http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 13 (12): 2037-2041, 2014
ISSN 1812-5638 / DOI: 10.3923/itj.2014.2037.2041

Data Puncturing in OFDM Channel: A Multicarrier Stego

Padmapriya Praveenkumar, K. Thenmozhi, J.B.B. Rayappan and Rengarajan Amirtharajan
Department of Electronics and Communication Engineering, School of Electrical,
Electronics Engineering, SASTRA University, Thanjavur, 613 401, India

Abstract: The prospects of the next generation wireless broadband applications will be enhanced by the features like improved Signal to Noise Ratio (SNR) and variable higher data rates. The Orthogonal Frequency Division Multiplexing (OFDM) system offers better tolerance against multipath effects faced by fading channels. Forward Error Correction (FEC) codes meliorate the system performance. In this study, firstly the data is encoded using Convolution encoders with Puncture codes in OFDM system. Then, the secret message is embedded and passed through Rayleigh and Rician fading channels. The BER graph prior and after embedding the confidential data are compared and simulated using BPSK modulation scheme. The system is made more reliable by reducing the redundancy, errors in the signals and making it more secure and robust in fading environment.

Key words: OFDM, convolutional encoders, puncture codes, steganography, BER

INTRODUCTION

The demand for achieving better data rates, making the fullest utilisation of the bandwidth available and increasing the capacity of the channel has always been in an ascent more than ever. The solution for this is to multiplex the available channel. Increasing the bandwidth efficiency remains as the target and out of the several multiplexing schemes frequency division multiplexing is considered to be more appropriate. To meet with the growing user requirements this scheme divides the channel into several sub carriers. This FDM ultimately led to the development of OFDM technique (Van Nee and Prasad, 2000) to support the expanding user base.

OFDM is a multi carrier broadband technique widely used in digital audio broadcasting (DAB), digital video broadcasting (DVB), Asymmetric Digital Subscriber Line (ADSL), wherein parallel transmission of data in the narrowly divided bands of the usable bandwidth takes place thereby providing for increased demand (Thenmozhi *et al*., 2012). Further in addition, the sub carriers are orthogonal having frequencies which are different integral multiples of a same fundamental frequency. Thus OFDM stalls Inter symbol interference and inter block interference, increasing the efficiency (Praveenkumar *et al*., 2012a-c). But OFDM technique only limits these interferences to a considerable extent but could not completely eliminate them (Joshi and Saini, 2011; Thenmozhi *et al*., 2011).

Cyclic prefixing is carried out at a point in the transmission to eliminate the interferences particularly IBI to a maximum possible extent (Van Nee and Prasad, 2000). It is greater than or equal to channel order. The implementation of FFT aids in the utilisation of harmonically related sub carriers (Liu *et al*., 2006). They are given to a single tap equaliser at the receiver end. OFDM technique is being utilised in almost all available means of wireless communication. Though wireless communication is a huge leap forward from the wired communication and has several advantages over it, the limitation here is the occurrence of bit errors during transmission (Salari *et al*., 2008, Kumar *et al*., 2008). This might even go on to an extent where the entire transmission of packets gets affected due to noise and becomes reusable. Hence FEC is used to successfully retrieve the packets sent, by including error correction bits along with the packets being sent (Van Meerbergen *et al*., 2006, 2009).

Even after applying complex cryptographic techniques to ensure data security, it is clear to the intruder which part of the message is in fact encrypted. To deny even that small amount of information, the technology called steganography was developed (Al-Azawi and Fadhil, 2010, Padmaa *et al*., 2011). This technology contains techniques to embed the message or cipher text inside an image or multimedia file called a stego-image (Bender *et al*., 1996; Zanganeh and Ibrahim, 2011). By using these techniques, the intruder is denied the clear cut information of the location of the message.

