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): 2047-2051, 2014
ISSN 1812-5638 / DOI: 10.3923/itj.2014.2047.2051

Reversible Steganography on OFDM Channel: A Role of Cyclic Codes

Padmapriya Praveenkumar, R. Deepak, K. Thenmozhi,
John Bosco Balaguru Rayappan and Rengarajan Amirtharajan
Department of Electronics and Communication Engineering, School of Electrical and Electronics Engineering,
SASTRA University, Thanjavur, 613 401, India

Abstract: In the era of wireless communication, the World Wide Web is the brain child of all the new technological development. This digital world has speeded up the data transfer and communication speed a manifold, creating new goods and services all along. Along with the development of internet, developed ways of hacking, modifying and stealing it also increased. There is an increasing demand to augment the data rates and to provide greater fidelity. Thus, technology provides us the finesse for increasing robustness over fading channels. The most prominent solution for increased speed is OFDM. And the security issues can be taken care of by embedding confidential data after encoding the message using cyclic codes.

Key word: Cyclic codes, data security, steganography, AWGN, QPSK, QAM

INTRODUCTION

Wireless communication is one of the demanding and challenging technologies from time to time. The exponential growth of multimedia over internet makes inevitable to digitize the data to be published, transmitted and shared on internet and the evolution of new products and services emerging on almost daily basis which demands for higher data rate (Van Nee and Prasad, 2000). The recent advances in communication are based primarily on wireless systems since it improves the transmission distance tremendously. Though this overcomes many of the limitations of the wired systems, security remains a major concern. The unauthorized tapping and tampering of data has been the major reason for encoding the data before transmission. Some additional features are incorporated nowadays to render the message unreadable even if tapped (Kumar *et al*., 2011).

Since man started communicating there has been an uninhibited development in the techniques and modes by which he does it. These developments focused primarily on improving the capacity (Peterson, 1961), integrity and privacy. One such development is the concept of Frequency Division Multiplexing (FDM) which allows many users to use the communication channel simultaneously at various frequencies (Bahai *et al*., 2004). To counter the drawbacks of FDM, Orthogonal FDM (OFDM) (Arioua *et al*., 2012; Amirtharajan *et al*., 2012) a digital signal processing mechanism, was proposed (Chang, 1966) and carried out by Chang, (1970). This improved the bandwidth efficiency and reduced the Inter Symbol Interference (ISI) (Thenmozhi *et al*., 2012; Karzenbeisser and Perircolas, 2000). The sub channels chosen were such that each of their bandwidth is made lesser than the total coherence bandwidth of the channel results in flat fading of the channels and allowed the overlapping of the sub spectra (Forney, 1971). A set of sinusoidal functions which were related harmonically were used as carriers which eliminated the need for guard bands between them. This also eliminates the use of band limited filters and oscillators for each sub channel. By making use of IFFT design complexity is reduced. A Cyclic Prefix (CP) is used while transmission to bring down Inter Block Interference (IBI) (Praveenkumar *et al*., 2012a-c). As like every other technology, OFDM also has its own disadvantages. Though it reduced ISI, during the spectral nulls of the signal, OFDM tones experience severe degradation. The use of harmonically related sinusoidal functions increased the Peak to Average Power Ratio (PAPR). Interference cancellation, synchronization and phase noise mitigation are not simple processes. Also, depending on the multipath fading experienced, OFDM may require post equalization (Elahmar *et al*., 2007). OFDM was primarily designed for wireless standards and since the deployment of this technology, wireless standard speeds have risen to 50 Mbps. But considering the features offered, OFDM has been widely in use for DAB, DVB, ADSL high speed internet, etc. Also proposals have been made to include OFDM as a transmission method for 4G cellular technology.

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

To deny the intruder the possibility of an existence of a message the modern technology employs a developed version of an age old technique called steganography (Amirtharajan and Rayappan, 2012a-d). The message which is to be transmitted is concealed behind a multimedia file like an image or an audio or a video called the cover image. Firstly the technique vastly tested the human senses as slight modifications in the file were caused by camouflaging the data. But as time proceeded various techniques were invented to detect and extract the message hidden in it, the process being termed steg analysis. The efficiency of the system ought to be in fooling the intruder about the presence of the message failing which the system fails. There are various steganographic techniques(Karzenbeisser and Perircolas, 2000) ranging from spatial domain techniques such as LSB method to palette based technique (Amirtharajan and Rayappan, 2012c) and Spread Spectrum Image Steganography (SSIS). The LSB technique focuses on the variation of the LSB of the image in RGB format. Though it is one of the easiest and primitive techniques, this is highly vulnerable to detection of the message.

