ISSN 2229-5518

Hash Based Data Text Fusion in Speech Signal Algorithm

Miss. Divya Sharma

Abstract— in this paper, Blind Source Separation technique for the security of the key after steganography has been implemented on the speech signal. Most steganography techniques are easily available online. In these techniques the security of the key is not particularly important therefore the security of the hidden message is jeopardized. I have proposed a new system in which we will be implementing contemporary spread spectrum technique steganography. The contemporary spread spectrum technique hiding text behind the speech signal which will be spread across the frequency domain randomly. In Spread Spectrum (SS) technique the information to be hidden is spread widely across the speech signal. For this we need to find those values for speech signal which have the minimum difference value when compared with ASCII value of information which is to be hidden. These location with the minimum value will be used to hide the secret message behind them. This system will generate a key which is meant to be sending along with the speech signal in which text file has been hidden. To ensure the safety of the key and the integrity of the hidden message we will apply Blind Source Separation on the key. Blind Source Separation will act as an encryption method. Blind Source Separation is the process in which we create segments and there sub segments which we will be mixing in a random order and finally concatenating this mixed sequence into one. The key can no longer be used by an eavesdropper for extract the hidden information. This key can be widely distributed across the Internet. The stego signal is imperceptible, transparent, and robust while the key is safe against any kind of attacks and can no longer be used by malicious sources for extracting or remove the hidden information.

Index Terms— Steganography, Cryptography, Speech Signal, Text File, Blind Source Separation, Spread Spectrum, Stego Signal.

1 INTRODUCTION

The word steganography is widely used throughout the world it simply means concealed writing. In steganography information is hidden such that an eavesdropper cannot detect the presence of information in the cover which a speech signals.

Steganography is the art of concealing the existence of message in its cover and any type of digital medium such as text, image, or audio/video can be used for steganography. Now days many steganography tools are available online which are easy and freely be implement. These tools are easy to access to all and hence are not that trust worthy for government use. We can explain steganography with the help of the example stated below. Suppose in an company environment meena wants to communicate with sita and the only medium of communication is being monitored by their boss ram and any type of communication or exchange between the two will be noticed by ram in such a scenario steganography can be used by meena and sita. With the help of steganography a hidden communication channel will be established between meena and sita without the third party ram having any knowledge of a communication taking place.

Steganography can be said to be art to conceal the existence of message in the hidden. Steganography can be implemented on any type of digital file format such as .txt, .doc, .jpg, .wav, and video files.

Steganography attempts to hide all evidence regarding the existence of secret communication taking place while cryptography converts the information such that no one can understand the information without the help of mathematical algorithms, substitution, shift operations, etc. Steganography creates a stego file while cryptography creates cipher text. Stego file has data hidden in a cover while cipher text the data will be right in front in a converted form or a non-understandable form. Cryptography implements the concept of keys and so does steganography.

If an attacker removes or changes the speech signal it can be detected in cryptography. It is difficult to achieve plain text out of cipher text as cryptography involves the concept of mathematical algorithms, substitution, repositioning of bits within the speech signal, table references and also concept of keys which makes it difficult for attacker to decrypt the message. While attacking steganography the attacker has to first make sure of the existence of a hidden message in the cover, and then apply the exact technique to extract the hidden message which has been used to hide the message, this makes it more time consuming and costly to implement.

Both steganography and cryptography ensure the security, authenticity, and privacy of information. Cryptanalysis is the art of achieving back the plain text from a cipher text while stegano analysis is the technique of achieving the hidden information in a cover.

- *Divya Sharma is currently pursuing Master's degree program in Computer Science and Engineering from Department of Computer Science and Engineering, Rayat and Bahra Institute of Engineering and Bio-Technology, Kharar, Mohali, Punjab, India, PH-9815944743 E-mail: divya009sharma@gmail com*

