Multi Carrier Steg against Omni Attacks

R.Amirtharajan
Assistant Professor
School of Electrical & Electronics Engineering
SASTRA University

K.Thenmozhi
Associate Dean ECE
School of Electrical & Electronics Engineering
SASTRA University

R.John Bosco Balaguru
Associate Dean Research
School of Electrical & Electronics Engineering
SASTRA University

ABSTRACT
Information is considered as the most valuable resource in today's data-centric world. In recent times there has been a prodigious growth in information transmission. Parallel to it the data hiding techniques have also developed to sustain information authentication and confidentiality. Traditionally data was hidden in covers such as text, images and audio. But, all these enclosed the data before transmission, thereby creating a necessary evil of time lag between information origination and information transmission. This paper proposes a novel steganographic methodology to overcome the drawback with the help of modern multiplexing technology. Here the physical layer of the Orthogonal Frequency Division Multiplexing (OFDM) is used to embed data. Observations are made by testing this methodology along with Additive white Gaussian Noise and random noise. The experimental results validate the superiority of this data hiding scheme, while retaining the normal functionality of the OFDM technique. This just-in-time data hiding method works well in random noise channel and AWGN channel and the result are presented.

General Terms
Information Security.

Keywords
BPSK, Steganography, OFDM.

1. INTRODUCTION
Traditionally information hiding schemes embed data into image, audio, video etc [1, 2, 3]. These kinds of schemes are called water marking. This is used for the purpose of copyright protection, authentication and authorized access control [3]. Water marking schemes [3] have been proposed in spatial [1, 2, 3] and spectral domain [3]. Spatial domain based texture characteristic methods are easily implemented but have worse performance than the spectral domain based methods, that usually embed into the DCT and DWT[5] coefficients. Several other techniques have been proposed for data hiding such as Embedding information into FIR filter [6], convolution code based information hiding [9] and multiple description coding [4].

Nowadays the technique that draws attention is OFDM [7, 8]. It is a multiple carrier transmission technique which exhibits excellent bandwidth utility and efficient interference rejection. Another advantage of OFDM is that it facilitates easy implementation. The modulation schemes used in subcarriers are QAM or MPSK. The modulation operation could be performed by IFFT and the demodulation operation can be carried out by FFT. It eliminates the use of multiple oscillators and band pass filter groups thereby reducing the system cost. One more advantage of OFDM is that it can effectively resist multipath interference and fading. All of these have given the OFDM a revert position in the modern multi carrier communication environment. However the need for precise synchronization and high Peak-to-Average Ratio (PAPR) compels the amplifier to have better performance which is a big disadvantage for the OFDM scheme.

Orthogonal Frequency Division Multiplexing [OFDM] is an improved and efficient version of normal Frequency Division Multiplexing [FDM] scheme. In normal FDM systems, the available frequency bandwidth is divided into sub bands or channels and each user is allocated a single channel. Each user, therefore, can transmit and receive in one unique channel but reuse of channel bandwidth is not possible in FDM scheme. Also FDM requires non overlapping frequency bands for each user. Hence, although FDM is widely used for single carrier transmission, it is not efficient for multi carrier transmission. Also more band width is wasted as Guard bands must be used to avoid the overlapping.

An OFDM symbol consists of a sum of orthogonal sub carriers each modulated using Quadrature Amplitude Modulation [QAM], Quadrature Phase Shift Keying [QPSK] or Phase Shift Keying [PSK]. The incoming serial data stream is converted into a number of parallel bit streams. These streams are allowed to modulate the orthogonal sub carriers and are transmitted through the channel. The individual frequency spectrum of sub carriers may overlap. At the maximum of each sub carrier frequency spectrum, all other sub carrier frequency spectrum is zero. The function of an OFDM receiver is to calculate the frequency spectrum values at those points corresponding to the individual sub carrier maxima. Thus it can demodulate each sub carrier frequency are that is free from other sub carrier frequencies. The pulse shape of OFDM is in frequency domain. The Inter Carrier Interference occurring due to this is eliminated by having maximum of one the sub carrier frequency spectrum corresponding to zero crossing of others.

