iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** VI **Month of publication:** June 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

SRWD Technique for Security Enhancement of Audio Steganography

Deepa Verma[1], Mr. Pushpendra Singh[2]
[1]M.E. Student,[2] Assistant Professor
[1,2]Department of Electronics and Telecommunication Engineering
[1,2]Chhatrapati Shivaji Institute of Technology Durg, Chhattisgarh India

Abstract: ***From the past few years with progression in era of information society and their related applications are becoming more and more popular. Attacks can occur due to system vulnerabilities or user misuse or program defects. Attackers can also combine multiple security vulnerabilities into an intelligent attacking system. Therefore, an efficient security technique is needed to secure secret data over the network system. Here's many of approaches have been proposed in to enhance the security of secrete data but each of them has its own limitation. These limitations require some new technique for data security in audio signal. This paper presents a new semantic steganography technique for more robust, efficient and perceptible audio steganography. This paper presents a novel audio steganography method using SRWD for undetectability of data in audio steganography. Our experimental values illustrated in terms of SNR & PESQ.***
Keywords- Cryptography, Steganography, secret message, SRWD, SNR, PESQ, HAS.

I. INTRODUCTION

Cryptography is a technique in which readable form of secret message is converted to an unreadable form to keep the secret message undetectable easily by simply jumbling sequence of original message or altered the sequence of message. Steganography stands for the cover writing. Steganography comes from Greek word stegano and garphy at where staganos means 'cover or protected' & graphin means 'drawing or writing'. Steganography is used for concealing the existence of secret message within the cover file. A secret file can be anything i.e. text, image, audio & video. Steganography is normally uses the features of cryptography. Hiding a message with Steganography methods reduces the chance of a message being detected from the adversary or unauthorised access & enemy. Terms used in steganography:

A. Cover Signal- Cover signal is an innocent signal at which the secret information is embedded called cover signal. Cover file can be any text, image, audio and video.
B. Stego file- The file which obtained after the secret message is embedded into the cover signal called stego signal.
C. Stego key- Key is used for provide more security for the secret message. This key is optional during the encryption & decryption process. \

II. LITERATURE SURVEY

Aarti Mehndiratta 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. 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.

Rohit Tanwar, Bhasker Sharma, Sona Malhotra 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.

Haider Ismael Shahadi and Razali Jidin presents a paper which gives high capacity and high stego-signal quality audio steganography scheme based on DWPT and bits block matching. Here's that message can be embedded up to 42 of the total size of

©IJRASET: All Rights are Reserved

the cover audio signal with at least of 50 dB signal to noise ratio.

Preety Jain,Vijay Kumar Trivedi they were 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 use to secure the secret data from others.

Soodeh Ahani, Shahrokh Ghaemmaghami, and Z. Jane Wang present speech steganography method using discrete wavelet transform and sparse decomposition to provide high security of secret data. This paper presents the highest signal quality of cover signal after the secret data is embedded. The paper shows the comparatively analysis of audio steganography according to their embedding time, extraction time and stego signal quality

III. PROBLEMS IN EXISTING AUDIO STEGANOGRAPHY TECHNIQUES

There are three main issues in designing a speech steganography method: undetectability, imperceptibility, and capacity [5]. Another problem is Human Auditory System is more sensitive than the human visual system & its is very easily detect the problem create by the noise in the process of steganography .so the data embedding into the audio signal is also a very difficult task because of HAS. The problem only with the any techniques of steganography is, its low robustness against the eavesdropper or enemy or attacker. The secret data should be unintelligible for the adversary.

IV. THE PROPOSED WORK

This section proposes a technique which shows the combination of sparse representation based wavelet domain (SRWD) is used for the audio steganography process. Here sparse reparation will be use for hiding the secret data. The work with Proposed technique will be with the increase capacity & also with the provide transparency, imperceptibility & undetectibility from adversary or eavesdropper.

In this propose algorithm the secret data will be hidden into the into the frames at where whose energy of frame is higher than specific threshold**.** Here the low frequency wavelet sub band will be sparsely represented & it is used for the embedding. the secret information over the non –zero coefficient of the low frequency wavelet sub band

& the high frequency wavelet sub band will be use.