Corresponding Author: Padmapriya Praveenkumar, Department of Electronics and Communication Engineering, School of Electrical, Electronics Engineering, SASTRA University, Thanjavur, 613 401, India

The simplest LSB steganography technique in a spatial domain is changing the LSB of any of the layers of the RGB colour pattern of an image (Amirtharajan and Rayappan, 2012a, b). The palette based technique hides the message in one of the colour palettes of the image. Alternatively, the transform based techniques employ an alteration in the coefficients of the frequency domain representation of the image. The weakness of human senses is exploited since we cannot detect the minute changes caused in the stego-image because of the embedded message (Amirtharajan and Rayappan, 2012c-d; Amirtharajan *et al*., 2012). The LSB, though primitive, is the easiest to implement and also the easiest one that can be detected (Kumar *et al*., 2011). Steganography has evolved over the years to very high levels and equally applicable to other type of digital media such as audio (Zhu *et al*., 2011), video (Al-Frajat *et al*., 2010) and text (Al-Azawi and Fadhil, 2010) as cover objects.

The technique used to retrieve the information from the stego-image is called steganalysis (Qin *et al*., 2010). Cryptography and watermarking are two techniques that are very closely related to steganography (Zaidan *et al*., 2010). Watermarking is used to protect the ownership of a file or a message or simply to copyright a file (Karzenbeisser and Perircolas, 2000). The creator's name is embedded in the file that is undetectable by steganalysis to prevent anyone else's claim over the ownership of that file. Cryptography generates keys that are known only to the sender and the receiver during each transmission to secure the message. Without the knowledge of these keys one cannot open the message. Various techniques and algorithms are being developed to conceal data which in turn makes the wireless high data rate transmission more secure against hackers. After completely reviewing the available literature on OFDM and steganography, this study proposes to embed secret after convolutional encoders with puncture codes. The code rate is increased, since punctured codes remove redundant bits from the convolutional coded data bit stream.

PROPOSED METHODOLOGY

OFDM is a parallel transmission technique which involves splitting up of the serial data stream having a high data rate into several low rate sub streams. These streams are then modulated on separate carriers and convolution encoding is done. Convolution encoding, a type of FEC is preferred the most as it is easy to be decoded. Another important feature that makes it superior is its sequential processing of data unlike the other codes. The transmitted data can be accessed by anyone and there is a possibility of data piracy and introduction of errors in the data. To avert this, confidential data is embedded in the redundant bits after encoding. Now, this data embedded with the confidential code is transmitted through OFDM system as shown in Fig. 1.

In the same way, proper decoding is necessary at the receiver. Of many decoders available, viterbi decoder tops the list in the aspect of error detection. It uses Maximum Likelihood (ML) decision rule that minimises the error. The efficiency in detecting errors increases as the constraint length of the convolution encoder increases. Then Puncturing is done which removes some of the parity encoded bits. This results in an error-correction code with reduced redundancy. In puncturing the redundant bits are deleted according to the pre arranged puncturing pattern adopted. This reduces the decoding complexity. At the receiver end, de-puncturing is done to enable the decoding process. Then Viterbi decoder is used in decoding the convolutional coded data bits.