2. METHODOLOGY
In the OFDM system the serial baseband signal is transformed into parallel basebands, and then in each of the subcarriers, one baseband signal is mapped into one complex number. The description of the OFDM baseband model is as follows. The basic principle of OFDM is to split a high rate data stream into a number of lower rate streams that are transmitted over overlapped but orthogonal subcarriers. The base band signal is mapped into complex numbers, converted from serial to parallel, then is transformed using N-point inverse Fast Fourier Transform to produce N dimensional signal in the time domain. By doing so,

the frequency-selective channel is converted into N parallel frequency-flat sub channels. Since the subcarriers are orthogonal with one another, overlapping between frequency spectrum corresponding to the different subcarriers is allowed, which enhances the bandwidth efficiency. Furthermore the N dimensional signal is converted to serial data stream by parallel-to-serial (P/S) converter. In the next stage the cyclic prefix is added to the modulated and serialized signal to resist the ISI and inter carrier interference. The final phase is Digital to Analog (D/A) conversion with band limiting filter option. Now the serial data is ready for transmission. At the receiver the process is reverted to recover the message.

2.1 Proposed information hiding method

This paper proposes the exploitation of OFDM technique for information hiding in wireless systems. Usually this technique will be used only for high speed data transmission. The next two sections discuss the procedure for embedding and extracting the data.

2.1.1 Information embedding

For implementing steganography in the physical layer of the OFDM, signal mapping scheme is employed. Data is modulated using BPSK scheme. Embedding process is carried out later in the modulated wave form. User provides the data to be embedded and also a phase shift. The user data is converted into binary format. The previously modulated wave serves as a carrier for user data. Here also BPSK modulation is used with a slight change. Normally in BPSK 180 degrees phase shift is used when there is a change in the input data. But here a user defined phase shift is utilized instead of the conventional 180 degree phase shift.

For example consider the case of two users. Each will specify a particular phase shift say $\phi_1 and \phi_2$ Let us assume that s(t) be the wave form. The above technique is implemented as follows. 'T' is the time period of the original carrier waveform and the modulation waveform is sampled at that interval to embed the data. But the sampling process will start at different points for each user. For the first user it is at T/2 and for the second it is at T/3. So the next sampling interval for user1 is 3T/2 and for user2 is 4T/3 and correspondingly according to the data phase shift is implemented. Data embedding is done by user1 and user2 in m1 and m2 respectively.

$S(t) = \text{Sin}(\omega t)$

For user 1

$S(t) = \text{Sin}(\omega t + \phi_1)$ if m1=1

$= \text{Sin}(\omega t)$ if m1=0

$S(t) = \text{Sin}(\omega t + \phi_2)$ if m2=1

$= \text{Sin}(\omega t)$ if m2=0

2.1.2 Information Extraction

In the receiver side, the embedded data and traditional data are extracted separately from the modulated signal. First embedded data is extracted and then the traditional one. For extracting the embedded data the phase shift provided by the user and the starting should be known. This ensures the security and confidentiality of the hidden data. During the process of extraction, the phase shift from the starting point is tracked. Whenever there is a phase shift, correspondingly a binary zero or one is taken. Thus whole of hidden data is extracted in the binary form. The data after extraction is converted into ASCII form to obtain the original embedded data.

The remaining section explores the working of the integral parts of the information hiding in OFDM methodology.

2.2 Block Diagram of the proposed system

The general schematic of the proposed system is shown in Fig 1.

