IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 11, Issue 6, Ver. III (Nov.-Dec .2016), PP 15-22
www.iosrjournals.org

A New Approach of Hybrid Model for Highly Secured Data Transfer in Audio Signals Using DWT

E. ANANT SHANKAR
Asst. Professor, Department of ECE S V College of Engineering, Tirupati. A.P.

Abstract: *In today's world there is rapid growth in computer technology and internet due to that security of information plays vital role in communication. To provide security there are two ways, Cryptography and Steganography. Steganography is process of hiding information in any media like Text, image, audio and video. Audio steganography is branch of this discipline in which data is embedded in Audio file. Cryptography is a technique which scrambles plain text (ordinary text) into cipher text (encrypted text). The paper could be a new hybrid approach, which mixes edges of each approach of cryptography and audio Steganography. The knowledge is to be transmitted as encrypted by victimization changed blowfish algorithmic program and resultant cipher text is embedded into a canopy audio file victimization separate wave remodel (DWT). The resultant stego audio is transmitted to the receiver and therefore the reverse method is finished so as to induce back the first plain text. Within the planned technique a steganographic theme at the side of the scientific discipline theme enhances the safety of the algorithmic.*

Keywords: *Blowfish, Cryptography, Security, Audio steganography, Wavelets, DWT.*

I. Introduction

The word steganography comes from the Greek name "steganos" (hidden or secret) and "graphy" (writing or drawing) and virtually means that hidden writing. The steganography is employed for several reasons. Steganography wont to communicate with complete freedom even underneath conditions that square measure censured or monitored. It can even defend non-public communications wherever the employment of the cryptography is generally not allowed or would raise suspicion. Steganography and Cryptography square measure the 2 standard approaches for secure communication. Steganography is concealment message by embedding it in exceedingly cowl media whereas cryptography is protective info by knowledge secret writing and transformation techniques. Steganography is completely different from cryptography within the method that steganography hides the existence of message whereas cryptography hides the means of message.

Hiding information in audio files become a lot of fashionable since human ear is insensitive to little distortions in audio signal, by slight modification within the binary sequence of the audio signals, the key info will be embedded. Steganography techniques [6, 7, 9, and 11] create use of audio signals in like WAV, AU and MP3 formats for embedding the knowledge. The LSB is that earliest technique accustomed entered message into audio signal [12]. It's straight forward to implement however ends up in changes in signal. Associate economical audio steganography ought to give a lot of payload capability, sensory activity transparency and hardiness.

The projected system combines the options of each steganography and cryptography. For encrypting the key message blowfish algorithmic program is employed. This encrypted message is hidden in a very cover audio file using discrete wavelet transforms. Finally the stego audio file is transmitted to supposed recipient to avoid the potential vulnerable attacks of intruder.

II. Literature Review

Cryptography and decipherment messages in order that messages will be firmly transmitted from a sender to a receiver without concern of an outside party intercepting and reading or neutering the message's contents. Information, confidentiality, integrity, information authentication and non-repudiation are the various aspects of data security that are self-addressed by cryptography. There are 2 basic varieties of cryptography out there are

***Symmetric key Cryptography*:** The algorithm use only one key, for both encryption and decryption.

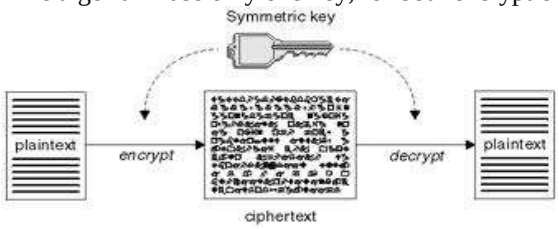

Figure1. Symmetric Key Cryptography

The symmetric key cryptography is implemented in two ways based on the input text mode
***Stream Ciphers*:** It is a symmetric key cipher in which one symbol of plain text is immediately converted into a symbol of cipher text.
Block Ciphers: It is a symmetric key cipher which encrypts a group of plaintext symbols as one block.
Asymmetric key Cryptography:
It additionally called public key cryptography; use 2 totally different keys public key and personal key, for coding and secret writing severally. The general public key may be freely distributed whereas non-public key ought to be secure.

