INFORMATION HIDING USING AUDIO STEGANOGRAPHY – A SURVEY

Jayaram P[1], Ranganatha H R[2], Anupama H S[3]

[1,2,3]Department of Computer Science and Engineering, R V College of Engineering, Bangalore, INDIA

[1]jayaram.ynk@gmail.com,
[2]ranganath.rvce@gmail.com,
[3]anupamahs@rvce.edu.in

ABSTRACT

Today's large demand of internet applications requires data to be transmitted in a secure manner. Data transmission in public communication system is not secure because of interception and improper manipulation by eavesdropper. So the attractive solution for this problem is Steganography, which is the art and science of writing hidden messages in such a way that no one, apart from the sender and intend recipient, suspects the existence of the message, a form of security through obscurity. Audio steganography is the scheme of hiding the existence of secret information by concealing it into another medium such as audio file. In this paper we mainly discuss different types of audio steganographic methods, advantages and disadvantages.

KEYWORD

Steganography, Cryptography, Audio Steganography, LSB.

1. INTRODUCTION

In cryptography, the structure of a message is scrambled to make it meaningless and unintelligible unless the decryption key is available. It makes no attempt to disguise or hide the encoded message. Basically, cryptography offers the ability of transmitting information between persons in a way that prevents a third party from reading it. Cryptography can also provide authentication for verifying the identity of someone or something [3].

In steganography does not alter the structure of the secret message, but hides it inside a cover image so that it cannot be seen. A message in a cipher text, for instance, might arouse suspicion on the part of the recipient while an "invisible" message created with steganographic methods will not. In other word, steganography prevents an unintended recipient from suspecting that the data exists. In addition, the security of classical steganography system relies on secrecy of the data encoding system. Once the encoding system is known, the steganography system is defeated [4, 1].

The following points can be attributed to the renaissance of steganography

i. Government ban on digital cryptography. Individuals and companies who seek confidentiality look to steganography as an important complementary since combining cryptography and steganography can help in avoiding suspicion and protect privacy.

ii. The increased need to protect intellectual property rights by digital content owners, using efficient watermarking.

iii. The trend towards electronic communications and humans desire to conceal messages from curious eyes. With rapid advancement in technology, steganographic software is becoming effective in hiding information in image, video, audio or text files [11,14].

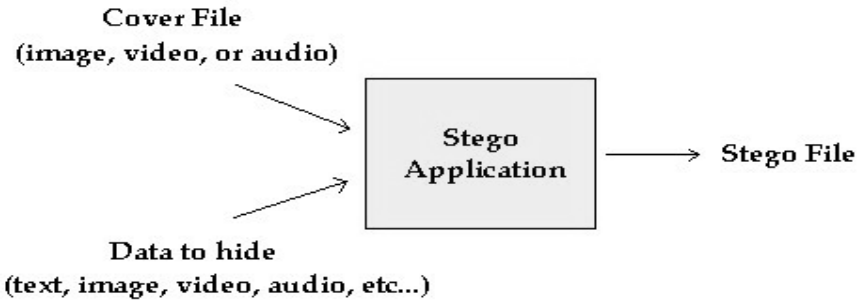

Figure 1. Steganography Application Scenario

The steganography application hides different types of data within a cover file. The resulting stego also contains hidden information, although it is virtually identical to the cover file. What Steganography essentially does is exploit human perception; human senses are not trained to look for files that have information hidden inside of them, although there are programs available that can do what is called Steganalysis (Detecting use of Steganography.)

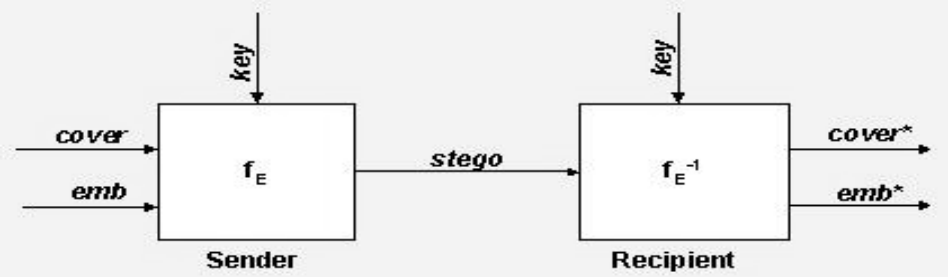

Figure 2. A generic Steganography System

Fig. 2 shows the block diagram of a secure steganographic system.Input messages can be images, texts, video, etc. The components of steganographic system are:

Emb: The message to be embedded.

