying an embedding algorithm. The paper simply gives the overview of the all steganogrphy technique and weakness. Weakness of substitution technique is it is low robust. In the transform domain system also attack can be simply apply by using digital signal processing .Spread spectrum technique requires more time and also having complexity. Cover generation technique is also heavy and complex technique.

Mazdak Zaman, Azizah Bt Abdul Manaf, Rabiah Bt Ahmad, Farhang Jaryani, Hamed Taherdoost, Akram M. Zeki, 2009 shows two problems of the traditional substitution methods .these two problems are First problem having low robustness against attacks which try to reconstruct the hidden message and second one is having low robustness against distortions with high average power. And it gives one new algorithm for overcome of these two problems the genetic algorithm .by using genetic algorithm the bits can be embedded into the inner layer of the cover file and provides high level of security and robustness.

.

III. CONCLUSION

These Different different techniques for data encryption & the data hiding technique have been studied. DWT technique is studied with its characteristics & it applied for data security more than others techniques..

REFERENCES

[1] Jain AK, Bolle R, Pankanti S. Biometrics: personal identification in network society. Kluwer Academic Publishers; 1999

[2] Manisha Rana & Rohit Tanwar (2014). Genetic Algorithm in Audio Steganography. International Journal of Engineering Trends and Technology (IJETT) – Volume 13 Number 1 – Jul 2014.

[3] Aarti Mehndiratta (2015). Data Hiding System Using Cryptography & Steganography: A Comprehensive Modern Investigation. International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056 Volume: 02 Issue: 01 | Apr-2015 p-ISSN: 2395-0072.

[4] Mahmood Maher Salih & Mudhafar Al-Jarrah (2015). Secret Message Integrity of Audio Steganography Using Bi-LSB Embedding. IJCSNS International Journal of Computer Science and Network Security, VOL.15 No.7, July 2015.

[5] Arfan Shaikh, Kirankumar Solanki, Vishal Uttekar & Neeraj Vishwakarma (2014). Audio Sreganography And Security Using Cryptography. International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 2, February 2014).

[6] Gaurav Singh,Kuldeep Tiwari & Shubhangi Singh (2014).Audio Steganography using RSA Algorithm and Genetic based Substitution method to Enhance Security. International Journal of Scientific & Engineering Research, Volume 5, Issue 5, May-2014 ISSN 2229-5518.

[7] Nagasehu .K, Srinivasa Rao .V , & Hima Deepthi .V (2011). A Novel Approach for Embedding Text in Audio to Ensure Secrecy. Nagaseshu.K et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (4) , 2011, 1592-1594 ISSN: 0975-9646.

[8] Satish Singh Verma, Ravindra Gupta & Gaurav Shrivastava (2014). A Novel Technique for Data Hiding in Audio Carrier by Using Sample Comparison in DWT Domain. 2014 Fourth International Conference on Communication Systems and Network Technologies.

[9] M. G. Jafari & M. D. Plumbley (2011). Fast Dictionary Learning For Sparse Representations Of Speech Signals. IEEE J. Sel. Topics Signal Process., vol. 5, no. 5, pp. 1025–1031, Sep. 2011.