Volume 4, Issue 5, May 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Designing of Algorithm for Hiding of Multimedia Information in to Colored Image Using Spread Spectrum Method

Ms. Lalita[1], Mr. Sumit Wadhwa[2]
[1]*M.Tech Student, CSE Department*[2]*Assistant Professor,CSE Department*
[1,2]*Samalkha Group of Institution, Kurukshetra University, India*

Abstract: ***In this paper, Implementation of steganography in audio data using Direct Sequence Spread Spectrum method has been presented. Spread Spectrum method is often used to send hidden message through radio waves. The message is transmitted through noise. The same technique can be applied to embed message in audio data. The embedded audio data will be heard as noise. In this paper, the method used is Direct Sequence Spread Spectrum. A key is applied to embed messages into noise. This key is helpful in generating pseudo-random key sequence. We have proposed a Random location selection to embed the data within the cover image pixels. These variations provide a more secure system, making guesses about the bit-rate or message length less feasible. The proposed stego and extraction system uses Direct Sequence Spread Spectrum technique. These are used to increase the security and robustness of the system. The inaudibility of the stego audio and extracted image is assessed by using peak signal-to-noise ratio (PSNR) and normalized correlation measure. MATLAB R2008a vol. 7.6 has been used as an implementation platform.***

Keywords: audio steganography, DSSS, PSNR, spread spectrum.

I. Introduction

In recent years, audio has become aprogressively favoured medium for steganography. However, animportant challenge exists in hiding information in an audio signal, the Human Auditory System. The Human Auditory System is able to detect sound over a wide dynamic range. In addition, humans have an acute sensitivity to additive random noise. As a result of these factors, a human is able to detect changes in a sound file as low as one part in ten million [1].Current steganographic applications with audio media are primarily limited to providing proof of copyright and assurance of content integrity [11].When embedding data in audio media, it is essential to consider the environments in which the data is kept and communicated.

A signal may pass through a variety of transmission surroundings between being sent and received. Examples of four different transmission surroundings are shown in Figure 1 [11]. If the audio media is transmitted only through a digital environment, the file is not modified in any way. Consequently, the file is consistent between sender and receiver. Transmitting in this way places the least constraints on the hiding of the data [11].

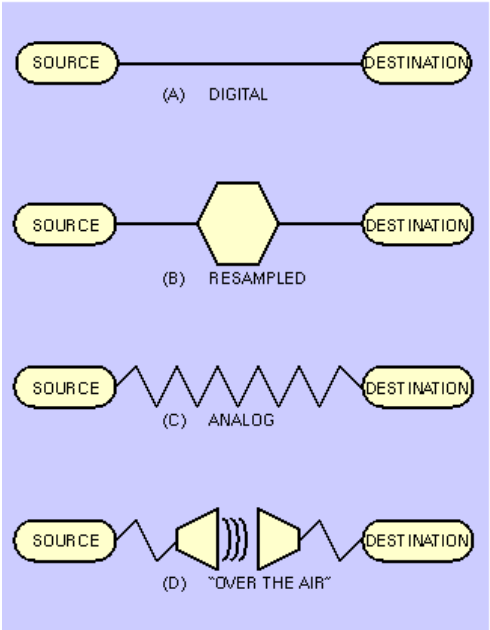

Fig.1: Transmission Environments[11]

Transmitting using re-sampling, as shown in Figure 1b is more problematic since the file is sampled to a higher or lower sampling rate. While transforming in this manner preserves the absolute magnitude and phase of the majority of the signal, the temporal characteristics of the signal is changed [1].The third transmission method involves playing the signal into an analog state and then transmitting the signal on an analog line before re-sampling [11]. In this case, although the phase is preserved, changes occur in the absolute signal magnitude, temporal sampling rate and sample quantization [1].The final transmission environment is the one in which we are most interested since it is the environment that covert communications may be expected to most frequently used. In this case, the signal is played into the air followed by re-sampling with a microphone. This mode of transmission places the highest constraints on the mode of hiding the data since the signal may be subjected to unknown nonlinear modifications. This may cause changes in phase and amplitude, and drift of different frequency components [1,11].