Cover: The data in which emb will be embedded.

Stego: A modified version of cover that contains the embedded message emb.

Key: Additional secret data that is needed for the embedding and extracting processes and must be known to both, the sender and the recipient.

f_E: A steganographic function that has cover, emb and key as parameters and produces stego as output.

F_E-1: A steganographic function that has stego and key as parameters and produces emb as output. F_E-1 is the inverse function of f_E in the sense that the result of the extracting process f_E-1 is identical to the input E of the embedding process f_E.

The embedding process f_E embeds the secret message E in the cover data C. The exact position (S) where E will be embedded is dependence on the key K. The result of the embedding function is slightly modified version of C: the stego data C'. After the recipient has received C' he starts the extracting process f_E-1 with the stego data C' and the key K as parameters. If the key that is supplied by the recipient is the same as the key used by the sender to embed the secret message and if the stego data the recipient uses as input is the same data the sender has produces (i.e., it has not been modified by an adversary), then the extracting function will produce the original secret message E.

2. OVERVIEW OF AUDIO STEGANOGRAPHY

The word steganography comes from the Greek Steganos, which means covered or secret and -graphy means writing or drawing. Therefore, steganography means, literally, covered writing. Steganography is the art and science of hiding secret information in a cover file such that only sender and receiver can detect the existence of the secret information [3]. A secret information is encoded in a manner such that the very existence of the information is concealed.

The main goal of steganography is to communicate securely in a completely undetectable manner [4] and to avoid drawing suspicion to the transmission of a hidden data [5]. It is not only prevents others from knowing the hidden information, but it also prevents others from thinking that the information even exists. If a steganography method causes someone to suspect there is a secret information in a carrier medium, then the method has failed [6,8].

The basic model of Audio steganography consists of Carrier (Audio file), Message and Password. Carrier is also known as a cover-file, which conceals the secret information.

Basically, the model for steganography is shown in Fig 3. Message is the data that the sender wishes to remain it confidential. Message can be plain text, image, audio or any type of file. Password is known as a stego-key, which ensures that only the recipient who knows the corresponding decoding key will be able to extract the message from a cover-file. The cover-file with the secret information is known as a stego-file.

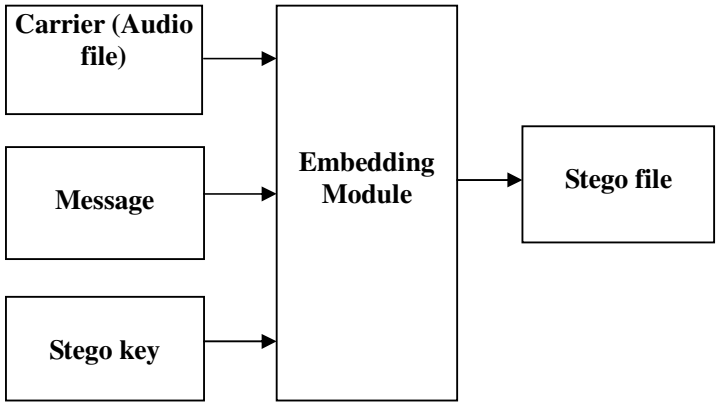

Figure 3: Basic Audio Steganographic Model

The information hiding process consists of following two steps [9, 10].

i. Identification of redundant bits in a cover-file. Redundant bits are those bits that can he modified without corrupting the quality or destroying the integrity of the cover-file.

ii. To embed the secret information in the cover file, the redundant bits in the cover file is replaced by the bits of the secret information.

3. AUDIO STEGANOGRAPHIC METHODS

There have been many techniques for hiding information or messages in audio in such a manner that the alterations made to the audio file are perceptually indiscemible. Common approaches include [7, 12]:

3.1 LSB CODING

A very popular methodology is the LSB (Least Significant Bit) algorithm, which replaces the least significant bit in some bytes of the cover file to hide a sequence of bytes containing the hidden data. That's usually an effective technique in cases where the LSB substitution doesn't cause significant quality degradation, such as in 24-bit bitmaps.

