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): 2052-2056, 2014
ISSN 1812-5638 / DOI: 10.3923/itj.2014.2052.2056

Reversible Steganography on OFDM Channel-A Role of RS Coding

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

Abstract: The kinetics of higher data requirements in the upcoming wireless generation is engendered by the fact that the usage of high quality multimedia applications in the form of data, audio, SMS and video is on the rise. In order to meet the challenging needs of the increasing data rate requirements, the wireless system employs Orthogonal Frequency Division Multiplexing (OFDM). Security is the need of the hour in today's wireless technological advancement. In this study, OFDM with Reed Solomon codes (RS) as Forward Error correction codes (FEC) has been proposed to achieve lower Bit Error Rate (BER) and data embedding has been carried out to ensure security in wireless communication. Further RS codes are used to restore the cover object.

Keywords: OFDM, FEC, reed Solomon codes, steganography, BER

INTRODUCTION

In today's era of internet and wireless media, the rise in use of high definition multimedia applications calls for higher data rates. In order to accomplish the requirement of increased data rates, Orthogonal Frequency Division Multiplexing (OFDM) is being recognized as a format for modulation for the future wireless communication such as Digital Multi-carrier Multiplexing/Modulation (DMCMM) (Kumar *et al*., 2008; Praveenkumar *et al*., 2012c). It is an orthogonal mode of Frequency Division Multiplexing (FDM) in which the orthogonal sub-carriers make the system spectrally efficient (Liu *et al*., 2006; Salari *et al*., 2008). Here, the cyclic prefix consists of the one-fourth of the OFDM symbol that is being inserted in the guard interval which is followed by the actual OFDM symbol which annihilates Inter Symbol Interference (ISI) (Joshi and Saini, 2011; Thenmozhi *et al*., 2011). It is proves immune to Multipath propagation and frequency selective fading channels (Van Nee and Prasad, 2000; Praveenkumar *et al*., 2012a, b).

Fast Fourier Transform (FFT) and Inverse Fast Fourier Transform (IFFT) pairs make the system design less complex and the Reed Solomon codes (RS) are called as Maximum Distance Separable (MDS) codes (Hussain *et al*., 2011). The redundant bits added to the encoder are very minimal for error correction and detection but it has better performance when Channel State Information (CSI) is known (Van Meerbergen *et al*., 2006). It outperforms the other Forward Error Correction codes (FEC) especially when the channel introduces burst errors. The minimum distance between the codes can be arrived by the largest possible way (Van Meerbergen *et al*., 2009). When the number of the inputs to the system is large, then RS codes are preferred which works efficiently on the channel.

Steganography literally means covered writing that is security through obscurity in any digital media (Al-Azawi and Fadhil, 2010; Al-Frajat *et al*., 2010; Bender *et al*., 1996). There are three types of steganography called pure, symmetric and public key steganography, in pure steganography no key is used, where as symmetric key uses single key for concealing and revealing the information and public key steganography uses two keys one for embedding and another for extraction (Amirtharajan *et al*., 2012). Cryptography, Steganography and Watermarking are multifarious in secret data communication (Amirtharajan *et al*., 2012; Zanganeh and Ibrahim, 2011; Zhu *et al*., 2011).

Cryptography scramble the confidential information, Steganography conceals the very existence of the confidential information and watermarking is for authorization or to prove the ownership (Amirtharajan and Rayappan, 2012a; Zhao and Luo, 2012). Al-Frajat *et al*. (2010) describes the data concealment for videos as cover object by identifying the redundant bits embed the encrypted data. However, while embedding the confidential information on the cover object, there always exists trade off between capacity and imperceptibility (Amirtharajan and Rayappan, 2012a-d; Kumar *et al*., 2011; Padmaa *et al*., 2011). A review on various random data embedding methods have been analysed by Amirtharajan *et al*. (2012), Thenmozhi *et al*. (2012) and Rajagopalan *et al*. (2012).

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

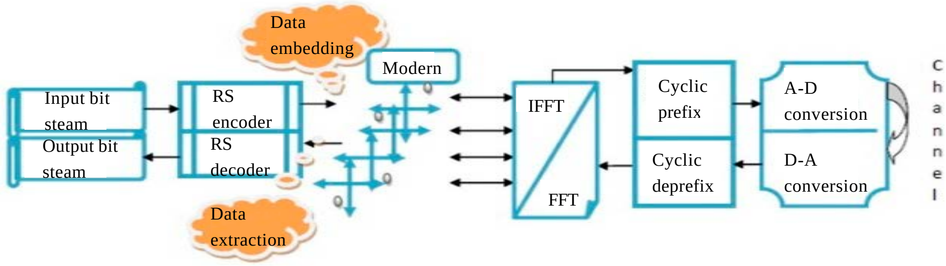

Fig. 1: OFDM transceiver model with RS codes

After carefully reviewing the existing literature on OFDM and steganography, this study has been proposed to implement Reed Solomon codes (RS) as Forward Error correction codes (FEC) to achieve lower Bit Error Rate (BER) and data embedding has been carried out to ensure security in wireless communication. Further RS codes revert the cover also.