II. Spread Spectrum

Spread Spectrum is a form of Radio Frequency communication. Spread Spectrum techniques intentionally spread the transmitted data signal over a wide frequency range, [2], as shown in Figure 2. The bandwidth used is in excess of the minimum bandwidth required for the data being sent. By Increasing the bandwidth improvements in the signal-to-noise performance are obtained. The fundamental idea behind this process is that, in channels with narrowband noise, increasing the transmitted signal bandwidth results in an increased probability that the information received will be correct [11]. The increase in performance for very wideband systems is called the process gain [2].

The theoretical background explaining the basis of Spread Spectrum technology came with the publication of a paper by Claude Shannon on the mathematical theory of communication [3]. Shannon's theorem is as follows:

$C = W \log2(1 + S/N)$ ……(1)

where C = data rate in bits per second, W = bandwidth (Hz), S = average signal power (W), N = mean white gaussian noise power (W) [11].

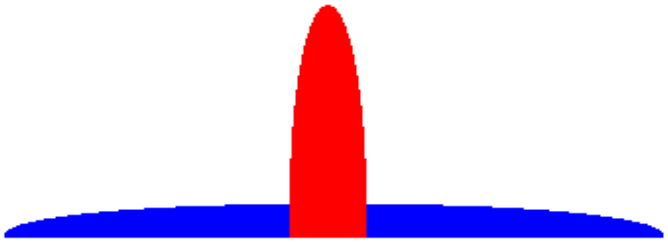

Fig.2: Bandwidth Spreading[11]

It can be seen from the equation that the only options available to increase a channel's capacity are to increase either the bandwidth (W) or the signal to noise ratio (S/N). We can see that there is a "relationship between the ability of a channel to transfer error free information, compared with the signal to noise ratio existing in the channel, and the bandwidth used to transmit the information" [4]. Equation 1 can be manipulated to:

$W = (NC)/S$ ……(2)

From equation 2, it can be observed that for any given noise to signal ratio, a low information error rate can be achieved by increasing the bandwidth used to transfer the information.

III. Spread Spectrum Techniques

Spread Spectrumstechniques include Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS), and Time Hopping Spread Spectrum. Each technique differs in its implementation and has certain pros and cons. [5].

A. Direct Sequence Spread Spectrum (DSSS)

The basic principle behind the Direct Sequence Spread Spectrum (DSSS) technique is the modulation of the RF carrier with a digital code sequence. A two-stage process is used to produce the DSSS. During the first stage, data is spread across the spectrum. This is achieved by dividing the data stream into a symbol stream (small pieces of one bit or more) and then allocating each part of the divided data to a frequency channel across the spectrum [6,7,11].Figure 3, [8], shows the time and frequency domains of the original data, the result of the stage 1 spreading and the final modulated data. By modulating the carrier with the digital code sequence, the signal produced is centered at the carrier frequency. The resulting spectrum has a $(\sin x/x)^2$ form as can be seen in Figure 6 which shows a DSSS Spectrum produced using a Binary Phase Shift Key (BPSK) to modulate the data with the code sequence [2]. Although DSSS has very good noise and anti-jamming performance and is very difficult to intercept, but it have some disadvantages [11]. The circuitry required to produce the spectrum is complex, it requires a large bandwidth channel with relatively small phase distortions and requires a long acquisition time since the PN codes are long. Also, DSSS suffers from what is known as a "Near-Far" effect [11]. This effect occurs when an interfering transmitter is much closer to the receiver than the intended transmitter. Consequently, proper data detection is not possible [9].