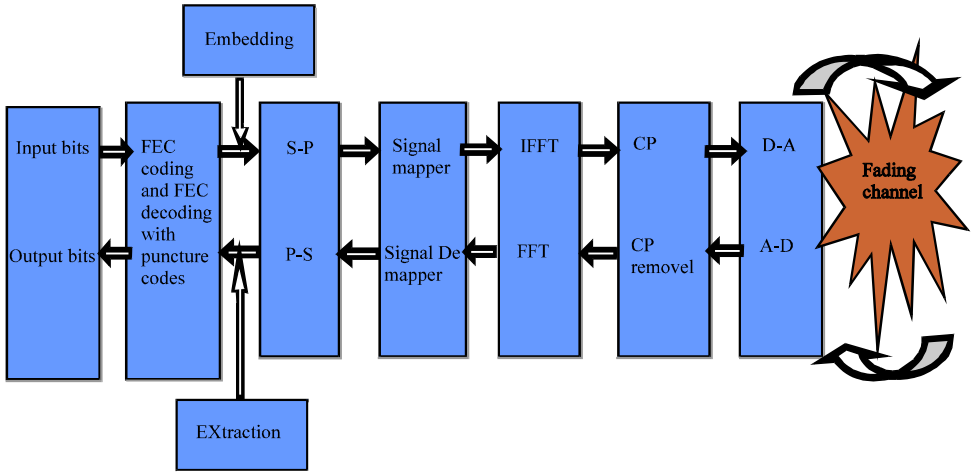

Fig. 1: Secured OFDM block diagram with FEC and puncturing

The data stream is grouped as per the modulation schemes as 1, 2, 3 bits for BPSK, QPSK and QAM respectively. This reduces the bandwidth of the subcarriers as compared to the coherence bandwidth of the channel. Then modulation is performed according to the chosen modulation scheme. This makes the symbol period of the sub-data streams longer than the delay spread of the time dispersive radio channel. The orthogonal carriers if chosen, has an advantage of providing high spectral efficiency without incurring Inter Carrier Interference (ICI). IFFT and FFT are used to serve the purpose of modulation and demodulation of data respectively. The output of the IFFT will be in time domain representing the data symbols on the orthogonal sub-carriers. Cyclic prefix can be incorporated to maintain orthogonality over a dispersive channel. The data is transmitted in analog through Rayleigh and Rician channels.

The data can be retrieved in the receiver by following the exact reverse procedure as done for transmission. The embedded bits can be retrieved before decoding only if the punctured pattern and the key value used for embedding is known.

RESULTS AND DISCUSSION

The BER analysis of OFDM using BPSK over Rayleigh and Rician Fading channels with FEC and Puncture codes is given in Fig. 2. From the graph, it can be justified that Rician channels are less faded compared to Rayleigh fading channel.

Figure 3 provides the BER of BPSK in OFDM with FEC and puncture codes before and after embedding confidential data in Rayleigh fading channel. From the graph, it can be illustrated that even after additional data bits over fading channel, BER graph are appreciable and not much deviating from the actual data bits.

The BER comparison of BPSK before and after embedding confidential data in Rician fading channel using BPSK in OFDM with FEC and puncture codes is given in Fig. 4.

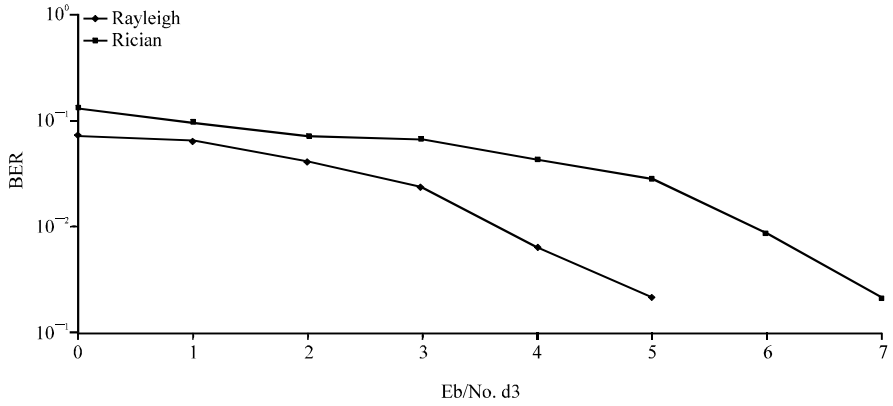

Fig. 2: BER comparison of Rayleigh and Rician fading channels in OFDM with FEC and puncture codes using BPSK modulation

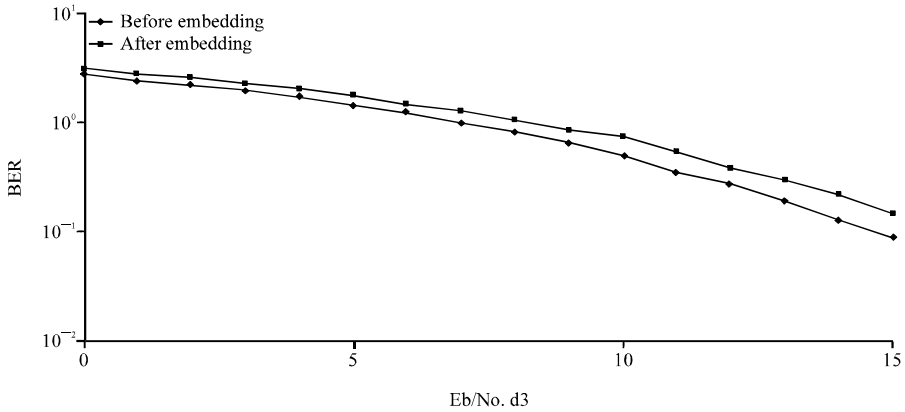

Fig. 3: BER comparison of modulation schemes like BPSK, QPSK and QAM in OFDM system with interleaving