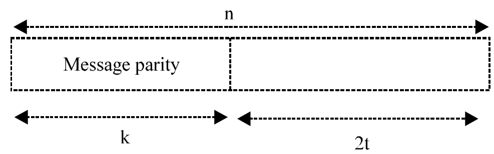

Fig. 2: RS code representation

PROPOSED METHODOLOGY

In OFDM technique, higher data rate bit streams are converted in to parallel slower data rates and then, their own digital modulation schemes can be chosen based on the requirement of power and spectral efficiency as shown in Fig. 1. It can either be BPSK or QPSK which gives out two phase values for binary digits and results in four phase output values. To accommodate more data bits in the pixel, M-ary QAM is preferred which will cause changes in both amplitude and phase of the subcarriers. With M-ary spectrum, efficiency can be increased and this supports variety of applications and provides large capacity at the cost of Eb/No. In order to avoid this, equalization is done in set of subcarriers rather than single carrier making the symbol period longer and applying Cyclic prefix wipes out Inter Symbol Interference (ISI).

As the data rate increases, probability of multipath propagation will results in Inter Symbol Interference (ISI). Thus, to minify Bit Error rate (BER), the reduction in data rate should be done and a solution to this can be arrived at by using OFDM which reduces the symbol rate without compromising the data rate. Since, it broadcasts larger number of subcarriers, which are very closely spaced and maintains orthogonality, the symbol rate of the subcarriers slow down and higher data rate can be maintained because of the huge number of orthogonal subcarriers. Further, each subcarrier can be modulated individually by IFFT to reduce cross talk between the adjacent users. One fourth of each OFDM symbol is then copied and the redundant value can be added to the symbol to avoid ISI.

Work on RS code was initially based on Mathematics and was invented by French mathematician Evariste Galois in 1830's, then known as the finite field or Galois field. It was further carried out by Irving Reed and Gustave Solomon at MIT laboratory in 1960. RS codes are systematic linear block codes and can also be called as non binary cyclic codes where the parity bits are appended to the original information. They add redundancy to the original information and thus, the extra information added to the original information decides the errors that can be corrected and detected. It is specified as RS (n, k) and is given in Fig. 2 where n refers to the encoded bits and K refers to the original bits. n-k = 2t refers to the parity bits that has to be appended to the original information in the form of encoding. n-k/2 symbols can be corrected by the RS decoder. The minimum distance of RS(n, k) code is n-k+1 which are often termed as the maximum distance separable codes. RS code(n, k) derives its symbols from Galois field called as GF(2m). They are intended for burst errors and is very effective for the systems considering fading channels with memory.

In this study, the input data bits are encoded using RS codes because they provide better results in case of burst errors especially when transmission channel information is known. Then, the covert data embedding is carried out in the redundant bits of the input information bits which is followed by the modulation of subcarriers with secret data using BPSK/QPSK/QAM which in turn depends on the required spectral efficiency. Further, the frequency to time domain conversion is carried out using IFFT which maintains the orthogonality between subcarriers because they are closely spaced. Then, CP is inserted and analog to digital conversion is carried out to transmit over AWGN channel. At the receiver end, the

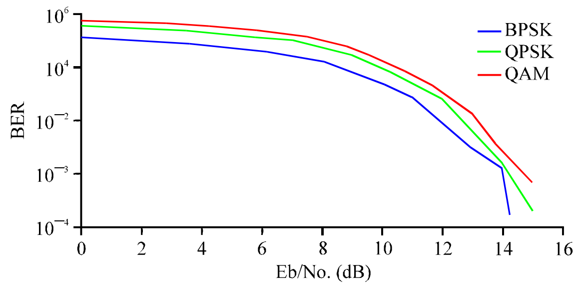

Fig. 3: Comparison among BPSK, QPSK and QAM in OFDM with RS codes

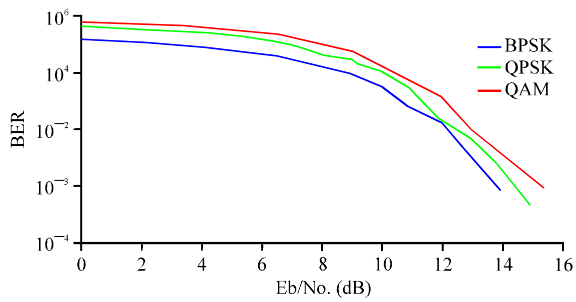

Fig. 4: Comparison between BPSK, QPSK and QAM after data embedding in OFDM with RS codes