The propose technique will concern several terms which are:

A. Discrete Wavelet Transform - Discrete wavelet

transforms the spatial domain function to the frequency domain function. Wavelet transforms gives the exact partition of the high frequency & the low frequency information. From these two frequency transform one is used for data embedding.

B. Sparse Representation - Sparse representations

of signal represents signal as a linear combination of atoms, at which most of the coefficients are zero. Sparse representations are used for the image processing image processing, audio processing, biology, and document analysis. Sparse decomposition of signal represents that its a linear combination of some structural element called atom & these atoms collectively form a dictionary.

V. EXPERIMENTAL VALUE

In the SRWD technique at the high & low frequency sub-band are sparsely presented. In our proposed technique only the low frequency non-zero coefficients are used for data embedding. The execution is fast & this also gives the better stego signal quality .the value of SNR is for frame length 16 is obtained 39.25.In general the PESQ measurement is between 0.5 and 4.5, where a higher score denotes a better quality. The other aspects of audio steganography shown in below figure.

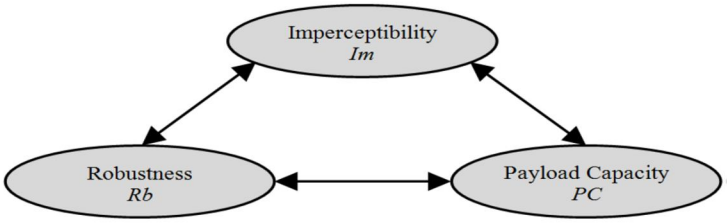


Fig1.Steganography Requirements

©IJRASET: All Rights are Reserved

Volume 5 Issue VI, June 2017
ISSN: 2321-9653

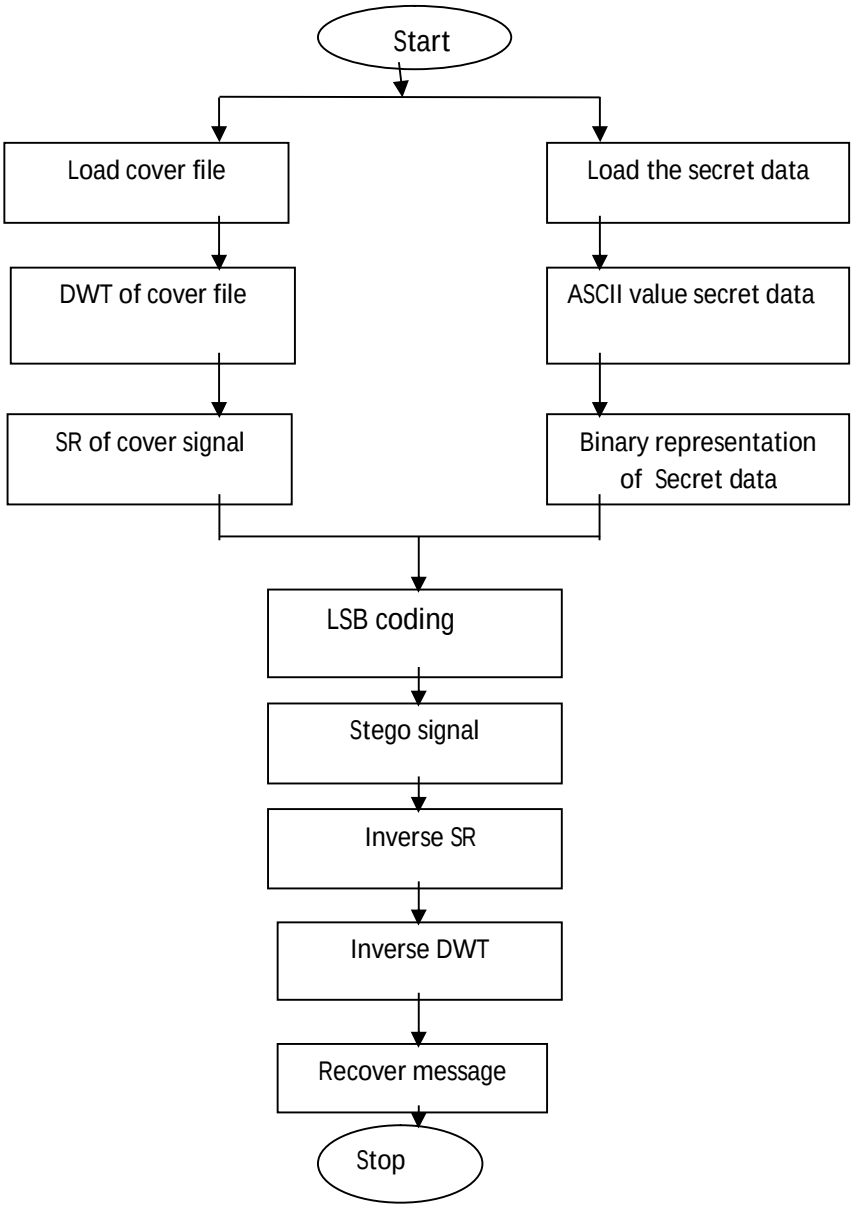


Fig2. Flow Diagram of SRWD Audio Steganography

VI. CONCLUSION

All the technique presented today have problem with relevant to the transparency of stego signal, capacity, robustness of data & the imperceptibility from the eavesdropper. This paper shows literature survey of some paper. Apart from these, here need of new technique which fulfils the three aspects of audio steganography transparency, imperceptibility & capacity. So here proposes a technique SRWD technique for obtaining a high capacity, perceptually transparent audio steganography which will be calculate in terms of SNR & PESQ values. This technique will surely work against attack, provides good stego signal quality & increases capacity also.