2 SPEECH STEGANOGRAPHY

Speech steganography is the art of hiding secret message within a human voice which has been recorded with a microphone this steganography signal will be then routed across the Internet. Internet is easily accessible, cheap medium for communication and is used worldwide which increases the risk of attacker attacking the confidential data which is meant to be kept safe and hidden from the common people from this purpose steganography is conducted. To guarantee the safety of data which concern the national security of a country speech steganography is practiced. Speech steganography is the process in which a secret message is hidden in a speech signal. This speech signal which is created after steganography is referred to as a stego signal. This stego signal on being transferred freely across the Internet will go undetected in most cases. Speech steganography can be used for hiding text, images, and speech signal within them. There are various technique with the help of which text data can be hidden in an speech signal most common are **LSB (Least Significant Bit), Phase Coding, Parity Coding, Echo Hiding, Spread Spectrum**. LSB technique the least significant bit is replaced with the hidden information. Parity Coding break the signal into separate region of samples and encode each bit into a sample region's parity bit. Echo Hiding where an echo of the signal is created. Three parameters of the echo speech file are varied these are amplitude, delay rate and offset. Spread Spectrum in this method the secret information is hidden by spreading it across the frequency domain speech signal.

There are two types of attacks are made against the stego signal: 1). Attack to completely destroy or remove the hidden message in a stego signal. 2). Attack for detection and extraction of hidden message from the stego signal.

Existing speech steganography algorithm can embed messages in .WAV, .AU, and .MP3 format .WAV is the commonly used format for speech steganography as it recognised throughout the world widely.

2.1 Disadvantages of Existing System:

- More time is consumed in the existing steganography system.
- Only few speech signals can be applied steganography.
- In the existing system designer have implemented complicated method for steganography which can easily be detected and code for extraction of information hidden with such logic is easily accessible.
- The user interface developed are not easy to understand and not graphically attractive.
- Hidden data in case of LSB gets stored in consecutive bytes.
- Cannot with stand attacks made to destroy or extract the hidden message.
- The safety of the key is not ensured any third party can remove or manipulate the key according to his/her requirement.
- Steganography is not practiced on audio because of their sensitivity.
- No method available for establishing a direct communication between sender and receiver.
- No existing system has paid enough attention to security of keys.

A speech signal is like a digital signature of a person. Therefore it is disadvantageous for a human being to hide information in speech signal. As speech is a biometrics component it not preferred for hiding text or any digital data format of information in them. If speech ends up in wrong hands it can be used for wrong purposes as speech is part of someone identity or a voice signature.

3 PROPOSED SCHEME

It is advantageous to use speech signal for the proposed scheme as speech consists of more noisy regions or none areas of interest which will be used by the system for hiding the secret text message.

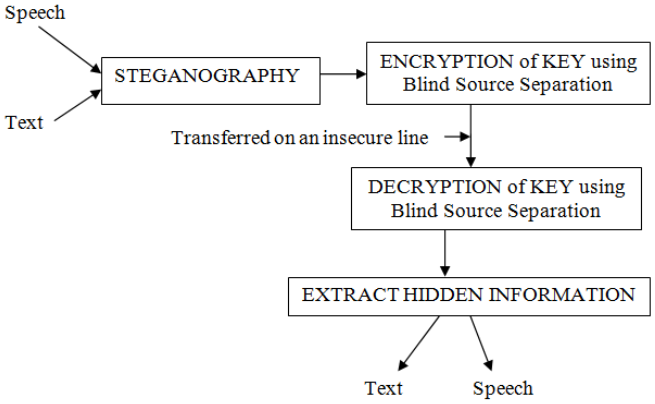

Figure 1: Detailed block diagram of the proposed system

A detailed block diagram of the proposed system can be seen in Figure 1 where a text file with .txt extension is read from the computer and the characters in the string are converted into ASCII with the help of UNICODE2NATIVE command and stored into a variable. UNICODE2NATIVE command takes the characters and convert it into ASCII values for the given text file which will be hidden within the speech signal using contemporary spread spectrum technique. Spread spectrum technique where the hidden message is spread across the frequency domain of the speech signal. In Spread spectrum we will find those areas in the speech signal that have the minimum difference with the ASCII value of the hidden text. These areas are used for hiding the secret message. It is advantageous to use speech signal for the proposed scheme as speech consist of more noisy regions or none areas of interest which will be used by the system for hiding the secret text message. This process will generate a key which is important for extracting the hidden message. This key will applied with Blind Source Separation which will act as an encryption method. The stego signal or the signal with the hidden message will be routed across the Internet along with the BSS key. After reaching the specified recipient the key will be applied with Blind Source Separation to reverse the Blind Source Separation which was performed by the sender on the key. This key can

now be used by the sender to extract the text file from the speech signal.