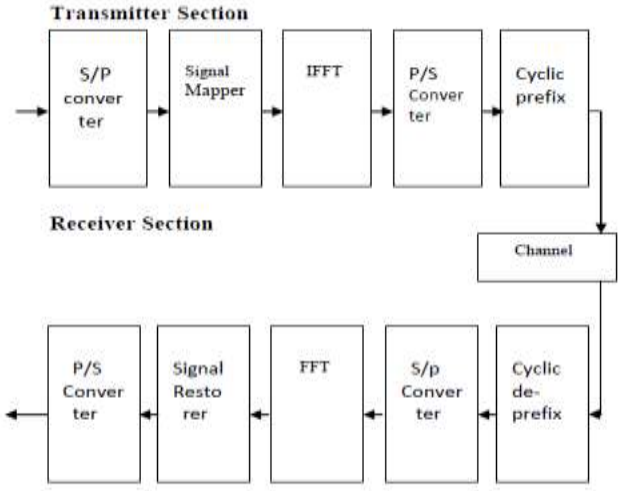


Figure 1. Block diagram of the proposed system

2.2.1 Serial to Parallel converter:

A serial to parallel conversion stage is required to convert the input serial bit stream to the data to be transmitted in each OFDM symbol. The data allocated to each symbol depends on the modulation scheme used and the number of sub carriers.

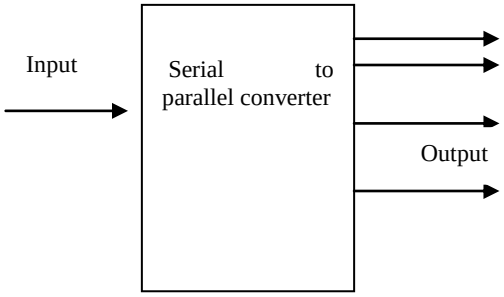


Figure 2. Serial to parallel converter

2.2.2 Signal Mapper:

The signal mapping is done here and it serves to achieve orthogonality between sub carriers. Thus the bandwidth of the channel is completely utilized and about 50% of the bandwidth is conserved.

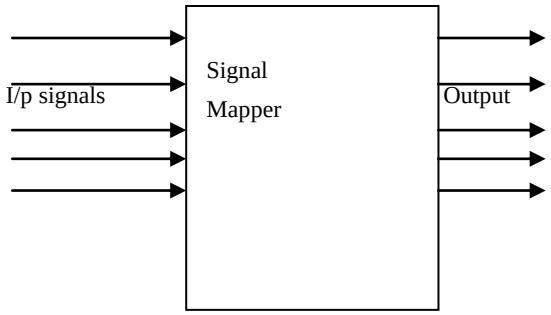


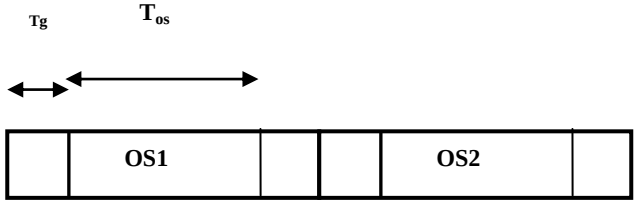
Figure 3. Signal mapper

2.2.3 IFFT:

Parallel data streams are passed into the Inverse Fast Fourier Transform [IFFT] block. IFFT provides a way of ensuring that the carrier signals produced are orthogonal. IFFT converts complex data points, of length in power of 2, into time domain signal of the same number of points. After this conversion, the parallel to serial converter reinstates the serial form of the signal.

2.2.4 Cyclic Prefix:

When multipath channels are involved, Orthogonality of the carrier is lost generating Inter Carrier Interference (ICI). ICI is eliminated by extending the OFDM symbol cyclically in the Guard time (cyclic prefix CP). A copy of the last part of the symbol added at the beginning of the Transmitted symbol. Adding CP can restore the orthogonality. Length of the CP is larger than multipath delay spread.



OS1, OS2 - OFDM Symbols
T_g - Guard Time Interval;
T_s - Data Symbol Period
T_{os} - OFDM Symbol Period - N * T_s

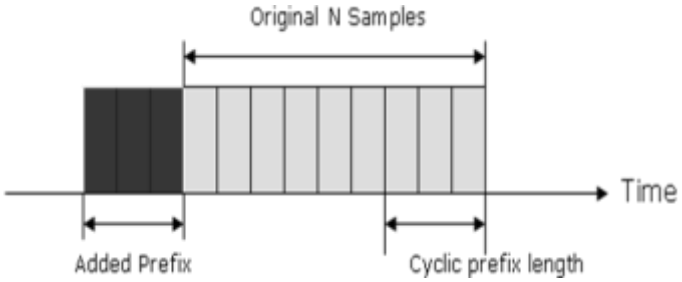


Figure 4. Cyclic prefix

2.2.5 FFT:

Fast Fourier Transform (FFT) is an advanced form of the Discrete Fourier Transform (DFT). The FFT use some clever algorithms to perform the same processes in DFT in a much less time than DFT. The FFT converts the time domain signal into its equivalent frequency domain spectrum.