Audio Steganographic Techniques:

There are several steganographic techniques for activity secret knowledge or messages in an exceedingly audio in approach that the modifications created to the file are perceptually indiscemible. These technique [9] area units are accessible in temporal domain, frequency domain, wavelet domain.
The various techniques in temporal domain are: LSB, parity coding, echo hiding. The main techniques under frequency domain are: phase coding and spread spectrum technique.

III. Proposed System

In the projected methodology, Cryptography and Steganography square measure effectively combined into a replacement hybrid model for transmittal the message in a very extremely secured manner. This paper created an effort so as to form the system in theory and much unbreakable

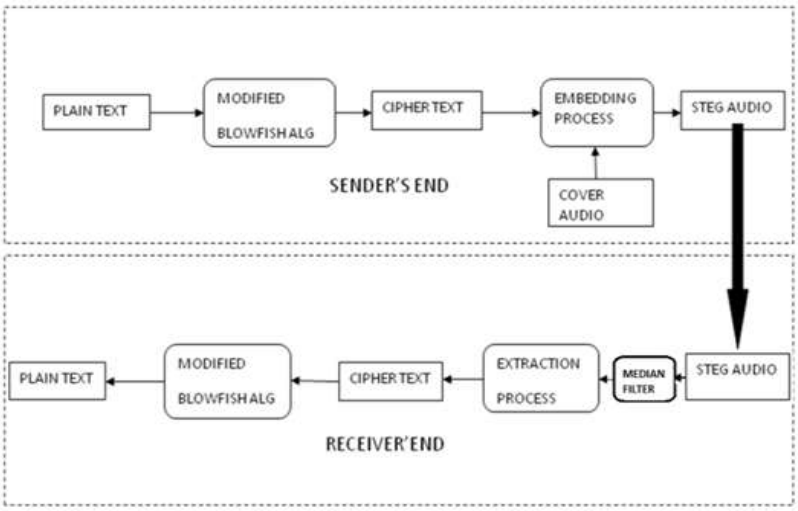

Figure 2. The block diagram of proposed approach

The steps concerned within the projected approach are

1. A Plaintext that is to be transmitted to the recipient from the user.
2. Exploitation the Blowfish rule for encoding of plaintext into cipher text.
3. Exploitation the discrete wave transforms and introduces the cipher text into the cover audio file.
4. The resultant stego audio is then transmitted through any channel to the receiver. The reverse of the above steps are taken place at the receiver facet that are as follows,
5. Median noise filter is applied at the receiver facet to get rid of noise from the stego audio enclosed throughout the transmission.
6. Apply the inverse DWT to stego audio for extracting the embedded info.
7. Blowfish secret writing method is applied to the extracted info because it is in dis-organized manner.
8. Finally, the receiver receives the particular secret info sent by the sender.

Blowfish Algorithm

In the planned methodology, a symmetric block cipher cryptography rule referred to as Blowfish is employed. Blowfish block cipher uses four S-boxes every of 256 entries of size thirty two bits and eighteen P-boxes of thirty two bit size. In Blowfish rule, the key plays an outstanding role whose size will vary from thirty two bit to 448 bits and it doesn't amendment oft and till now no science will destroy the message while not the coding key.

The operating of blowfish is as follows: The plain text is to be encrypted taken as sixty four bits so splitted into 2 blocks, XL and XR, of thirty two bit size. Left block XL is XORed with P1 and therefore the results fed to F-function, wherever substitution operations are performed and therefore the ensuing thirty two bit block is XORed with the proper half XR. Then the results of higher than operation are changed i.e. XL to XR and XR to XL.

To perform this operation for sixteen times. For seventeenth and eighteenth iterations, XL and XR won't be swapped, however XORed with the corresponding p-arrays. The fiestal structure of Blowfish cipher is as shown in the figure 3.