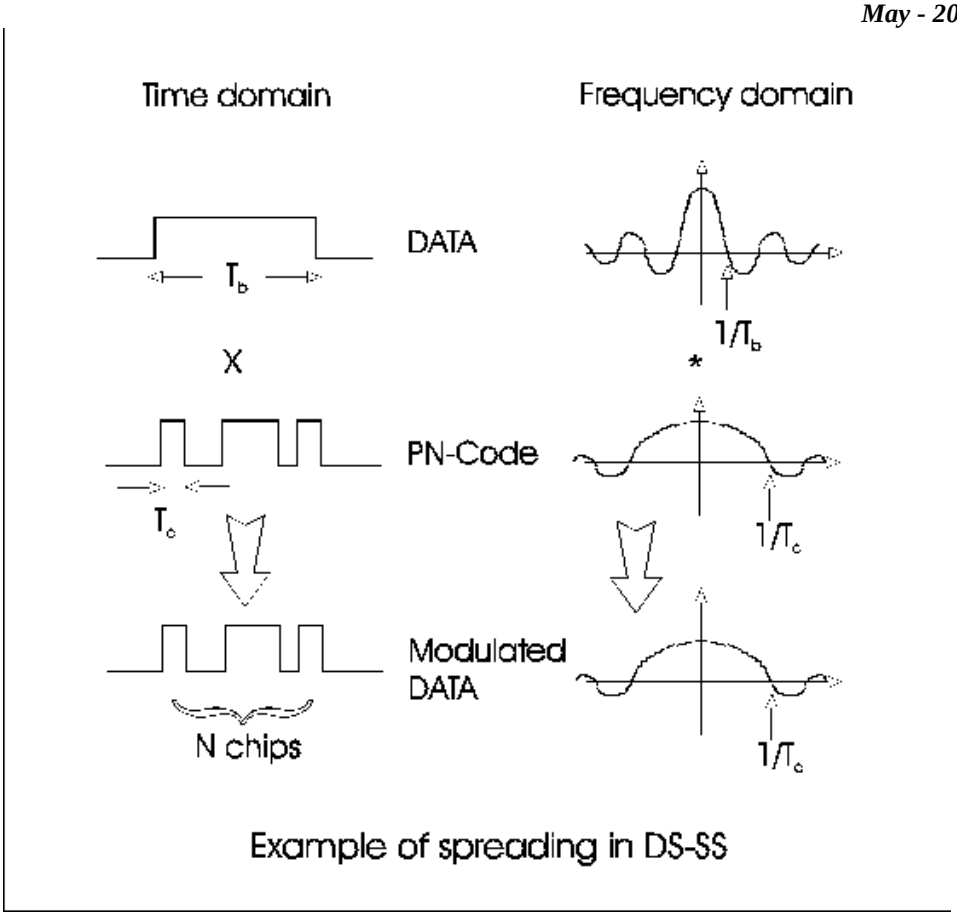

Fig.3: Time and frequency domains of the original data, the result of the stage 1 spreading and the final modulated data [11].