3.1 Spread Spectrum Technique for Speech Steganography:

In spread spectrum technique the text message which is to be hidden is spread across the frequency domain of the speech signal. In this technique we will find the areas of non interest or the noisy areas in the speech signal. These areas will be used to hide the ASCII value which we have generated for the text file with the help of UNICOD2NATIVE command. In spread spectrum technique those areas in speech signal are located which have the minimum difference with what we have to hide those location which resemble the text data to be hidden are used for hiding the information and a key is generated. This method will result in imperceptible speech which cannot be distinguished by human ear and unnoticeable changes in the speech signal.

Small amount of noise will be added in few cases where the duration of recorded speech is small and amount of text data to be hidden is more. But in most cases the resulting signal is transparent, robust, and of good quality. In spread spectrum technique it is hoped that no attack will be made on the key or on the location where the hidden information is placed. The major drawback of this technique is that if an attacker removes the key then the hidden information can be achieved back this drawback is dealt with in the proposed scheme. A stego-signal is what we achieve after applying steganography on the speech signal. In case of the proposed system this stego-signal will be accompanied by the key while being transferred across the Internet.

Say, a speech signal S for a time of t seconds as shown in (1). Here t is the duration of speech which can be 5, 10, and 15 seconds which will be same throughout.

$$S(t) = (S_1(t), S_2(t) \ldots\ldots, S_n(t)) \qquad (1)$$

$$t = 5, 10, 15$$

$$U = \sum_{i=1}^{m} T_i \qquad (2)$$

Here, U is the ASCII value of the string existing in a text file and T is the ASCII value of text which is to be hidden, m is the size of text which is to be hidden and S is the speech signal which will hide the information (2). Shows that say T3 is any value of hidden text message for any character which is at a location 3 in the string.

$$S_1 = \sum_{i=1}^{n} S(x_i, y_i) - Uj \qquad (3)$$

Uj is the ASCII value of text which is to be hidden at any specific time say j (j=1, 2, 3, 4… m) where j is independent of i and m is total number of ASCII values to be hidden in the speech signal and n is the number of samples which exists in a speech while S1 is the new signal while S is the original speech signal as shown in (3).

The stego signal is represented by S1 as shown in (5):

$$S1(t) = (S1(t), S2(t), U1, S3(t), U3, \ldots\ldots, Sn(t)) \qquad (5)$$

And key K = K1, K2…Km

The proposed system will perform steganography on speech signal stored in .WAV (Windows Audio Visual) file format. A .TXT text file will be hidden using the Spread Spectrum technique for steganography. Speech signal which is meant to be sampled is of 8 KHZ which has 8000 samples in it the duration of the speech will be 10 second which will hide ASCII characters in them.

3.2 Advantages of Proposed Scheme

Few advantages of the proposed system are mentioned below:

- To ensure the security of the hidden information the key is applied with Blind Source Separation.
- In the proposed scheme Spread Spectrum technique is applied which hides the information in a random order based on their threshold value.
- It is perceptual method for hiding information.
- The quality of audio is not lost after steganography.
- The stego signal which is created is transparent.
- It is simple to implement Spread Spectrum technique.
- It is disadvantageous to use speech for hiding information as speech is a biometrics component this is overcome in the proposed system as cryptography technique get applied on the stego file.
- The information which is to be hidden is stored in a random manner.
- In proposed system the key is encrypted with the help of Blind Source Separation.
- Interactive and user friendly GUI for user interfacing.
- The stego signal will withstand against removal attacks
- The detection of the hidden message is difficult in the proposed system.
- To increase the capacity the user needs to record speech for a higher duration of time.

3.3 Blind Source Separation

Blind source separation is the process in which we have to implement two basic sub operations which are creation of segments and Sub Segments and inter mixing of these segments and Sub Segments and finally concatenation which can be explained clearly as below:

1. **Creation of Segments and Sub Segments:** In this step, segments and sub segments of the key are create. In the proposed system k segments and l sub segments are created. The size of segments will be equal to one another and so will the size of sub segments.
2. **Mixing of these Segments:** These l sub segments will intermix amongst one another in a random manner and concatenate into k different segments. Now the k segments will be intermixed and finally concatenated into one single larger segment which will be the new key. This key is meant to be transferred across the network along with the stego signal.