The SSIS technique offers higher security and efficiency (Petitcolas *et al*., 1999) as it uses the principles of spread spectrum as the data is interleaved before getting embedded into the file. Watermarking and cryptography are techniques that are closely related to steganography. In fact, watermarking is a form of steganography that is used to embed the signature of the file's creator. Rightly it is used to protect the file against misuse or tampering. On the other scale, cryptography is an encryption technique that uses a key known only to the sender and receiver (Schneier, 2007). It attempts to foolproof the system by generating the keys during each transmission. Though all these techniques attempt to provide privacy during transmission, the algorithms used by the intruders to detect or destroy the data in the file convincingly have also increased exponentially.

After reviewing the available literature on OFDM and steganography, this paper proposes the confidential data embedding scheme after encoding using cyclic codes and transmitted using OFDM and Bit Error Rate (BER) graphs are plotted before and after embedding.

PROPOSED METHODOLOGY

The OFDM technique implements the conversion of higher data bit rates to slower parallel data bit rates. These are later on modulated digitally by either BPSK or QPSK which rely on power and spectral efficiency requirements as mentioned in Fig. 1. Further the accommodation of more bits is accomplished with M- Array QAM technique. This also enhances the spectral efficiency and attributes to its increased applications and large capacity. In order to debar the inter symbol inference; equalisation is done to the sub carriers rending a longer symbol period. But usually ISI occurs when the data rate increases leading to the multipath propagation. This calls for minified BER which in turn demands reduction in symbol rate without reduction in the data rate which is aesthetically auctioned by OFDM. OFDM transmits large number of orthogonal sub carriers that results in higher data rate and the symbol rate slows due to them being very closely spaced. Each sub carrier is modulated individually by IFFT to avoid the cross talk. Later one-fourth of each OFDM symbols are added as redundant bits to further diminish the effect of ISI.

Cyclic codes are the codes developed by shift registers. It's a form of linear block code which is organized by well suited algebraic structures and hamming metrics. It is preferred for correcting single errors and burst errors in a wireless environment. Any linear code x is said to be cyclic, if its cyclic shift in X is also a linear code in X.

The objective of this paper is to encode the input data using cyclic codes, especially when the data on the transmission channel is transparent. This renders good efficiency in case of burst noise. This is followed by embedding the covert data in redundant bits of the input and the sub carriers are modulated by using

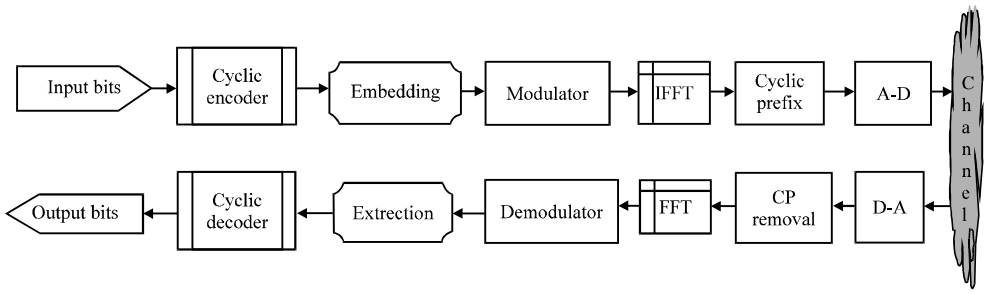

Fig. 1: Proposed block diagram

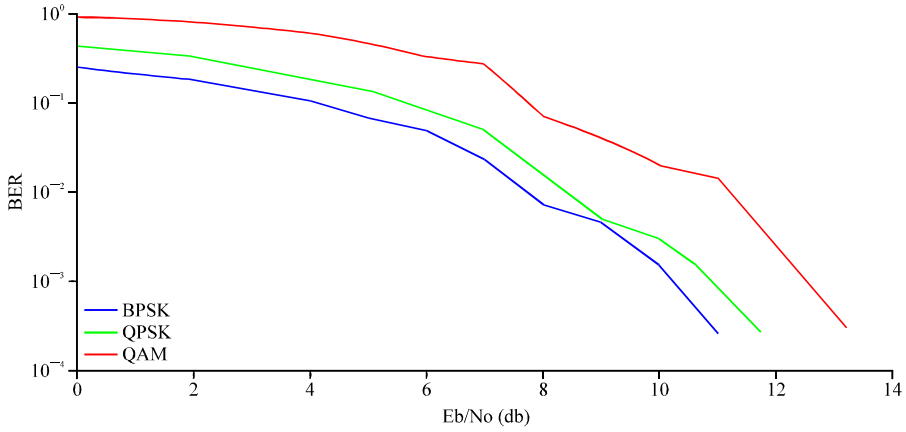

Fig. 2: Comparison between BPSK, QPSK and QAM in OFDM system using cyclic codes in OFDM system