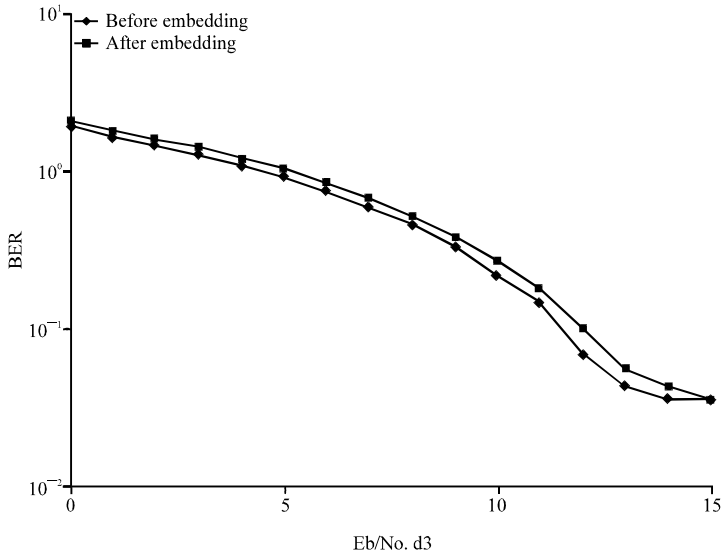

Fig. 4: BER comparison of modulation schemes like BPSK, QPSK and QAM in OFDM system with embedding after interleaving

From the Fig. 4, it is justified that additional data bits over fading channel does not deviates more from the actual data bits.

CONCLUSION

The use of orthogonality concept makes OFDM to eliminate ICI and ISI. In this study, the higher data rate with the appreciable level of SNR is achieved. Convolutional codes with puncture codes are used as error control codes in OFDM system which mitigates errors and redundant bits encountered by the channel. BER graph of OFDM using BPSK modulation scheme over Rayleigh and Rician fading channels before and after embedding confidential data has been analysed. From the results, even over fading channels BER graphs after secret data embedding is appreciable. By knowing the puncturing format and the embedding key, the actual data bits and secret bits can be retrieved. Puncturing codes enhances the security of the OFDM system.

REFERENCES

Al-Azawi, A.F. and M.A. Fadhil, 2010. Arabic text steganography using kashida extensions with huffman code. J. Applied Sci., 10: 436-439.

Al-Frajat, A.K., H.A. Jalab, Z.M. Kasirun, A.A. Zaidan and B.B. Zaidan, 2010. Hiding data in video file: An overview. J. Applied Sci., 10: 1644-1649.

Amirtharajan, R. and J.B.B. Rayappan, 2012a. An intelligent chaotic embedding approach to enhance stego-image quality. Inform. Sci., 193: 115-124.

Amirtharajan, R. and J.B.B. Rayappan, 2012b. Brownian motion of binary and gray-binary and gray bits in image for stego. J. Applied Sci., 12: 428-439.

Amirtharajan, R. and J.B.B. Rayappan, 2012c. Inverted pattern in inverted time domain for icon steganography. Inform. Technol. J., 11: 587-595.

Amirtharajan, R. and J.B.B. Rayappan, 2012d. Pixel authorized by pixel to trace with SFC on image to sabotage data mugger: A comparative study on PI stego. Res. J. Inform. Technol., 4:: 124-139.

Amirtharajan, R., J. Qin and J.B.B. Rayappan, 2012. Random image steganography and steganalysis: Present status and future directions. Inform. Technol. J., 11: 566-576.