REFERENCES

[1] Aarti Mehndiratta, "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.

[2] Rohit Tanwar, Bhasker Sharma & Sona Malhotra , "A Robust Substitution Technique to implement Audio Steganography", 2014 International Conference on Reliability, Optimization and Information Technology ICROIT 2014, India, Feb 6-8 2014.

[3] Preeti Jain & Vijay Kumar Trivedi , " A Novel Technique for Data Hiding in Audio by Using DWTS", IJCEM International Journal of Computational

©IJRASET: All Rights are Reserved

Engineering & Management, Vol. 15 Issue 4, July 2012 ISSN (Online): 2230-7893.

[4] Soodeh Ahani, Shahrokh Ghaemmaghami, & Z. Jane Wang, "A Sparse Representation-Based Wavelet Domain Speech Steganography Method",IEEE/ACM Transactions On Audio, Speech, And Language Processing, Vol. 23, No. 1, January 2015.

[5] Haider Ismael Shahadi & Razali Jidin," High Capacity and Inaudibility Audio Steganography Scheme", 2011 7th International Conference on Information Assurance and Security (IAS), 978-1-4577-2155-7/11/$26.00_c 2011 IEEE.

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

[7] Ali M. Meligy, Mohammed M. Nasef and Fatma T. Eid, "An Efficient Method to Audio Steganography based on Modification of Least Significant Bit Technique using Random Keys", I. J. Computer Network and Information Security, 2015, 7, 24-29, DOI: 10.5815/ijcnis.2015.07.03.

[8] Saravanan Chandran & Koushik Bhattacharyya," Performance Analysis of LSB, DCT, and DWT for Digital Watermarking Application using Steganography", International Conference on Electrical, Electronics, Signals, Communication and Optimization (EESCO) – 2015 978-1-4799-7678-2/15/$31.00 ©2015 IEEE.\