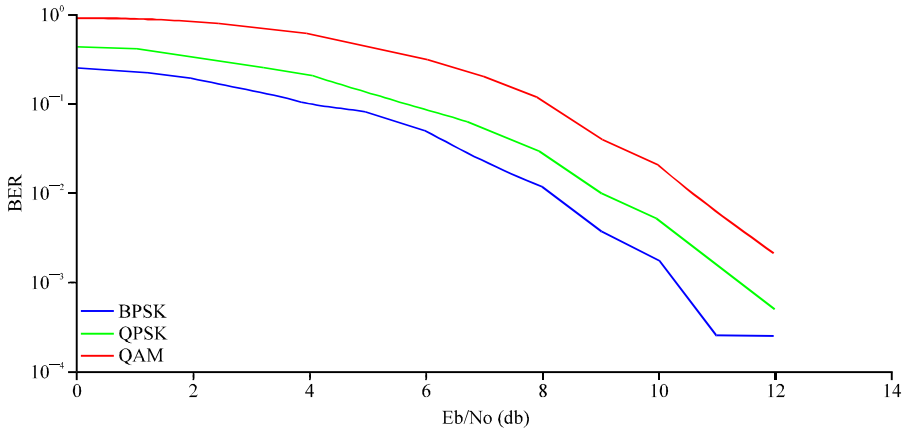

Fig. 3: Comparison between BPSK, QPSK and QAM in OFDM system using cyclic codes with data embedding

BPSK/QPSK/QAM which in turn depends on the spectral efficiency of the channel. In order to maintain the orthogonality of the closely spaced sub carriers, the conversion of the frequency to time domain is implemented using IFFT. Analog to digital conversion is accomplished over AWGN channel by infixing CP. At the receiver end, the exact reverse modulation occurs and the carriers along with the covert data are retrieved and the corresponding BER graph is plotted.

RESULTS AND DISCUSSION

The input data is coded using cyclic codes and modulated over BPSK or QPSK or QAM and passed over OFDM platform. Then the analysis was made by comparing the modulation schemes in OFDM and BER is computed. Figure 2 depicts the comparison results between BPSK, QPSK and QAM with cyclic codes. From the graph, it is proved that BPSK provides better BER and at Eb/No = 11 db, it approaches to zero.

Figure 3 gives the comparison results between BPSK, QPSK and QAM with cyclic codes after including additional secret information. From the graph, it can be illustrated that BPSK provides better BER as mentioned by Praveenkumar *et al*. (2012a) and at Eb/No=12 db it approaches to zero.

Figure 4-6 gives the comparison between cyclic coded, uncoded and additional secret data embedding using BPSK, QPSK and QAM, respectively.

Cyclic codes provides better results in all the three modulations schemes. After embedding the

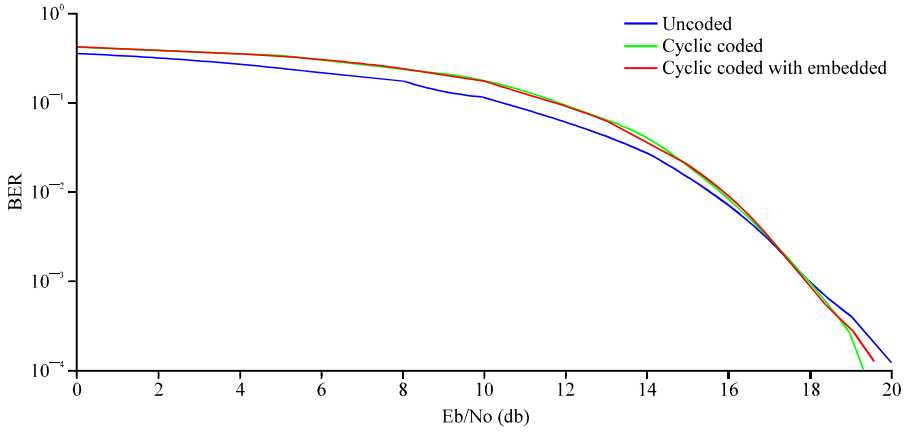

Fig. 4: Comparison between uncoded, cyclic coded, cyclic coded with embedded data using BPSK modulation