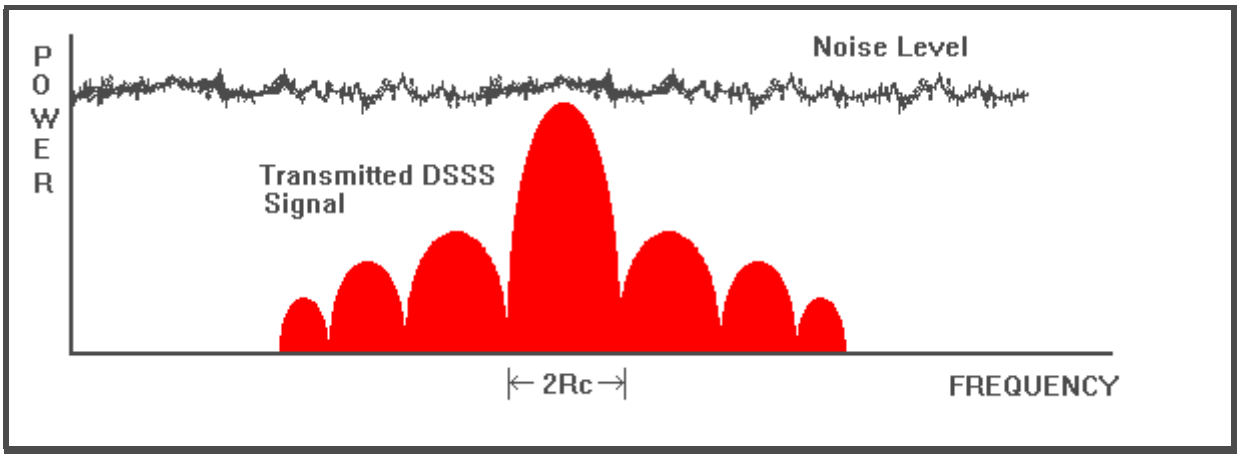

Fig.4: BPSK Direct Sequence Spread Spectrum [11].

B. Frequency Hopping Spread Spectrum (FHSS)

Another, Spread Spectrum technique is the Frequency Hopping Spread Spectrum (FHSS). FHSS is not as affected by the "Near-Far" effect. The basic principle behind the Frequency Hopping Spread Spectrum (FHSS) technique is that the carrier frequency is periodically modified (hopped) across a specific range of frequencies. The frequencies, across which the carrier jumps is the spreading code. The shifting pattern is determined by the chosen code sequence (frequency shift key – FSK). The amount of time spent on each hop is known as the dwell time and is in the range of 3ms-100ms [10].Two types of Frequency Hopping signals may be used, slow hopping and fast hopping. With slow hopping, the hopping rate is smaller than the message bit rate, meaning that in one hop, one or more data bits are transmitted [11]. While in fast hopping, one data bit is divided over more than one hop (the hopping rate is greater than the message bit rate) [8, 10].

IV. Related Works

AlaaIsmat Al-Attili et al. propose a method using the space between frames of mp3 file. Limitation of this method isthat the MP3 file must be of CBR type only. But the suggested method satisfies the capacity and complexity ofsteganography

properties. In addition, the suggested method for hiding is robust against noise. It is also consideredhighly secure since data is encrypted using RSA algorithm before embedding data which makes the system secureespecially against passive attack [12].Quantized frequency domain embedding and reversible integer transformsSos S. Agaian et al. present two algorithms for secure digital audio steganography. In the first algorithm that is calledQuantized-frequency Secure Audio Steganography algorithm (QSAS), they use classical unitary transforms withquantization in the transform domain to embed the secure data. In the second algorithm that is called Integer Transform based Secure Audio Steganography (ITSAS),they use a reversible integer transform to obtain the transform domain coefficients. The QSAS algorithmhas lower embedding capacity but has much better SNR values. The ITSAS algorithm is preferred as it is reversible,simple, and efficient with acceptable SNR values. Two novel methods have been proposed by H.B.Kekre et al., one is considering parity of the digitized samples ofcover audio and the other is considering the XOR operation.Considering Parity method uses LSB coding technique for data hiding in audio. However, instead of directly replacingLSBs of digitized samples with the message bits, it first checks the parity of the samples and then carries out dataembedding.Using XORing of LSB's method performs XOR operation on the LSBs and then depending on the result of XORoperation and the message bit to be embedded, the LSB of the sample is modified or kept unchanged. The methoddescribed below performs XOR operation on first 2 LSBs. The XORing can be further expanded to 3 LSBs, 4 LSBsupto 16 LSBs so as to increase the level of encryption.From experimental results, it is seen that the proposed methods are effective. From listening tests, no difference isfound between the original audio signal and the stego audio signal. The hidden information is recovered without anyerror. Also, this approach increases the capacity of the cover audio by as much as 8 times and provides robustencryption [13].MazdakZamani et al. propose the GA for optimizing the steganography using LSB. A new approach is proposed toresolve two problems of substitution technique of audio steganography. First problem is having low robustness againstattacks which try to reveal the hidden message and second one is having low robustness against distortions with highaverage power. Proposed solution is using GA. An intelligent algorithm will try to embed the message bits in thedeeper layers of samples and alter other bits to decrease the error and if alteration is not possible for any samples itwill ignore them. Using the proposed genetic algorithm, message bits could be embedded into multiple, vague anddeeper layers to achieve higher capacity and robustness [14].NedeljkoCvejic et al. present another high bit rate LSB audio watermarking and steganography method. The basicidea of the proposed LSB algorithm is watermark embedding that causes minimal embedding distortion of the hostaudio. Using the proposed two-step algorithm, watermark bits are embedded into higher LSB layers, resulting inincreased robustness against noise addition or MPEG compression. Listening tests showed that the perceptual qualityof watermarked audio is higher in the case of the proposed method than in the standard LSB method. The results ofsubjective tests showed that perceptual quality of watermarked audio, if embedding is done using the novel algorithm,is higher in comparison to standard LSB embedding method[15].Ajay.B.Gadicha1 explores another 4th bit rate LSB audio steganography method that reduces embedding distortion ofthe host audio. Using the proposed algorithm, Message bits are embedded into 4th LSB layers, resulting in increasedrobustness against noise addition [16].