2.2.6 Cyclic De-prefix:

In the receiver side the added cyclic prefix in the transmitter side has been eliminated as shown in Fig 5. Thus, the normal transmitted symbol is being retrieved.

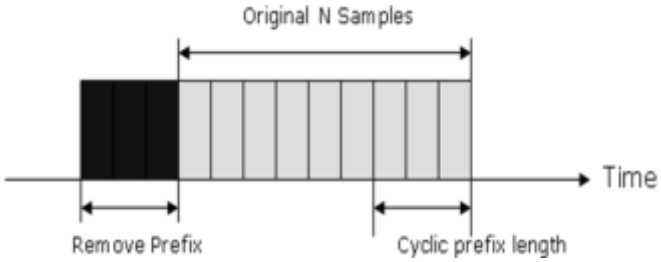


Figure 5 Cyclic de-prefix

2.2.7 Phase shift technique:

The phase shift given as input by the user is added with the conventional 180 degree phase shift of BPSK technique and the new phase shift obtained is used for modulation.

2.2.8 Spread spectrum technique:

It is the process of spreading the bandwidth of a narrow band signal across a wide band of frequencies. In this technique, hidden data is spread throughout the cover-image making it harder to detect. This can be accomplished by adjusting the narrowband waveform with a wideband waveform. After spreading, the energy of the narrowband signal in any frequency band is low and therefore it is complicated to detect which increases the security to the user data.

In spread spectrum image steganography, the message is embedded in noise and then combined with the cover image to produce the stego image. Since the power of the embedded signal is much lower than the power of the cover image, the embedded image is not perceptible to the human eye or by computer analysis without access to the original image.

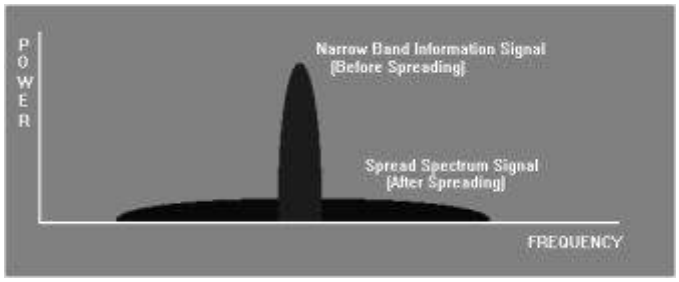


Figure 6: spread spectrum technique

3. Results & Discussion

To illustrate the concept, the input is generated through a signal generator (data input) .Fig. 7 shows the generated input signal.

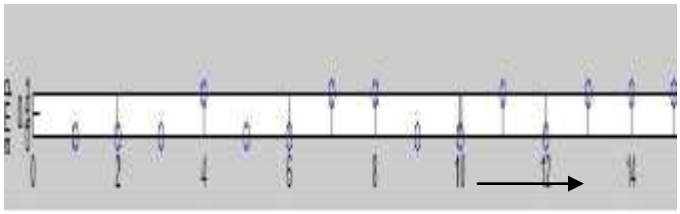


Figure 7. Input bit sequence

The proposed methodology uses the BPSK (binary phase shift keying) technique for modulation. In this technique, 180 degree phase shift is used for modulating the binary bit stream(1's and 0's). Fig. 8 shows the two waves that are 180 degree phase shifted.

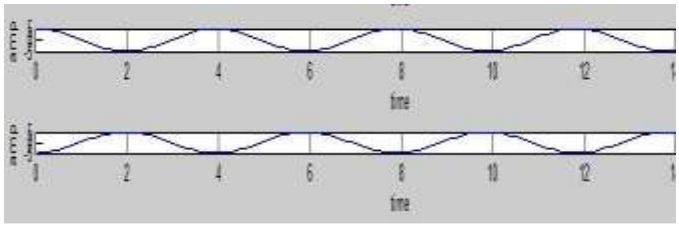


Figure 8. Carrier wave forms for modulation

The present work utilizes the phase shift method for hiding the data. The phase shift provided as input by the user is added with the conventional 180 degree phase shift of the BPSK scheme. Fig. 9 shows the carrier waveform after adding the user phase shift of 15 degree with normal 180 degree phase of BPSK.