The proposed system will work against attack made to detect the hidden message not only because the key has been encrypted with Blind Source Separation but because the Blind

Source Separation will result in a new key which will be totally different from the original key and of a different size than the original key. This system will withstand against removal attacks which are second category of attack made against the stego file which are made to remove the hidden message and also against attack made to reveal the hidden message.

Blind Source Separation can be described as follows:

$$K = K_1, K_2, K_3 \ldots K_k \quad (6)$$

K is the original key and $K_1, K_2, K_3 \ldots K_k$ are the k segments in the key as in (6).

$$K_1 = K_{11}, K_{12}, K_{13}, \ldots K_{1l} \quad (7)$$

K1 is the first segment of key and $K_{11}, K_{12}, K_{13}, \ldots K_{1l}$ is the l sub segments of segment K1as in (7).

$$K_1 = K_{1l}, K_{11}, K_{13}, K_{12} \quad (8)$$

$$K = K_3, K_k, K_1 \ldots K_2 \quad (9)$$

Key after implementation of Blind Source Separation on sub segment K1 is in (8) this will be repeated for each sub segment and in the segments is (9) and final key K.

3.4 Application

The proposed algorithm can be applied for military purposes, as well as protection of intellectual possessions, for government use (therefore to hide information which is of high secrecy from the common people). It can be used to establish a secret channel for communication for industrial application within an industry to set up a secure channel between the top authorities of the industry. This technique can be used in banking sector for routing passwords through the Internet these password can be either ATM or internet banking or net banking Information which holds high importance for the peace and security between the countries can be applied with hash based fusion of text data in speech signal. This system can be used speech based media system and recording an audio bibliography of a person while the hidden text will consist of information such as the speaker name, time of recoding and publisher details, etc.

This system is implemented for a confidential communication and secret data storing and data sharing. Steganography also protects data from getting altered. It is used in Media Database systems, Access control system for digital content distribution and can also be used to hide illicit, unauthorized or unwanted activity, criminal communication, fraud, hacking, electronic payment, viruses and gambling which is the biggest disadvantage of steganography as it promotes criminal activty.

4 Proposed Scheme

In the proposed scheme a .txt file is hidden within a speech signal recorded in .wav format. Spread spectrum technique is used in which the information which is to be hidden is spread widely across the speech signal. After application of spread spectrum technique a key will be created. This key which will be for distributed purposes and will be the same and known to everyone. For the safety of this key I have applied Blind Source Separation on the key.

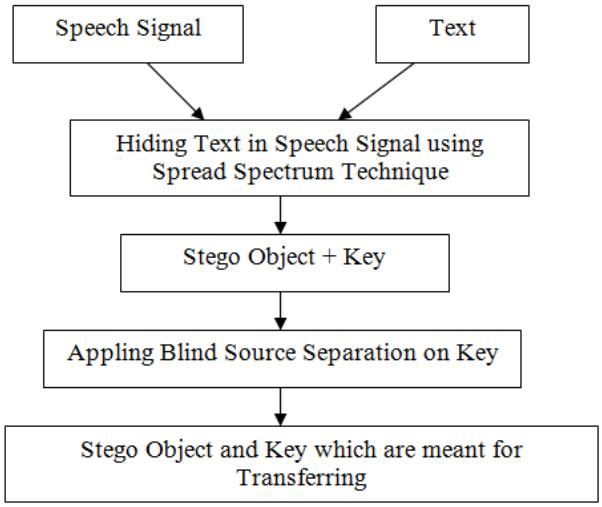

Figure 2: Block diagram of proposed technique at sender end.

4.1 Steps for Proposed System

At the receiver end, the following steps will take place:

Step 1: Record a speech signal and create a .TXT file which is to be hidden in the speech signal.

Step 2: Read the text file into a variable and save there ASCII value in a new matrix.

Step 3: The noisy areas or the areas of none interest are found in the speech signal. These areas are regions of none interest and have no meaning to them. The addresses for these locations are recorded.

Step 4: Spread Spectrum technique is applied on speech signal. With the help of which the ASCII values of .txt file are compared with the speech signal and location with the minimum difference are found and used for hiding the text file on them.