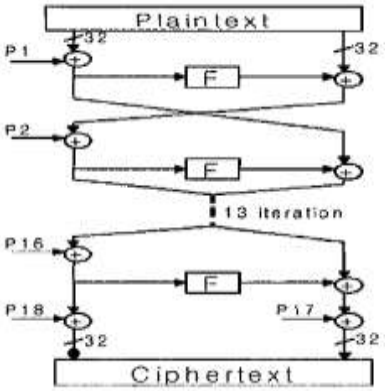

Figure 3. Fiestal Structure of Blowfish Algorithm

The function F[13] is defined as

F= ((S1+S2 mod 2^{32}) XOR S3) +S4 mod 2^{32} ----Eq.1

Here 32 addition operations and 16 XOR operations are performed in sequential order. In order to reduce the time of execution, F-function can be modified and is written as

F = (S1 XOR S2 mod 232) + (S3 XOR S4 mod 232) ---Eq.2

In the case of changed F-Function thirty two XOR and sixteen addition operations are needed and since of parallism of execution, time is reduced. The changed F-Function is shown in figure 4.

In Blowfish algorithmic program S-box and P-box sub key generation is extremely complicated, so resulting in the facility of blowfish in terms of security and performance.

P-box and S-box key values area unit calculated as follows:

1. Initialize 4 S-boxes and 18 P-boxes with hexadecimal digits of Pi.
2. P1 is XORed with first 32 bit key; P2 is XORed with second 32-bit key and so on. Perform the XOR operation for all P boxes with the key bits.
3. A string consisting of all zeroes is taken as the input and is encrypted using the sub keys defined in steps 1 and 2.
4. Output of step3 is taken as P1 and P2 values. Also pass this as input to the Blowfish algorithm and encrypt with the modified P values.
5. Output of step 4 is taken as P3 and P4 values.
6. The above process is repeated until all the P-box and S-box values are obtained.

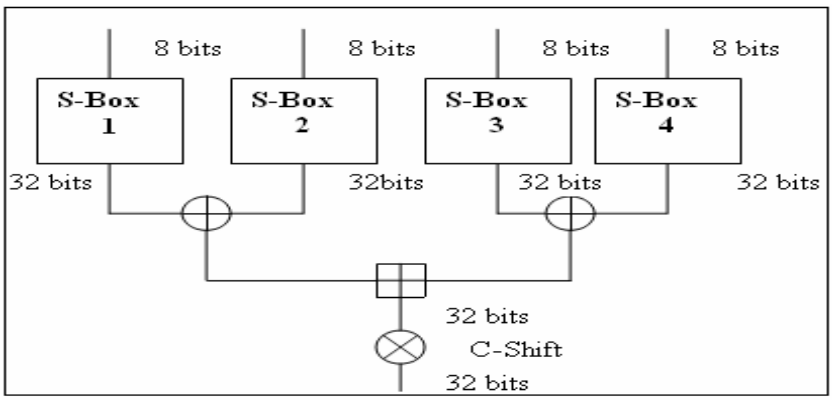

Figure4. Modified F-Function

Discrete Wavelet Transform

In order to beat the short returning of Short Time Fourier rework (STFT) and to investigate the non-stationary signals, a time–frequency illustration of the signal known as wavelet transforms square measure developed. By victimization the multi-resolution technique, signals completely different of various frequencies with different resolutions are often analyzed by moving

Ridge transforms. Discrete wavelet transform needs minimum resources and takes less computation time. It's easy to implement because it relies on sub band cryptography and may cipher the moving ridge rework in no time. By victimization the digital filtering techniques, the time-scale illustration of the signal is obtained. The signal is capable filters with totally {different completely different} cutoff frequencies at different scales. Wavelets are obtained by iteration of filters with rescaling. The DWT is computed by consecutive low pass and high pass filtering of distinct time domain signal. Through the filters, the detail data and approximate signals are often obtained at every level. By victimization the synthesis filters, original signal are often reconstructed

Wavelets are categorized into Orthogonal and Biorthognal. Orthogonal class wavelets are used in signal processing applications and here all the filters are of same length but not symmetric. Biorthognal wavelets are used in data compression applications and in this class high pass filter will be symmetric for odd length and anti-symmetric for even length where as low pass filter is symmetric. Some of the commonly used wavelet functions are given below figure 5. In the proposed method, Haar wavelets are used.