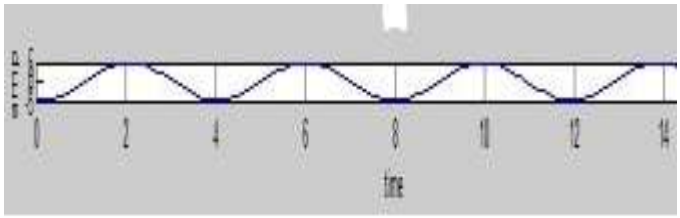


Figure 9. Carrier wave form after implementing user phase shift

The above generated signal is phase shifted by 180 degree and both signals are employed for modulation. Fig. 10 shows the phase shifted waves and the modulated wave.

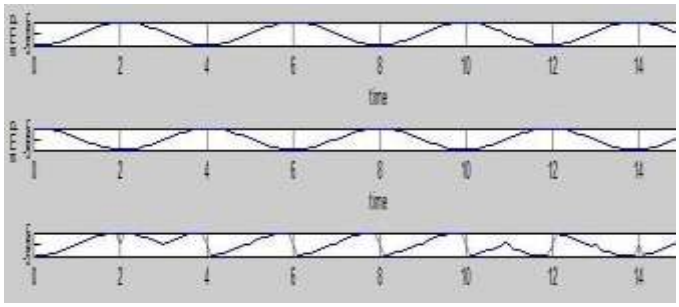


Figure 10. Modulated wave form

In the proposed information hiding system, the user data is embedded on normal OFDM transmitted signal. The ASCII input data from the user is converted to binary form. The binary stream is modulated with the phase shifted carriers generated above after getting the phase shift from the user. After modulation, the signal is transmitted. Fig. 11 shows the sample.

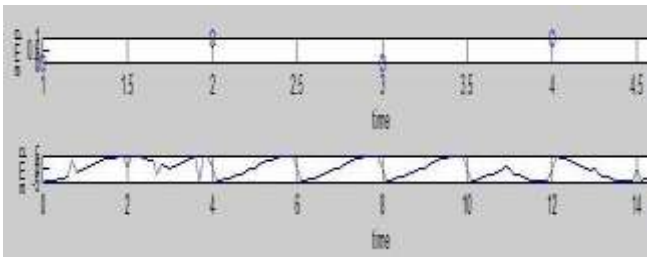


Figure 11. Modulated wave form after embedding data

In fig 11 the first wave is the binary representation of the given ASCII input. The second wave is the modulated wave.

At the receiver side, for retrieving the transmitted data, the phase shift used in the transmitter should be known. Based on the phase shift, the data extraction is done and is converted back to ASCII format. Fig 12 shows the retrieved data and also the retrieved random generated signal.

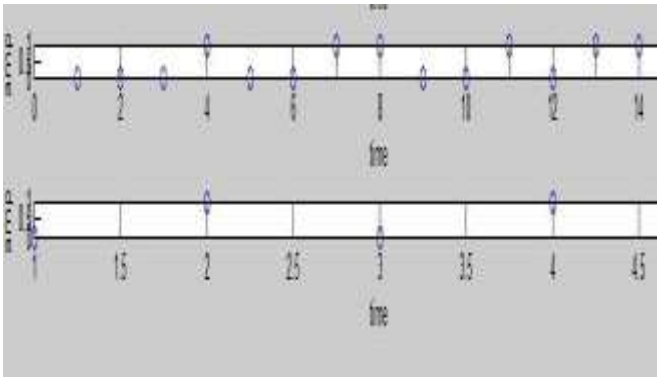


Figure 12. At receiver after extracting original data and embedded data

A simulation has been performed with image as the input data, Fig. 13 depicts the obtained results.