In computing, the least significant bit (LSB) is the bit position in a binary integer giving the units value, that is, determining whether the number is even or odd. The LSB is sometimes referred to as the right-most bit, due to the convention in positional notation of writing less significant digit further to the right. It is analogous to the least significant digit of a decimal integer, which is the digit in the ones (right-most) position.

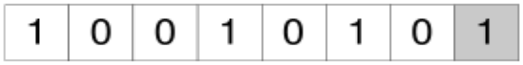

Figure 4: Binary representation of decimal 149

The binary representation of decimal 149, with the LSB highlighted. The MSB in an 8-bit binary number represents a value of 128 decimal. The LSB represents a value of 1. For example, to hide the letter "a" (ASCII code 97, which is 01100001) inside eight bytes of a cover, you can set the LSB of each byte like this:

10010010

01010011

10011011

11010010

10001010

00000010

01110010

00101011

The application decoding the cover reads the eight Least Significant Bits of those bytes to re-create the hidden byte—that is 0110001—the letter "a." As you may realize, using this technique let you hide a byte every eight bytes of the cover. Note that there's a fifty percent chance that the bit you're replacing is the same as its replacement, in other words, half the time, the bit doesn't change, which helps to minimize quality degradation.

Fig 5 illustrates how the message 'HEY' is encoded in a 16-bit CD quality sample using the LSB method. Here the secret information is 'HEY' and the cover file is audio file. HEY is to be embedded inside the audio file. First the secret information 'HEY' and the audio file are converted into bit stream. The least significant column of the audio file is replaced by the bit stream of sectet information 'HEY'. The resulting file after embedding secret information 'HEY' is called Stego-file.

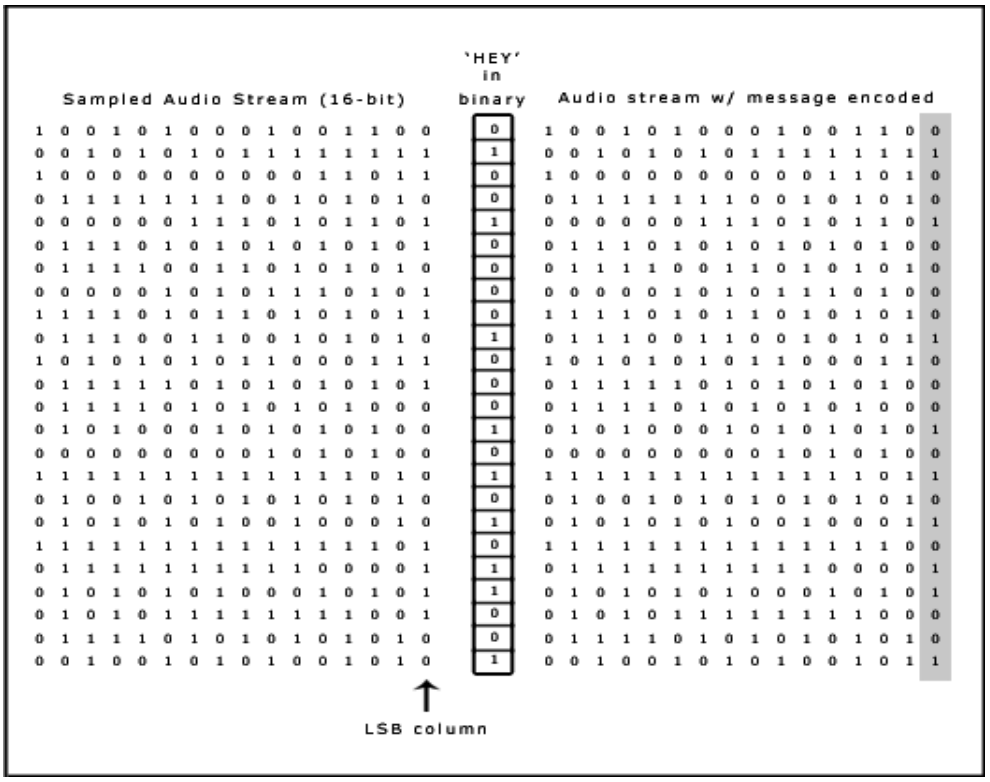

Figure 5. LSB coding example

3.2 PARITY CODING

Parity coding is one of the robust audio steganographic technique. Instead of breaking a signal into individual samples, this method breaks a signal into separate samples and embeds each bit of the secret message from a parity bit. If the parity bit of a selected region does not match the secret bit to be encoded, the process inverts the LSB of one of the samples in the region. Thus, the sender has more of a choice in encoding the secret bit. Figure 6, shows the parity coding procedure.