Step 5: Blind Source Separation is applied on the Key which will result in an encrypted key. This step can be divided into two sub steps which are:

Step 5.1: Creation of k segments and further division to create l sub segments of equal size.

Step 5.2: Inter mix these l sub segments into one another and then concatenation such that k segments are formed and finally intermixing of k segment and concatenation them into one block which will be the new key.

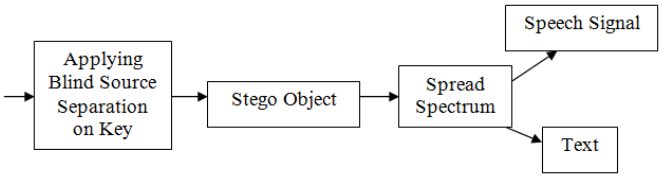

Figure 3: Block diagram of proposed technique taking place at receiver end.

At the receiver end, block diagram shown in figure 3 is implemented. This has been explained below:

Step 1: First the key is applied with reverse Blind Source Separation or decryption will be done here we will be creating the segments and further sub segments which will then intermix in a same manner as at the sender end and concatenated into one to achieve the original key.
Step 2: With the help of the key the ASCII value of the information which has been hidden are extracted from the stego signal using the reverse spread spectrum technique. **Step 3:** These ASCII values are later concatenated into one and converted to character to reveal the hidden text file.
Step 4: This file is then saved on the receiver computer.

5 Experimental Results

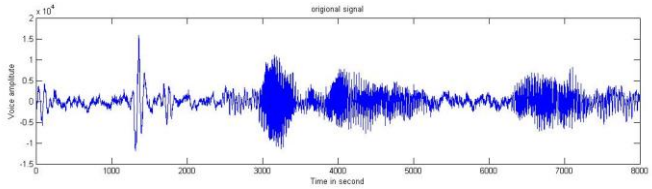

Figure 4: Original signal.

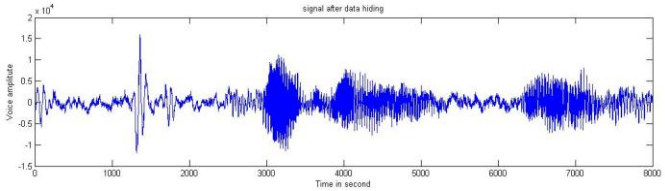

Figure 5: Signal after implementation of Spread Spectrum.

The figure 4 shows the speech signal before the hiding any information in it while figure 5 shows the stego signal after text data is hidden in it. It is visible with the help of these figures that the stego signal is transparent, robust, and imperceptible for the Human Auditory System (HAS).

The results obtained after implementation of Blind Source Separation on the key ensure the secrecy of the hidden data and protects it against attack made to reveal and destroying the hidden message.

In steganography the security of the key is very important and plays a huge role in hiding the secret message. Any addition of noise or change in the speech signal will be noticed by the human ear. The proposed technique on implementation will not add any noise in the speech signal and is easy to implement. With blind source separation intermix of the sub segments and segments will take place in the same manner as on the sender end. This will increase the work load of the attacker as the attacker now also need to decrypt the key or figure out the correct sequence in which words exists in the original text file. This increases the security of information which is hidden within the speech signal as Blind Source Separation in our case will act as a cryptography technique which will alter the key.

6 Performance Evaluation

A Steganography speech signal is subjected to some test for finding out the quality, transparency of the stego file, and robustness of the speech signal after steganography has been applied on it. To check the transparency of the signal after steganography we can play the signal or compare their plots with one another which in proposed system case sound the same for the human ear and when plotted seem the same. For this purpose, Signal to Noise Ratio (SNR) is calculated with the help of SNR we can detect the amount of noise which will be added in the signal after it has undergone steganography. These results have been taken on a computer with 2GB RAM and 2.3 GHZ processor.

$$\mathrm{SNR} = 10 \log_{10} \left\{ \frac{\sum_{n=1}^{N} S^2(n)}{\sum_{n=1}^{N} (S_1(n) - S(n))^2} \right\} \quad (10)$$

In (10) I have calculated the SNR for the proposed system. Here S (n) is the original signal and S1 (n) is the stego signal and SNR is Signal to Noise Ratio for a given signal and units that are used for measurement of SNR are Decibel (DB). SNR can be used for finding out the quality of the signal after spread spectrum technique has been applied on the speech signal.