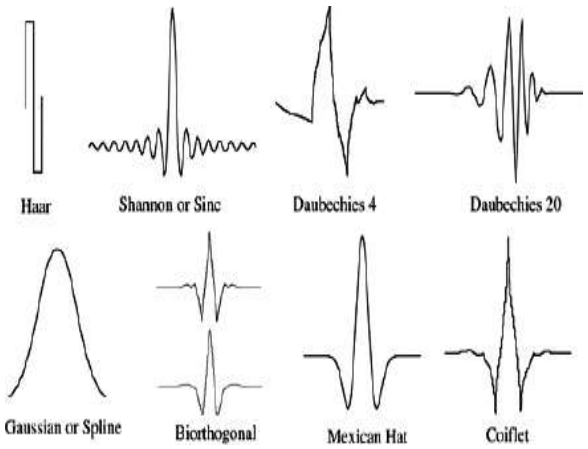

Figure 5. Wavelet Families

IV. Result Analysis

Different experiments were conducted to prove the potency of planned methodology. Associate in audio file with ".wav" extension has been chosen as cowl file. Modification of bits shouldn't degrade sound quality. Figure nine shows graph of original audio that is employed as host file. Figure ten shows graph of audio when embedding and figure11 shows graph of recovered audio when extraction. Graph of original audio, embedded audio and recovered audio is sort of same. The simulation was applied in MATLAB code.

The performance of the proposed scheme is evaluated from quality of stego audio. The peak signal to noise ratio (PSNR) was used to evaluate the stego audio quality. PSNR [15] is often expressed on a logarithmic scale in decibels (dB), it is defined as:

$$PSNR= 10 *\log_{10}(255^2/MSE)\ (dB)\ \text{-----Eq.3}$$

Where, MSE is the mean square error between the cover and stego audio. For a cover audio whose size is defined in terms of Amplitude and frequency as W,H respectively, MSE[15] is defined as:

$$MSE=\frac{1}{W*H}(\sum_{i=1}^{W}\sum_{j=1}^{H}(A_{ij}-A^{1}_{ij})^2) \quad \text{------Eq.4}$$

Where A_{ij} and A^{1}_{ij} are pitch values of cover and Stego audios.

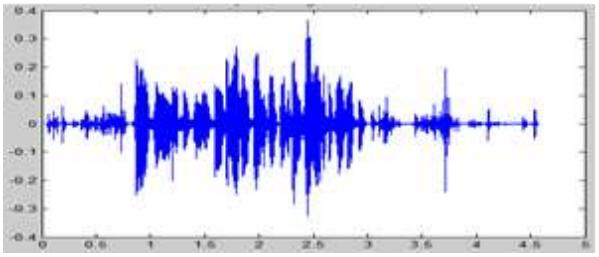

Figure 6. Original Audio

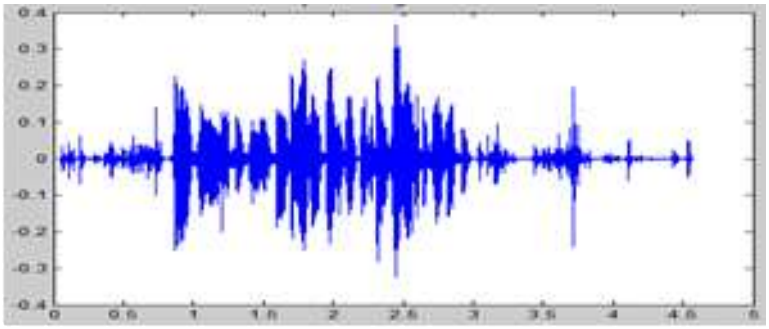

Figure 7. Stego Audio.