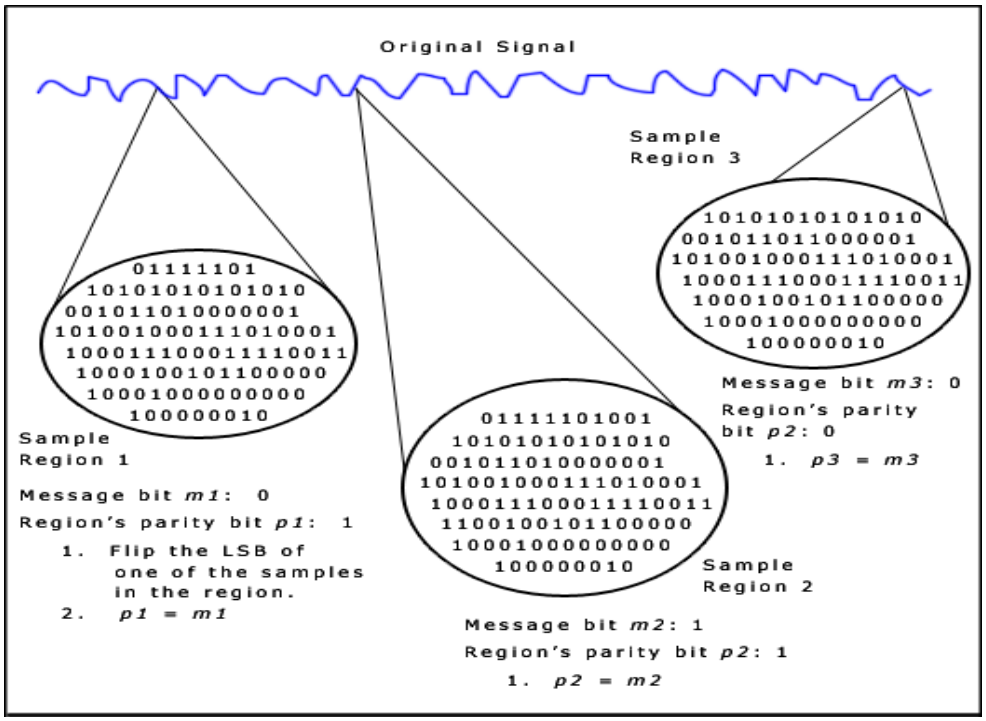

Figure 6. Parity coding

3.3 PHASE CODING

The phase coding technique works by replacing the phase of an initial audio segment with a reference phase that represents the secret information. The remaining segments phase is adjusted in order to preserve the relative phase between segments. In terms of signal to noise ratio, Phase coding is one of the most effective coding methods. When there is a drastic change in the phase relation between each frequency component, noticeable phase dispersion will occur. However, as long as the modification of the phase is sufficiently small, an inaudible coding can be achieved [4, 19]. This method relies on the fact that the phase components of sound are not as perceptible to the human ear as noise is.

Phase coding is explained in the following procedure:

a. Divide an original sound signal into smaller segments such that lengths are of the same size as the size of the message to be encoded.

b. Matrix of the phases is created by applying Discrete Fourier Transform (DFT).

c. Calculate the Phase differences between adjacent segments.

d. Phase shifts between adjacent segments are easily detectable. It means, we can change the absolute phases of the segments but the relative phase differences between adjacent segments must be preserved. So the secret information is inserted only in the phase vector of the first signal segment as follows:

$$phase\_new = \begin{cases} \pi/2 & if \quad message \quad bit = 0 \\ -\pi/2 & if \quad message \quad bit = 1 \end{cases}$$

e. Using the new phase of the first segment a new phase matrix is created and the original phase differences.

f. The sound signal is reconstructed by applying the inverse Discrete Fourier Transform using the new phase matrix and original magnitude matrix and then concatenating the sound segments back together.

The receiver must know the segment length to extract the secret information from the sound file. Then the receiver can use the DFT to get the phases and extract the secret information (consider Figure 4 for phase coding procedure) [20].