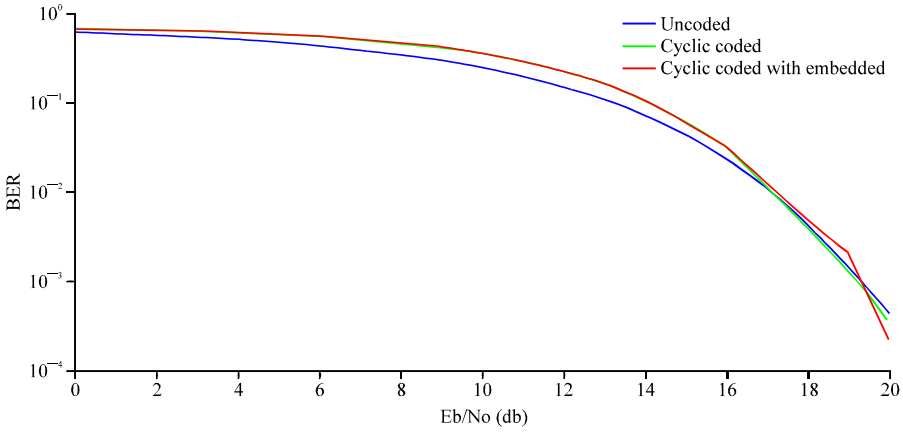

Fig. 5: Comparison between uncoded, cyclic coded, cyclic coded with embedded data using QPSK modulation

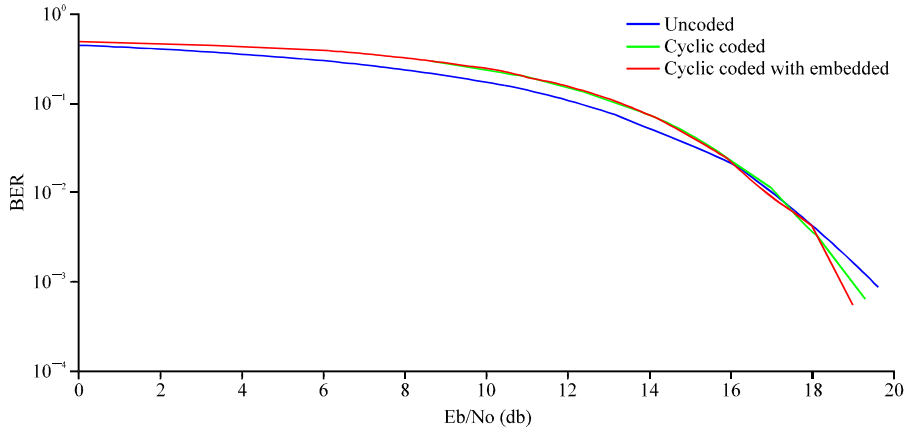

Fig. 6: Comparison between uncoded, cyclic coded, cyclic coded with embedded data using QAM modulation

additional secret information, BER of OFDM system employing QAM system provides better error performance as discussed by Kumar *et al.* (2011).

CONCLUSION

OFDM by making use of orthogonality concept it eradicates ICI and ISI. It provides higher data rate and improved signal to noise ratio demanded by broad band application. In this study, cyclic codes are used as error control codes in OFDM system which mitigates errors encountered by the channel. BPSK, QPSK and QAM are the three modulation schemes employed in the OFDM system. BER comparison graphs between the three modulation schemes was plotted. Also BER graphs for un-coded, cyclic coded before and after data embedding was plotted. The result elucidates that all three modulations schemes employing cyclic codes in OFDM system are equally good and also proves that QAM out performs the remaining two modulation schemes after additional information has been embedded.

REFERENCES

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.

Arioua, M., S. Belkouch and M.M. Hassani, 2012. Efficient 16-points FFT/IFFT architecture for OFDM based wireless broadband communication. Inform. Technol. J., 11: 118-125.

Bahai, A.R.S., B.R. Saltzberg and M. Ergen, 2004. Multi-Carrier Digital Communications: Theory and Applications of OFDM. 2nd Edn., Springer, USA., ISBN-13: 978-1441935502.

Chang, R.W., 1966. Synthesis of band-limited orthogonal signals for multi channel data transmission. Bell Syst. Tech. J., 45: 1775-1796.

Chang, R.W., 1970. Orthogonal frequency division multiplexing. U.S. Patent No. 3488445.

Elahmar, S., A. Djebbari, M. Bouziani and J.M. Rouvaen, 2007. New results with blind time domain equalization for OFDM system. Inform. Technol. J., 6: 207-211.

Forney, D.G., 1971. Burst-correcting codes for the classic bursty channel. IEEE Trans. Commun. Technol., 19: 772-781.

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.

Peterson, W.W., 1961. Error-Correcting Codes. The MIT Press, Cambridge, MA.

Petitcolas, F.A.P., R.J. Anderson and M.G. Kuhn, 1999. Information hiding-a survey. Proc. IEEE, 87: 1062-1078.

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.

Schneier, B., 2007. Applied Cryptography: Protocols, Algorithm and Source Code in C. 2nd Edn., Wiley, India.

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.

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