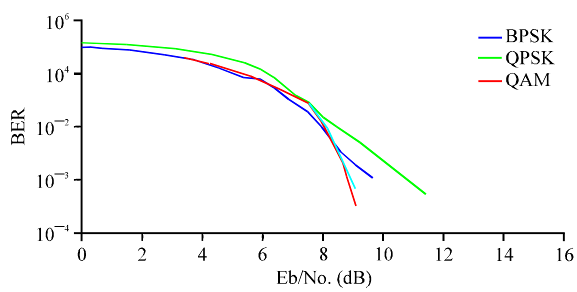

Fig. 5: Comparison between Uncoded, RS coded and RS coded with data embedding using BPSK

reverse operation of modulation is carried out and the input and the embedded secret data is retrieved and BER graphs are plotted.

RESULTS AND DISCUSSION

The comparative results among BPSK, QPSK and QAM in OFDM using RS codes were analysed. (Van Meerbergen *et al*., 2006). Then, BER was plotted after embedding the secret data. Figure 3 depicts the comparison results between BPSK, QPSK and QAM with

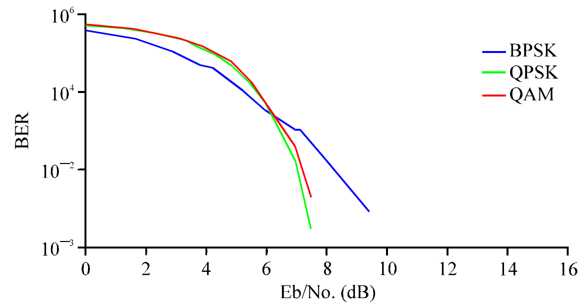

Fig. 6: Comparison between Uncoded, RS coded and RS coded with data embedding using QPSK

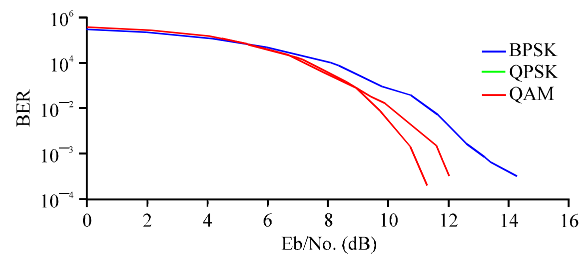

Fig. 7: Comparison between Uncoded, RS coded and RS coded with data embedding using QAM

RS codes. From the graph, it is proved that BPSK provides better BER and at Eb/No = 14.2 db, it approaches to zero.

Figure 4 gives the comparison results among BPSK, QPSK and QAM with RS codes after data embedding. From the graph, it can be illustrated that BPSK provides better BER as mentioned by Praveenkumar *et al.* (2012a, b) and at Eb/No = 14 db it approaches to zero.

Figure 5-7 gives the comparison between RS coded, uncoded and data embedding using BPSK, QPSK and QAM, respectively.

RS coded in all the three modulations provides better results. After the embedding of data, BER of OFDM system employing QAM system provides better error performance as discussed by Kumar *et al.* (2011).

CONCLUSION

OFDM has attracted the Wireless environment by adapting higher data rate with improved spectrum efficiency by utilising orthogonal subcarriers. In this study, BPSK, QPSK and QAM has been adapted as a base modulation prior to IFFT block along with RS codes to control channel errors and the BER performance has been plotted. This result confirms that all three modulations are good with RS codes, even after additional data embedding. In addition, this study also proves that QAM out performs the remaining two (QPSK, BPSK) as proved by many researchers, even with additional data through information hiding. Furthermore, this study also confirms that the BER performance is excellent for RS coded and good for RS coded with data embedding also to get back the cover object and then decent for Uncoded data.

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.

Hussain, G.A., M.B. Mokhtar and R.S.A.B. Raja, 2011. Concatenated RS-convolutional codes for MIMO-OFDM system. Asian J. Applied Sci., 4: 720-727.

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.

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.

Rajagopalan, S., R. Amirtharajan, H.N. Upadhyay and J.B.B. Rayappan, 2012. Survey and analysis of hardware cryptographic and steganographic systems on FPGA. J. Applied Sci., 12: 201-210.

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., 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.

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 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.

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.

Zhao, Z. and H. Luo, 2012. Reversible data hiding based on Hilbert curve scan and histogram modification. Inform. Technol. J., 11: 209-216.

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.