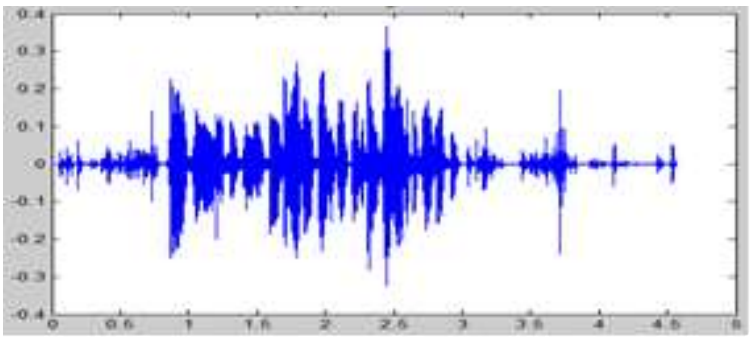

Figure 8. Recovered Audio

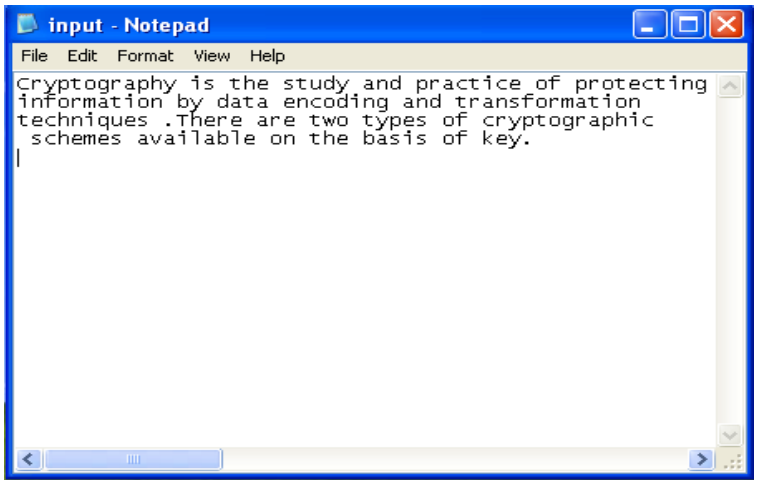

Figure 9. Original text message

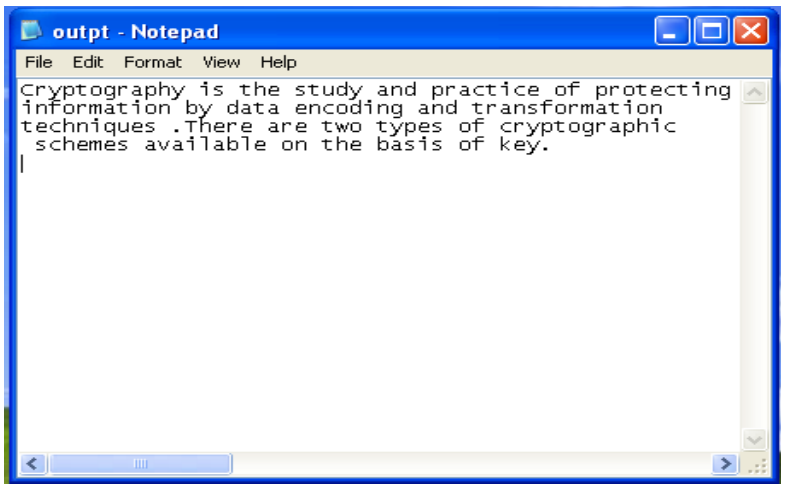

Figure 10. Recovered message

Table I. MSE values of different audio files for different message sizes

Message size in bytes	Male	Female	Male song	Female song
10	**1.56**	**1.4**	**1.3**	**2.2**
25	**2.3**	**2.09**	**1.7**	**2.4**
35	**3.1**	**2.6**	**2.04**	**2.5**
55	**5.4**	**4.0**	**2.68**	**2.9**