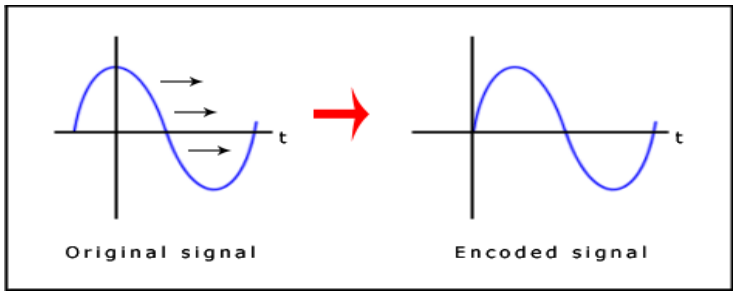

Figure 7. Phase coding

3.4 SPREAD SPECTRUM

In audio steganography, the basic spread spectrum (SS) method attempts to spread secret information across the frequency spectrum of the audio signal. This is similar to a system which uses an implementation of the LSB that spreads the message bits randomly over the entire sound file. However, unlike LSB coding, the Spread Spectrum method spreads the secret information over the frequency spectrum of the sound file using a code which is independent of the actual signal [21]. As a result, the final signal occupies a bandwidth which is more than what is actually required for transmission.

The Spread Spectrum method is capable of contributing a better performance in some areas compared to LSB coding, phase coding, and parity coding techniques in that it offers a moderate data transmission rate and high level of robustness against removal techniques. However, the Spread Spectrum method has one main disadvantage that it can introduce noise into a sound file [16, 19]. The Spread Spectrum steps are shown in Figure 8.

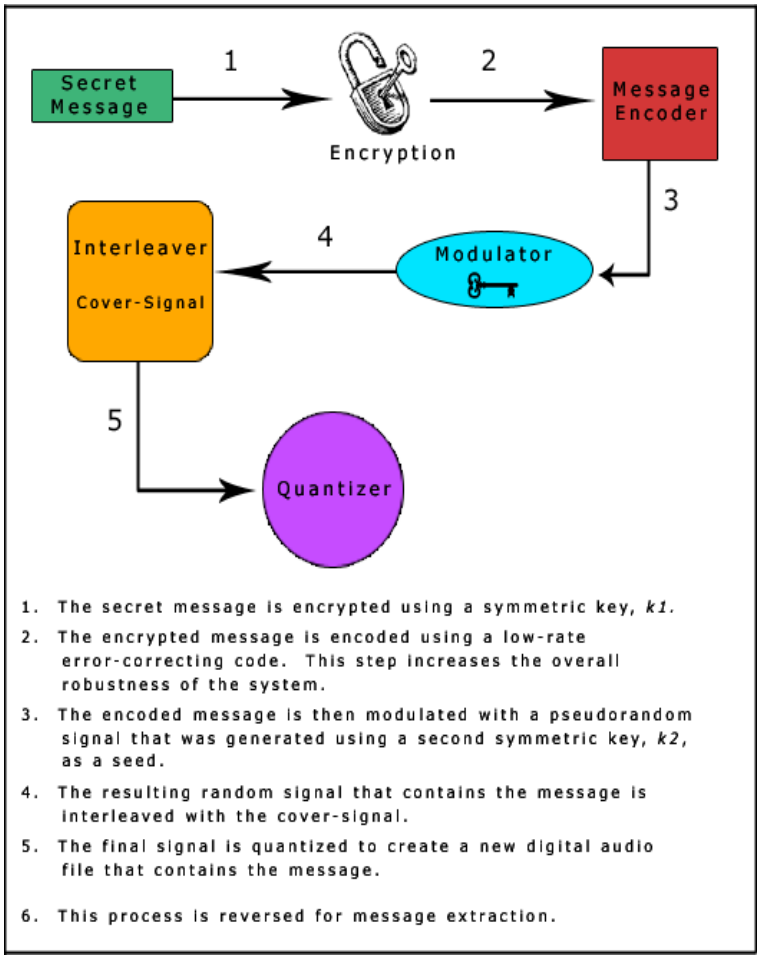

Figure 8. Spread Spectrum (SS)

3.5 ECHO HIDING

Echo hiding technique embeds secret information in a sound file by introducing an echo into the discrete signal. Echo hiding has advantages of providing a high data transmission rate and superior robustness when compared to other methods. Only one bit of secret information could be encoded if only one echo was produced from the original signal. Hence, before the encoding process begins the original signal is broken down into blocks. Once the encoding process is done, the blocks are concatenated back together to create the final signal [5, 20]. Echo Hiding is shown in Figure 9.