V. Methodology

1. Reading and converting of cover audio signal and watermark image into 2D matrix.
2.Calculation of size of matrix in terms of rows and column.
3.Conversion of watermark matrix into binary matrix.
4.Getting of spreading size by multiplying spreading factor i.e. 2 with total number of elements of binary watermark matrix and generation of a random binary key sequence according to spreading size, so as to provide security.
5.Now, Encoding of watermark matrix by Binary XORing of row vector watermark matrix with key sequence and then encoded watermark matrix has a double size as compared to that of original.
6.Next step is, Selection of a block size, which must be suitable to the size of first part of cover image matrix.
7.Division of cover image matrix into first and second part and segmentation of first part matrix into an array of sub-matrix.
8.Each sub-matrix has a specific number of elements which depends upon block size.
9.Apply Discrete Cosine Transform (DCT) on each element of all the sub-matrices and embedding of watermark by multiplication of encoded watermark matrix with cosine transform matrix.
10.Now, Reconstruction of matrix by application of inverse discrete cosine transform on resultant matrix and joining of reconstructed matrix with second part of cover image matrix and getting of embedded image.
11.Plotting of frequency coefficients of both audio cover signals, so as to make comparison.

VI. Results

For simulations, MATLAB R2008a tool is used. The results or output parameters derived are: value of PSNR, computational time and value of normalized correlation and figures representing input and output from the simulation. First two figures are derived from simulation for embedding of watermark image in cover audio signal Fig. 5 has been partitioned into two parts, first part has the plot of frequency coefficients of cover audio signal and other part has the plot of frequency coefficients of watermarked audio signal to compare cover and watermarked audio signal. It can be easily seen that both have almost similar characteristics, which can be proved by Normalized correlation value i.e. 0.9913. Fig. 6 is the snapshot of command window, shows the value of other two mentioned parameters. The PSNR value of embedded audio signal is 85.7760 dB. The time which elapsed during whole simulation is 1.5469s. Next two figures have been driven from the extraction simulation of watermark. Fig. 7 is also partitioned into two parts, so as to compare

original watermark image and extracted watermark image. The similarity between both images can be described by Normalized correlation value i.e. 0.9009. Fig. 8 is the snapshot of command window, shows the value of other two mentioned parameters. The PSNR value of extracted watermark is 61.9850dB. The time elapsed during whole simulation is 1.0469s. If we compare both the watermark analytically, then they have no difference, which means that, it is a good sign for proposed method in terms of correlation. Table 1 indicates the values of PSNR of different existing methods and proposed method.