Table II. PSNR values of different audio files for different message sizes

Message size in bytes	Male	Female	Male song	Female song
10	**60.22**	**62.66**	**58.67**	**63.39**
25	**60.39**	**63.45**	**60.12**	**63.37**
35	**58.17**	**60.34**	**59.28**	**61.13**
55	**56.21**	**58.89**	**57.27**	**60.15**

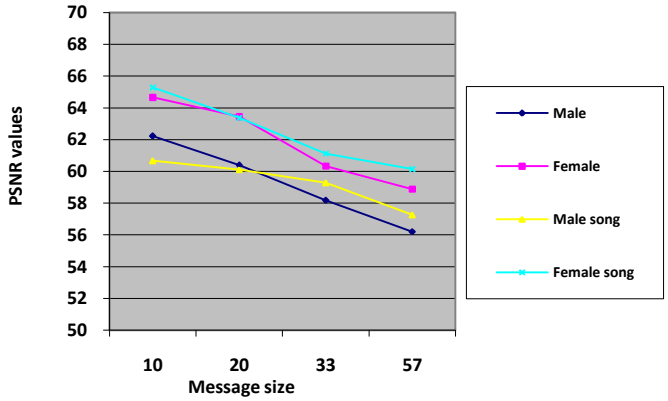

Figure 11. Graphical representation of MSE values for Different Songs

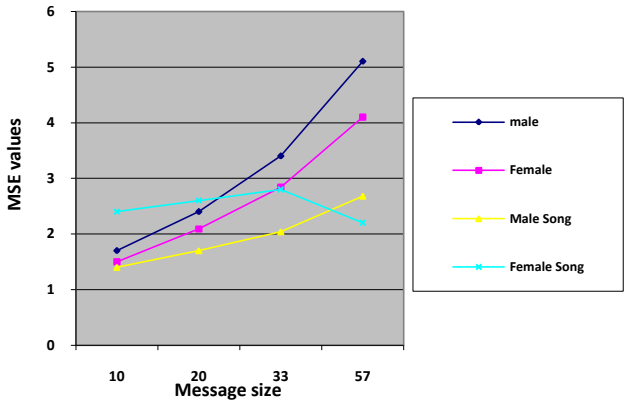

Figure 12. Graphical representation of PSNR values for Different Songs

Table III. MSE values of different categories for Audio file with same text content

Audio file	MSE
Hip-hop	0.11
Jazz	1.54
Pop	1..86
Rock	0.14

Table IV. PSNR values for different categories of Audio file with same text content

Audio file	PSNR
Hip-hop	43.65
Jazz	63.18
Pop	57.52
Rock	33.99

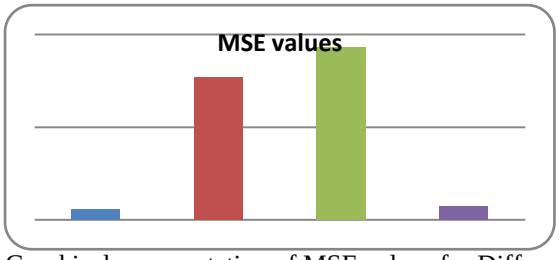

Figure 13. Graphical representation of MSE values for Different music files

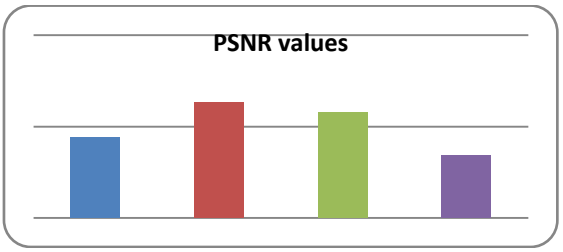

Figure 14. Graphical representation of PSNR values for Different Music files

V. Conclusion

The projected system is taken into account to be associate economical methodology for concealment text during audio files such knowledge will reach the destination in a safe manner while not being changed. PSNR and MSE values for numerous kinds of audio files are recorded. Victimization the tactic of embedding technique by DWT together with the coding and coding of the key message victimization Blowfish formula makes knowledge safer and transparency is reduced. In Future the strategies of dealing numerous malicious attacks are often studied