Bender, W., D. Gruhl, N. Morimoto and A. Lu, 1996. Techniques for data hiding. IBM Syst. J., 35: 313-336.

Joshi, A. and D.S. Saini, 2011. Performance analysis of coded-OFDM with ICI due to frequency offset. Proceedings of the 3rd International Conference on Advances in Recent Technologies in Communication and Computing (ARTCom 2011), November 14-15, 2011, Bangalore, India, pp: 47-50.

Karzenbeisser, S. and F.A. Perircolas, 2000. Information Hiding Techniques for Steganography and Digital Watermarking. Artech House, UK., ISBN: 9781580530354, Pages: 220.

Kumar, P.P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2011. Steg-OFDM blend for highly secure multi-user communication. Proceedings of the 2nd International Conference on Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology, February 28-March 3, 2011, IEEE, Chennai, India, pp: 1-5.

Kumar, R., S. Malarvizhi and S. Jayashri, 2008. Time-domain equalization technique for intercarrier interference suppression in OFDM systems. Inform. Technol. J., 7: 149-154.

Liu, H., H. Zhong, T. Zhang and Z. Gong, 2006. A quasi-newton acceleration EM algorithm for OFDM systems channel estimation. Inform. Technol. J., 5: 749-752.

Padmaa, M., Y. Venkataramani and R. Amirtharajan, 2011. Stego on 2^n: 1 Platform for users and embedding. Inform. Technol. J., 10: 1896-1907.

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2012a. Phase for face saving: A multicarrier stego. Procedia Eng., 30: 790-797.

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2012b. Regulated OFDM-role of ECC and ANN: A review. J. Applied Sci., 12: 301-314.

Praveenkumar, P., R. Amirtharajan, Y. Ravishankar, K. Thenmozhi and J.B.B. Rayappan, 2012c. Random and AWGN road for MC-CDMA and CDMA bus to phase hide: A MUX in MUX stego. Proceedings of the International Conference on Computer Communication and Informatics, January 10-12, 2012, Coimbatore, India, pp: 1-6.

Qin, J., X. Xiang and M.X. Wang, 2010. A review on detection of LSB matching steganography. Inform. Technol. J., 9: 1725-1738.

Salari, S., M. Ardebilipour and M. Ahmadian, 2008. Channel and frequency offset estimation for MIMO-OFDM systems. J. Applied Sci., 8: 809-815.

Thenmozhi, K., P. Praveenkumar, R. Amirtharajan, V. Prithiviraj, R. Varadarajan and J.B.B. Rayappan, 2012. OFDM+CDMA+Stego = Secure Communication: A Review. Res. J. Inform. Technol., 4: 31-46.

Thenmozhi, K., V.K. Konakalla, S.P.P. Vabbilisetty and R. Amirtharajan, 2011. Space Time Frequency coded (STF) OFDM for broadband wireless communication systems. J. Theor. Applied Inform. Technol., 3: 53-59.

Van Meerbergen, G., M. Moonen and H. de Man, 2006. Combining reed-solomon codes and ofdm for impulse noise mitigation: RS-OFDM. Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing, May 14-19, 2006, Toulouse,.

Van Meerbergen, G., M.S. Moonen and H. De Man, 2009. Reed-Solomon codes implementing a coded single-carrier with cyclic prefix scheme. Communi. IEEE Trans., 57: 1031-1038.

Van Nee, R. and R. Prasad, 2000. OFDM for Wireless Multimedia Communications. Artech House, Norwell, MA., USA., ISBN-13: 978-0890065303, Pages: 284.

Zaidan, B.B., A.A. Zaidan, A.K. Al-Frajat and H.A. Jalab, 2010. On the differences between hiding information and cryptography techniques: An overview. J. Applied Sci., 10: 1650-1655.

Zanganeh, O. and S. Ibrahim, 2011. Adaptive image steganography based on optimal embedding and robust against chi-square attack. Inform. Technol. J., 10: 1285-1294.

Zhu, J., R.D. Wang, J. Li and D.Q. Yan, 2011. A huffman coding section-based steganography for AAC audio. Inform. Technol. J., 10: 1983-1988.