Transmitted image: Received image:

Figure 13. Transmitted and received images over OFDM channel Sample Results

Fig. 14 shows an OFDM transmitter and receiver waveforms using random generator as the input.

The first wave is randomly generated wave. Here a 16 bit random sequence is used. Bit sequences of 32-bit, 64bit etc can also be used.

The second wave shows the BPSK modulated wave, and next is the 180 degree phase shifted of the above. These 2 waves are used as carriers for modulating '1' and '0' respectively.

The fourth wave is the BPSK modulated wave of randomly generated bit sequence using the 180 degree phase shifted carriers(conventional BPSK modulation).

Next two represents the IFFT (Inverse Fast Fourier Transform) signal and FFT (Fast Fourier Transform) signal.

The final wave represents the retrieved signal which is identical to the transmitted signal.

3.1 Results-wave forms of OFDM internal blocks :

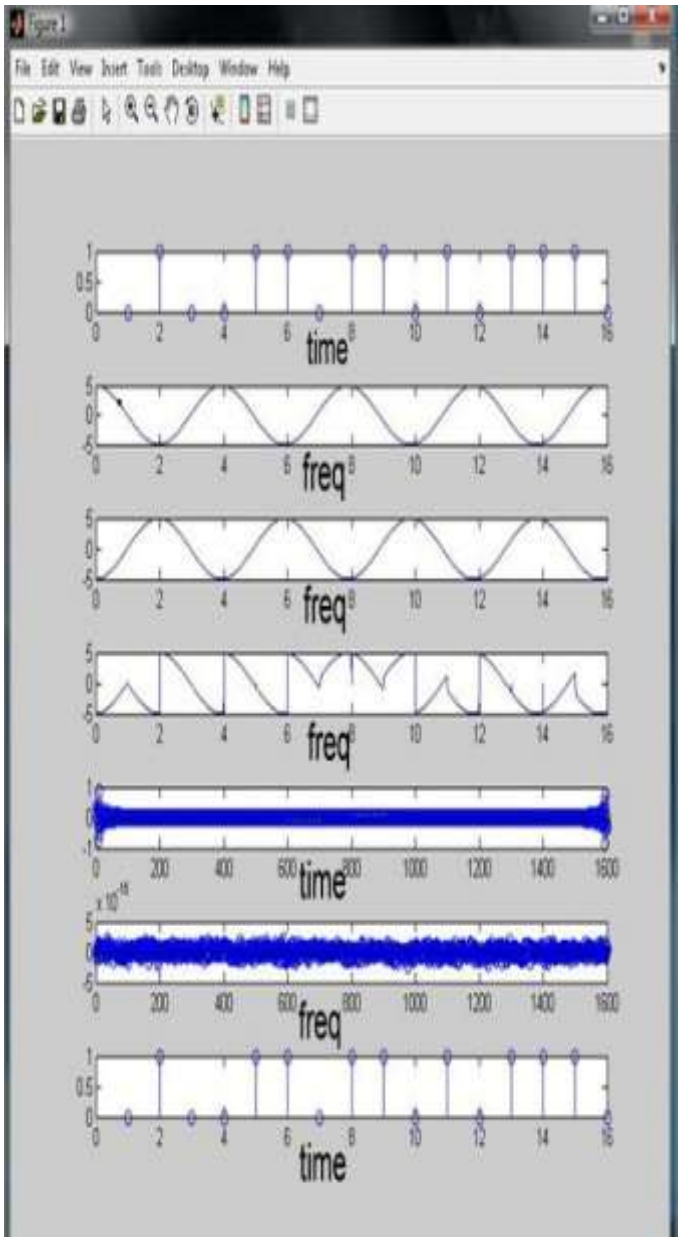


Figure 14. Output at each internal block

3.1.1 Time domain representation of OFDM output:

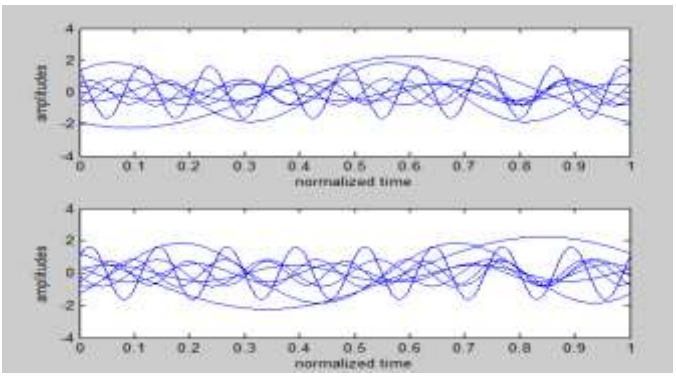


Figure 15: Time domain representation