References

[1]. A.Cheddad,J.Condell, K.Curran, P.M.Kevitt, "Digital image Steganography:survey and analysis of current methods", *Journal of Siganl processing*, Vol.90,No.3, pp.727-752, Mar 2010.

[2]. K.Bailey, K.Curran, "An Evaluation of image based steganography methods ", *Journal of multimedia tools andapplications*, Vol.30, No.1,pp.55-88,July,2006.

[3]. N.Meghanathan, L.Nayak, "Steganalysis algorithms for detecting the hidden information in image, audio and video cover media", *International journal of Network Security and its Applications (IJNSA),* Vol.2, No.1,pp 43-55, Jan 2010.

[4]. Z.K.Al-Ani, A.A.Zaidan, B.B.Zaiden, H.O.Alanazi, "Overview :Main fundamentals for Steganography", *Journal of Computer* , Vol.2, No.3,pp. 158-165,2010.

[5]. W.Bender, D.Gruhl, N.Morimoto, A.Lu, "Techniques for data hiding", *IBM Systems Journal*, Vol. 35, No. 3 , pp. 313-336, 1996.

[6]. Jisna Antony, Sobin c. Sherly. A.P " Audio Steganography in Wavelet Domain – A Survey" I*nternational Journal of Computer Applications,* Vol 52, No.13, pp 975 – 987Aug 2012.

[7]. M.Wakiyama, Y.Hidaka, K.Nozaki, " An Audio Steganography by a low bit coding method with wave files", *Sixth International conference on Intellegent Information Hiding and MultimediaSignal Processing*, pp.530-533, Oct, 2010.

[8]. B.Schneier,"descriptionofanewvariable-lengthkey,64-bit blockcipher (blowfish),"in *Proceedings ofFast Software Encryption, Cambridge Security Workshop*, pp.191-204, Springer-Verlag,1994.

[9]. SiwarRekik, DrissGuerchi, Sid-Ahmed Selouani, HabibHamam "Speech steganography using wavelet and Fourier Transforms" ,*EURASIP Journal on Audio, Speech, and MusicProcessing*, 2012.

[10]. B. Santhi, G. Radhika and S. RuthraReka "Information Security using Audio Steganography -A Survey" *Research Journal of Applied Sciences, Engineering and Technology* ,Jul 2012.

[11]. Dr.Osamah Abdulgader, Al-rababah, "A Steganography method based on hiding secrete data in MPEG/Audio layer III", *International Journal of Computer Science and Network Security*, Vol.10, No.7, July 2010.

[12]. Bhagyashri A. Patil, Vrishali , A. Chakkarwar "Review of an Improved Audio Steganographic Technique over LSB through Random Based Approach" *IOSR Journal of Computer Engineering (IOSR-JCE) 7*Vol. 9, No.1 ,Feb 2013.

[13]. V.Vaidhiyanathan, G.Manikandan, G.Krishnan,"Anovelapproachto the performance and security enhancement using blow fish algorithm," *International Journal of Advanced Researchin Computer Science*, Vol.1, No. 4,pp. 451-454, 2010.

Authors Profile

E. ANANT SHANKAR, M.Tech is faculty member in ECE Department at S V College of Engineering, Tirupati. He received his Degree of Master of Technology in Electronic Instrumentation & Communication Systems from Sri Venkateswara University, Tirupati. Since his keen interest in Communications, the author is involved in the development of monitoring, Communication Systems, Processor based applications and other automation applications for Research & Development.