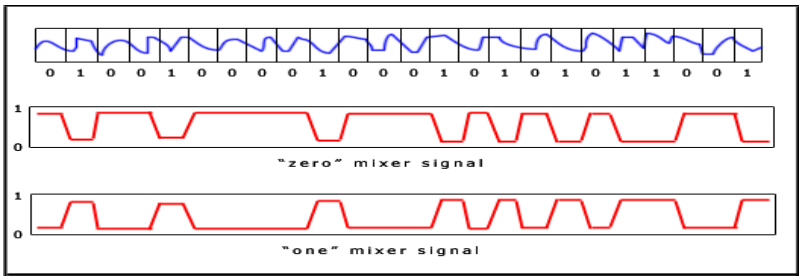

Figure 9. Echo hiding

4. PROPOSED WORK

Here we will discuss the disadvantages of the previous procedure and how those are different with present method. The main disadvantages associated with the use of existing methods like echo hiding, spread spectrum and parity coding are, human ear is very sensitive to noise and it can often detect even the slightest bit of noise introduced into a sound file and another problem is robustness.

Phase coding has main disadvantage of low data transmission rate because of the fact that the secret message is encoded only in the first signal segment. Hence this method is used only when a small amount of data needs to be transferred.

Among different information hiding techniques proposed to embed secret information within audio file, Least Significant Bit (LSB) coding method is the simplest way to embed secret information in a digital audio file by replacing the least significant bit of audio file with a binary message. Hence LSB method allows large amount of secret information to be encoded in an audio file.

Steps to hide secret information using LSB are:

a. Covert the audio file into bit stream.

b. Convert each character in the secret information into bit stream.

c. Replace the LSB bit of audio file with the LSB bit of character in the secret information.

This proposed method provides greater security and it is an efficient method for hiding the secret information from hackers and sent to the destination in a safe and undetectable manner. This proposed system also ensures that the size of the file is not changed even after encoding and it is also suitable for any type of audio file format.

5. AUDIO STEGANOGRAPHIC APPLICATIONS

Audio data hiding can be used anytime you want to hide data. There are many reasons to hide data but most important is to prevent unauthorized persons from becoming aware of the existence of a message. In the business world Audio data hiding can be used to hide a secret chemical formula or plans for a new invention [9, 17].

Audio data hiding can also be used in the non commercial sector to hide information that someone wants to keep private. Terrorists can also use Audio data hiding to keep their communications secret and to coordinate attacks. In the project ARTUS1 which aims to embed animation parameters into audio and video contents [10]. Data hiding in video and audio, is of interest for the protection of copyrighted digital media, and to the government for information systems security and for covert communications [21, 18]. It can also be used in forensic applications for inserting hidden data into audio files for the authentication of spoken words and other sounds, and in the music business for the monitoring of the songs over broadcast radio.

6. CONCLUSION

In this paper we have introduced a robust method of imperceptible audio data hiding. Thus we conclude that audio data hiding techniques can be used for a number of purposes other than covert

communication or deniable data storage, information tracing and finger printing, tamper detection. As the sky is not limit so is not for the development. Man is now pushing away its own boundaries to make every thought possible. So similarly these operations described above can be further modified as it is in the world of Information Technology.

7. ACKNOWLEDGEMENTS

The authors gratefully acknowledge the support for this paper from Department of CSE, RVCE (Rashtreeya Vidyalaya College of Engineering), Bangalore, India and the anonymous reviewers of this paper.

8. REFERENCES

[1] W. Bender, W. Butera, D. Gruhl, R. Hwang, F. J. Paiz, S. Pogreb, "Techniques for data hiding", IBM Systems Journal, Volume 39 , Issue 3-4, July 2000, pp. 547 – 568.

[2] Samir Kumar Bandyopadhyay, Debnath Bhattacharyya, Poulami Das, Debashis Ganguly and Swarnendu Mukherjee, "A tutorial review on Steganography", International Conference on Contemporary Computing (IC3-2008), Noida, India, August 7-9, 2008, pp. 105-114.

[3] Robert Krenn, "Steganography and steganalysis", An Article, January 2004.