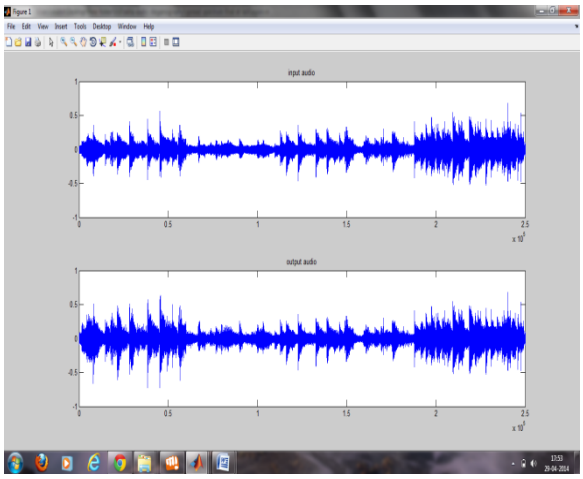

Fig. 5 comparison original cover audio signal and embedded audio signal

Fig. 6 snapshot of command window for embedding of watermark

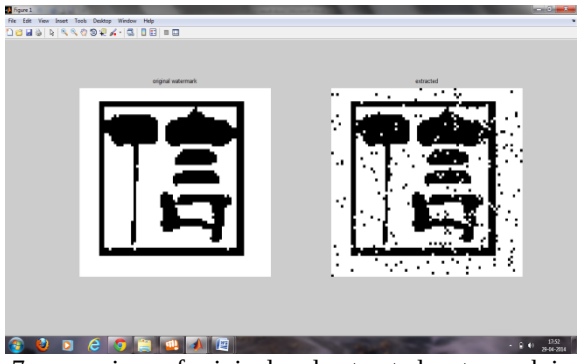

Fig. 7 comparison of original and extracted watermark image

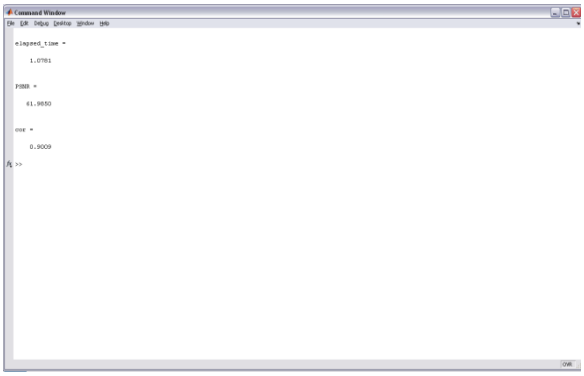

Fig. 8 snapshot of command window for extraction of watermark

Table I Comparison of various techniques for PSNR of extracted watermark

Technique	PSNR
Simple Low Bit Encoding	42.0815
Modified LSB	10.5010
Parity Coding	41.5486
Echo Hiding	44.8130
Proposed method	61.9850

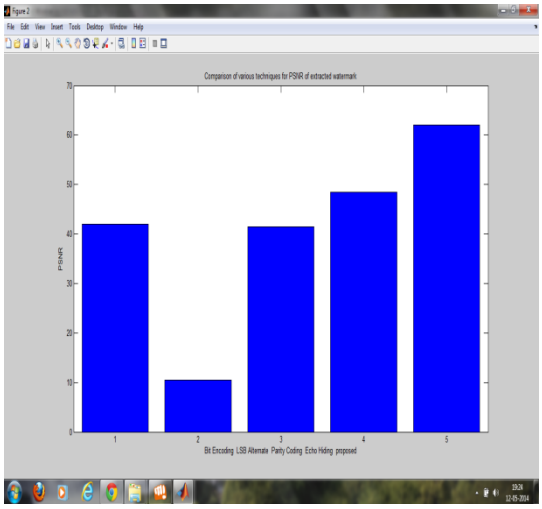

Fig.9 bar chart for comparison of PSNR values of existing methods with that of proposed method