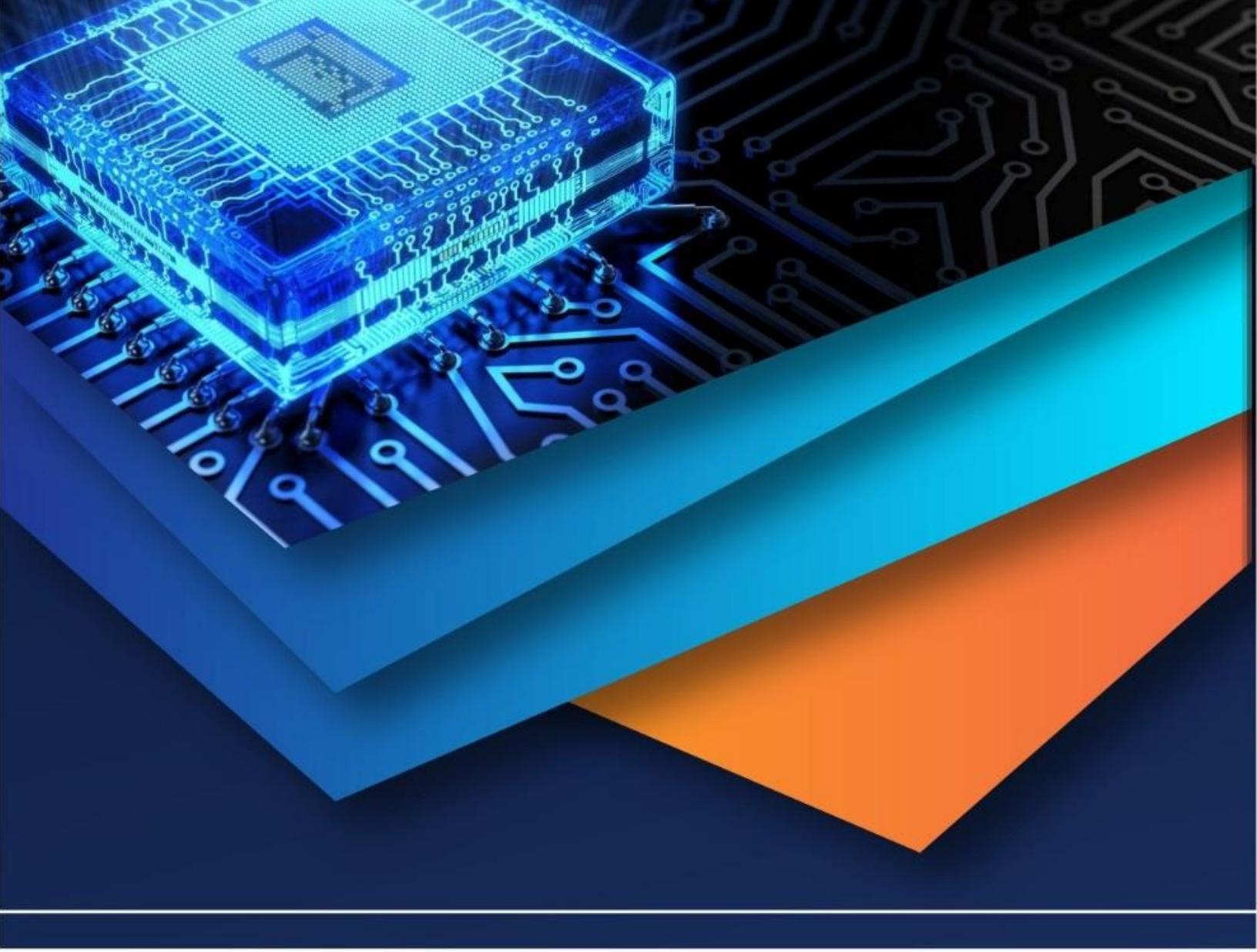
[9] Hinal Somani & Kaushal M. Madhu," A Survey on Digital Audio Steganography Techniques Used for Secure Transmission of Data", International Journal of Engineering Development and Research 2015 (IJEDR) | Volume 3, Issue 4 | ISSN: 2321-9939.

[10] Priyanka Khattar , Dr. Amrita Rai & Mr. Subodh Tripathi," Audio De-noising using Wavelet Transform", International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056, Volume: 03 Issue: 07 | July-2016.

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

[12] S.S. Divya & M. Ram Mohan Reddy," Hiding Text In Audio Using Multiple LSB Steganography And Provide Security Using Cryptography", International Journal Of Scientific & Technology Research Volume 1, Issue 6, July 2012 Issn 2277-8616.

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)