The OFDM symbols are plotted as function of normalized time as shown in the above figure. The various signal amplitudes of different frequency components of the symbols are observed.

3.1.2 Sample output after embedding

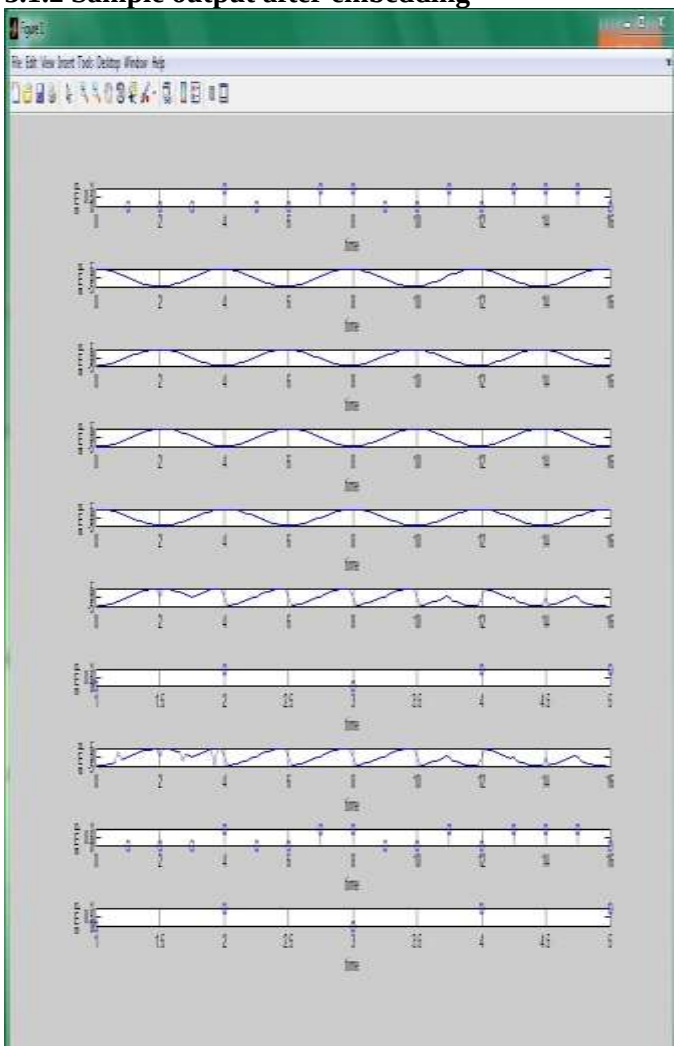


Figure 16 Output after embedding data

In this figure, the first wave is the randomly generated wave a 16 bit input sequence. Second is the BPSK (Binary Phase Shift Keying) wave and third wave is the 180 degree phase shifted

waveform. The fourth wave is the phase shifted wave, i.e. the user defined phase shift added with the conventional 180 degree phase shift of BPSK. Next wave is 180 degree phase shifted wave of above wave. These two waves serve as carriers for modulation. Next wave is the input sequence given by the user. Here the ASCII input is converted into binary sequence. The binary bit stream is modulated using the phase shifted carriers and transmitted. Next wave shows the modulated wave at the transmitter side.

Last two waves show the randomly generated binary sequence and the user data after extraction. The data could be retrieved only if the phase shift used in the transmitter side is known beforehand.