[4] Nedeljko Cvejic, Tapio Seppben "Increasing the capacity of LSB-based audio steganography " FIN-90014 University of Oulu, Finland ,2002.

[5] Sajad Shirali-Shahreza M.T. Manzuri-Shalmani "High capacity error free wavelet domain speech steganography" ICASSP 2008

[6] Neil F.Johnson, Z.Duric and S.Jajodia. "Information Hiding Steganography and Watermarking-Attacks and Countermeasures",Kluwer Academic Publishers, 2001

[7] F.A.P.Petitcolas, R.J.Anderson, M.G.Kuhn:"Information Hiding- A Survey", Process of IEEE, vol.87, no.7, pp.1062-1078, July, 1999.

[8] Min Wu, Bede Liu. "Multimedia Data Hiding", Springer- Verlag New York, 2003.

[9] N. Taraghi-Delgarm, "Speech Watermarking", M.Sc. Thesis, Comptuer Engineering Department, Sharif University of Technology, Tehran, IRAN, May 2006.

[10] M. Pooyan, A. Delforouzi, "LSB-based Audio Steganography Method Based on Lifting Wavelet Transform", in Proc. 7th IEEE International Symposium on Signal Processing and Information Technology (ISSPIT'07), December 2007, Egypt.

[11] R.A. Santosa and P. Bao, "Audio-to-image wavelet transform based audio steganography," Proc. of 47th Int. Symposium ELMAR, June 2005, pp. 209- 212.

[12] Xuping Huang, Ryota Kawashima, Norihisa Segawa, Yoshihiko Abe. "The Real-Time Steganography Based on Audio-to-Audio Data Bit Stream",Technical report of IEICE, ISEC, vol.106 pp.15-22, September 2006.

[13] Aoki, Naofumi. "A Band Widening Technique for VoIP Speech Using Steganography Technology", Report of IEICE, SP,106(333), pp.31-36, 2006.

[14] Xuping Huang, Ryota Kawashima, Norihisa Segawa, Yoshihiko Abe International Conference on Intelligent "Information Hiding and Multimedia Signal Processing" © 2008 IEEE.

[15] A. Delforouz, Mohammad Pooyan, "Adaptive Digital Audio Steganography Based on Integer wavelet transform ", IEEE Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2007, 26-28 Nov 2007, pp 283-286.

[16] R. A. Santosa, P. Bao," Audio-to-Image Wavelet Transform based Audio Steganography", 47th International Symposium ELMAR-2005 , 08-10 June 2005, Zadar, Croatia, pp 209-212.

[17] S. Shirali-Shahreza, M. T. Manzuri-Shalmani, "Adaptive Wavelet Domain Audio Steganography with High Capacity and Low Error Rate", IEEE International Conference on Information and Emerging Technologies, 2007, 06-07 July 2007 pp 1-5.

[18] Yincheng Qi, Jianwen Fu, and Jinsha Yuan, "Wavelet domain audio steganalysis based on statistical moments of histogram", Journal of System Simulation, Vol 20, No. 7, pp. 1912-1914, April 2008.

[19] Yin-cheng qi, liang ye, chong liu "Wavelet domain audio steganalysis for multiplicative embedding model" Proceedings of the 2009 International Conference on Wavelet Analysis and Pattern Recognition, Baoding, 12-15 July 2009.

[20] V. Vapnik, "Statistical Learning Theory", John Wiley, 2008.

[21] Mengyu Qiao, Andrew H. Sung , Qingzhong Liu "Feature Mining and Intelligent Computing for MP3 Steganalysis" International Joint Conference on Bioinformatics, Systems Biology and Intelligent Computing 2009.

AUTHORS

Jayaram P is currently doing his Engineering degree in R V College of Engineering Bangalore. He has published many papers in National Conferences. His areas of research are Networking, Operating Systems, Data Structures, Computer Graphics and Mobile Computing.

Ranganatha H R is currently doing his Engineering degree in R V College of Engineering Bangalore. He has published many papers in National Conferences. His areas of research are Algorithms, Distributed Systems, Network security and Business Intelligence.

Anupama H S is working as an Assistant Professor in R V College of Engg Bangalore. She did B E in S.I.T College of Engg Tumkur and M.Tech in J.N.N.C.E College Shimoga, Karnataka, India. Her research of interest are Security, Steganography, Brain Computer Interface and Virtual Keyboard.

.