These results have been taken for a speech signal recorded for varying duration. The size of the text file which is to hidden is also varied starting from 502 bytes to 3000 bytes.

Implementation consideration: these results are computed in MATLAB 7 b. The result obtained for steganography have high perceptual making and are robust in nature.

Table 1:

Comparison table for signal to noise ratio, time for hiding the secret message and for extracting the secret message from the signal after undergoing steganography.

Duration of speech signal (in seconds)	Size of text file (in Bytes)	SNR (DB)	Time FOR HIDING (in seconds)	Time for extracting (in seconds)
5	502	61.5490	0.43692	0.069786
	1950	10.7515	0.285972	0.073589
	1400	16.3841	0.192667	0.072186
	1840	70.8108	0.364205	0.085936
	2410	8.1091	0.306255	0.079192
10	502	84.4082	0.173573	0.071421
	1000	74.5712	0.194668	0.074056
	1536	60.8681	0.21514	0.047824
	1840	68.2803	0.26341	0.077177
	2410	61.8251	0.798341	0.080408
15	502	86.8481	180456	0.102997
	1000	74.5240	0.21 129	0.075391
	1840	75.7344	0.343355	0.089065
	1950	69.0833	0.404081	0.082495
	2410	70.8108	0.364205	0.085936

The graph is plotted in figure 6 has been plotted for 11 different text file which are of varying sizes and three different speech of varying duration. Few of these values are shown in Table 1. It is seen that with the increase in the duration of the speech the quality of the stego signal is also increased. Therefore to obtain better SNR the duration of the speech file should be increased as this will also increase the capacity for storing hidden information and increase the performance of the system.

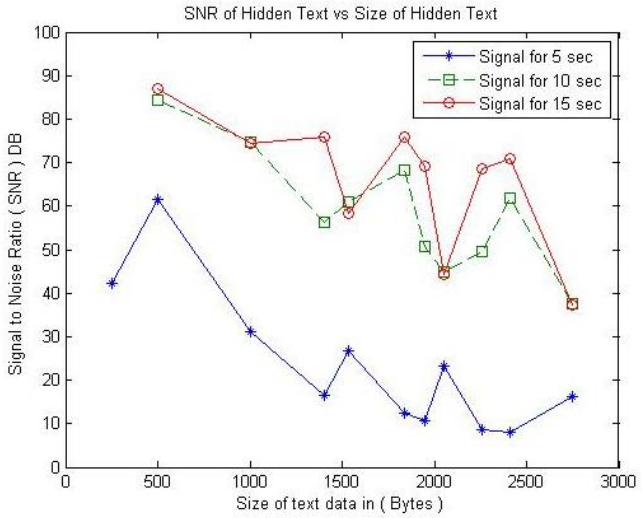

Figure 6: Graphical view of SNR for the proposed technique for 3 signals of varying durations (5, 10, and 15 second) and for 11 different text file of varying size

7 Conclusions

A method has been proposed which is easy to implement, transparent, and imperceptible for the human ear. Here we have used spread spectrum technique for steganography which spreads the messages to be hidden across the frequency domain of the speech signal. This technique is easy to implement, not that easy to detect, transparent for the human ear, and robust, highly accurate in nature as the recipient can achieve back what they had hidden without any error. The quality of the signal after steganography is maintained. The proposed system will also deal with solving the problem of key distribution in steganography as in proposed case the key is applied with Blind Source Separation which acts as an encryption method and results in an encrypted key which can be distributed widely across the Internet. As Key in the hands of an eavesdropper or attacker can be used for extract or destroy the hidden information. By applying Blind Source Separation we have eliminated the possibility of any third party discovering and destroying the hidden message. A signal after application of steganography is not distinguishable to the human ear therefore transparent for HAS.

Acknowledgment

I would like to thank my guide Mr. Deepankar Verma, Assistant Professor in Department of Computer Science and Engineering at R.B.I.E.B.T. (Kharar), Punjab, India for motivating me to work on steganography. I would also like to thank my sister, my mother, and my father for their continuous support, cooperation, and guidance throughout my M.Tech. work.