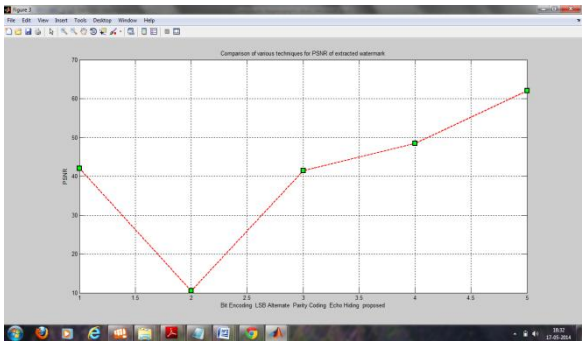

Fig.10 plot for comparison of PSNR values of existing methods with that of proposed method

VII. Conclusion and Future work

It can be concluded from the results that proposed methodology is much efficient in various terms PSNR, correlation with original watermark, invisibility and computational time as compared to existing audio steganography methods. Proposed method is based on advanced spread spectrum methodology, the PSNRis85.7760 dB and 61.9850dB and normalized correlation which is0.9913and 0.9009very high and computational time 1.5469sec and 1.0469sec is very low. Performance evaluation results shows that advancement of spread spectrum methodology improved the performance of the already existed watermarking algorithms that are based solely on the normal spread spectrum methodology. We can conclude from the results that this algorithm is much better for invisible watermarking and has is advantageous for some common signal processing operations. In Future, this work can be extended by improving the performance of methodology by making it more robust and less complex for low frequency audio signal. We can also reduce time consumption for embedding as well as for extraction of watermark.

REFERENCES

[1] W. Bender, D. Gruhl, N. Morimoto and A. Lu, Techniques for Data Hiding, IBM Systems Journal, Vol. 35, Nos 3 & 4, 1996, pp 313-336.

[2] Randy Klassen, Spread Spectrum – A Brief Tutorial, Omnex Control Systems Inc, 2003.

[3] James A. Vincent, Voice Link Over Spread Spectrum Radio, Electronics World and Wireless World, September/October 1993.
[4] Robert C. Dixon, Spread Spectrum Systems with Commercial Applications, third edition, Wiley and Sons, 1994, ISBN 0-471-59342-7.
[5] George R. Cooper, Clare D. McGillem, Modern Communications and Spread Spectrum, McGraw-Hill Book Company, 1986.
[6] MadhaviChalamalasetti, Direct Sequence Spread Spectrum, October 2003 URL: http://www.bsnl.in/Telecomguide.asp?intNewsId=21019&strNewsMore=more.
[7] KavehPahlavan and Allen H. Levesque, Wireless Information Networks, Wiley and Sons, March 1995.
[8] Jack Glas, The principles of Spread Spectrum communication, URL: http://cas.et.tudelft. nl/~glas/ssc/techn/techniques.html.
[9] Sorin M. Schwartz, Frequency Hopping Spread Spectrum (FHSS) vs. Direct Sequence Spread Spectrum (DSSS) in Broadband Wireless Access (BWA) and Wireless LAN (WLAN), Alvarion Professional Education Center (ALPEC), version 7, December 2001.
[10] WitoldJachimczyk, Spread Spectrum, http://webpages.charter.net/witek/ss/ss.html.
[11] Nick Sterling, Sarah Summers, Sarah Wahl ,"Spread Spectrum Steganography" http://paperedu.org/docs/index-5772.html
[12] AlaaIsmat Al-Attili, OsamahAbdulgader Al-Rababah, New technique for hiding data in audio file, IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.7, July 2010.
[13] H.B.Kekre, ArchanaAthawale, Swarnalata Rao, Uttara Athawale, Information Hiding in Audio Signals, International Journal of Computer Applications (0975 – 8887) Volume 7– No.9, October 2010.
[14] MazdakZamani, Azizah A. Manaf, Rabiah B. Ahmad, Akram M. Zeki, and Shahidan Abdullah, A Genetic-Algorithm-Based Approach for Audio Steganography World Academy of Science, Engineering and Technology 54 2009.
[15] NedeljkoCvejic, TapioSeppänen, Increasing Robustness of LSB Audio Steganography Using a Novel Embedding Method, Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04).
[16] Ajay.B.Gadicha1, Audio Wave Steganography, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-1, Issue-5, November 2011.