3.1.3 Transmitted and Received Images over The proposed Communication System

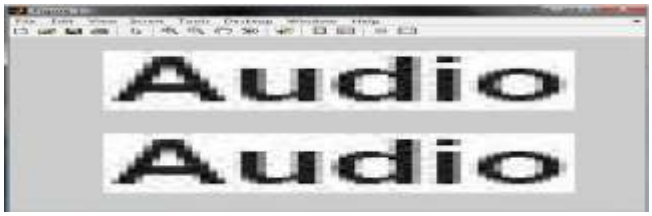


Fig 17: Final output after embedding data and extracting data from the image.

The above Fig 17 shows the transmitted and received images. Furthermore a simulation has been performed to investigate the BER performance of the proposed system in the presence of random noise channel and Additive White Gaussian Noise (AWGN). The results are depicted in Fig 18. It shows that the BER performance comparison of the proposed scheme in both AWGN and Random noise channels. It is inferred from the Fig 18 that the proposed scheme performs better in AWGN channel than random noise channels with lower bit error rate.

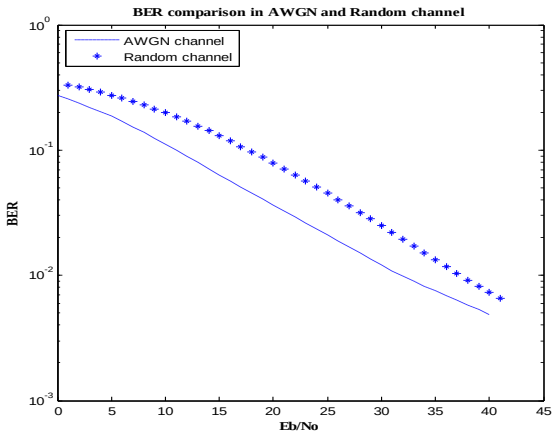


Fig 18 BER comparison in AWGN and Random channel.

4. CONCLUSION

This scheme has profound applications. The burst transmission that is employed can be used to retrieve individual information blocks again in case of improper or corrupt reception thus preventing retransmission of whole message. This method has a very high commercial potential, because of security and high data rate support. This can serve the interests of the future mobile customers who demand high bandwidths. It can also be used to achieve Forward Compatibility in 4G technology and other physical layer devices. The simulation modules developed are mostly behavioral; the structural implementation would take development to next stage.

5. ACKNOWLEDGEMENT

The author wants to thank Prof. R.Varadharajan Professor / ECE School of Electrical & Electronics Engineering SASTRA University for his valuable guidance and moral support.

6. REFERENCES

[1]. R.Amirtharajan, Krishnendra Nathella and J Harish, “Info Hide – A Cluster Cover Approach” International Journal of Computer Applications 3(5) (2010)11–18.

[2]. W. Bender, D. Gruhl, N. Morimoto, A. Lu, Techniques for data hiding, IBM Syst. J. 35 (3&4) (1996) 313–336.

[3]. S. Katzenbeisser, F.A.P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Norwood, MA, 2000

[4]. J.S. Pan, Y.-C. Hsin, H.-C. Huang and K.-C.Huang, "Robust image watermarking based on multiple description vector quantisation," Electronics letters, vol. 40(22) October 2004.

[5]. Po-Yueh Chen, Hung-Ju Lin, A DWT Based Approach for Image Steganography, International Journal of Applied Science and Engineering 4(3) (2006) 275-290.

[6]. Roy Chapman and Tariq S. Durrani, "IP Protection of DSP algorithms for system on chip implementation," IEEE Transactions on signal processing, 48(3) (2000) 854-861.

[7]. K. Thenmozhi , R. Varadarajan , V.Prithiviraj, "IEEE 802.11a Physical layer implementation using OFDM" International Journal of Systemics, Cybernetics and Informatics (IJSCI), October 2006, 57-60.

[8]. Van Nee, Richard & Ramjee Prasad, “OFDM for Wireless Multimedia Communications”, Boston: Artech House, 2000.

[9]. Yimin Jiang, and Feng-Wen Sun, “User Identification for convolutionally/turbo-coded systems and its applications,” IEEE Transactions on communications, 51(11) (2003)1796-1808