References

[1] Deng Lixin, "A New Approach Of Data Hiding Within Speech Based On Hash And Hilbert Transform", International Conference on Systems and Networks Communications, 2006. ICSNC '06.

[2] Marina Ponomar,"On Acceptance Modification Limits of Electro acoustic Speech Signals for Data Hiding", Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing 2009.

[3] Vandana S. Inamdar, Priti P. Rege, Aarti Bang," Speech Based Watermarking for Digital Images", TENCON 2009 - 2009 IEEE Region 10 Conference 2009.

[4] Dmitriy E. Skopin, Ibrahim M. M. El-Emary, Rashad J. Rasras, Ruba S. Diab, "Advanced Algorithms in Audio Steganography for Hiding Human Speech Signal", 2nd International Conference on Advanced Computer Control (ICACC), 2010.

[5] Dmitriy E Skopin1, Ibrahim M M El-Emary, Rashad J Rasras, Ruba S Diab, "Advanced Algorithms in Audio Steganography for Hiding Human Speech Signal", 2nd International Conference on Advanced Computer Control (ICACC), Volume 3, 2010.

[6] Sarosh K. Dastoor, "Comparative Analysis of Steganographic Algorithms intacting the information in the Speech Signal for enhancing the Message Security in next Generation Mobile Devices ", 2011, IEEE.

[7] Fatiha Djebba, Beghdad Ayad, Habib Hamam and Karim Abed-Meraim, "A view on latest audio steganography techniques", International Conference on Innovations in Information Technology (IIT), 2011.

[8] Mohammadreza Narimannejad, Seyed Mohammad Ahadi ,"Watermarking of Speech Signal through Phase Quantization of Sinusoidal Model"

[9] Shashikala Channalli, Ajay Jadhav, "Steganography an Art of Hiding Data "International Journal on Computer Science and Engineering, Vol 1 (3), 2009.

[10] K. Geetha, P. Vanitha Muthu, "Implementation of ETAS (Embedding Text in Audio Signal) Model to Ensure Secrecy", International Journal on Computer Science and Engineering (IJCSE), Vol. 02, No. 04, 1308-1313, 2010.

[11] S. Suma, Christal Mary, "Improved Protection In Video Steganography Used Compressed Video Bit streams ", (IJCSE) International Journal on Computer Science and Engineering, Vol 02, No 03, 2010.

[12] Pradeep Kumar Singh, R K Aggrawal, "Enhancement of LSB based Steganography for Hiding Image in Audio", (IJCSE) International Journal on Computer Science and Engineering, Vol 02, No 05, 2010.

[13] Herman Kabetta, B Yudi Dwiandiyanta, Suyoto, "Information Hiding In Css: A Secure Scheme Text-Steganography Using Public Key Cryptosystem ", International Journal on Cryptography and Information Security (IJCIS), Vol 1, No 1, December 2011.

[14] E. Anupriya, "Encryption using XOR based Extended Key for Information Security – A Novel Approach", 2011.

[15] Lalitha G., Ashish Jain, U. Raja, "Secure Transmission of Compound Information Using Image Steganography ", International Journal on Computer Science and Engineering (IJCSE), Vol. 3 No. 4, 2011.

[16] R. Darsana , Asha Vijayan ,"Audio Steganography using Modified LSB and PVD", Trends in Network and Communications and Communications in Computer and Information Science, Volume 197, Part 1, 11-20, 2011.

[17] R. Sridevi, Dr. A. Damodaram, Dr. Svl Narasimham, "Efficient Method of Audio Steganography Modified Lsb Algorithm and Strong Encryption Key with Enhanced Security", Journal of Theoretical and Applied Information Technology, 2011.

[18] Tanmay Bhattacharya, Nilanjan Dey, "A Novel Session Based Dual Image Encoding and Hiding Technique Using DWT and Spread Spectrum", International Journal on Computer Science and Engineering (IJCSE), Vol. 3 No. 11 November 2011.

[19] Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt, "Towards Objectifying Information Hiding "
[20] Anant Umbarkar, Abhijit Joshi, Ajay Jadhav, "Wave Steganography ", 2011.
[21] Manoj Kumar Sharma, Dr. P. C. Gupta, "A Comparative Study of Steganography and Watermarking ", IJRIM Volume 2, Issue 2 (February 2012).