Information Technology Journal, 2013
ISSN 1812-5638 / DOI: 10.3923/itj.2013.

Inserted Embedding 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, 613401, India

Abstract: Stupendous advances in Digital Communication have brought about the advent of internet culture benefiting the people in many ways. Just as fire is a good servant, but a bad master, so is the case with internet. With internet, stealing and unauthorised usage of data remains unrestrained. In addition, use of high multimedia applications demands for higher data rates. To accommodate the challenging needs of higher data rate requirements, Orthogonal Frequency Division Multiplexing (OFDM) proves to be the propitious solution. Hacking over wireless environment can be staved off by incorporating the emerging information hiding techniques with OFDM system. This study analyses the performance of OFDM system using modulation schemes like Binary Phase Shift Keying (BPSK), Quadrature Phase Shift Keying (QPSK) and Quadrature Amplitude Modulation (QAM) and then the confidential information is embedded after interleaving and passed over AWGN channel. Interleaving serves two purposes primarily it reduces burst errors and it needs two different keys intact, one to stipulate the scrambling of the data bits and the other to identify the secret data embedding. It is observed from the simulation results that the BER of the system can be improved by rearranging the input data streams through interleaving, thereby reducing the random errors due to noisy wireless channel environment. The BER graph is simulated for various modulation schemes prior to embedding and after embedding the confidential information.

Key words: OFDM, interleaving, steganography, BER

INTRODUCTION

Present day electronic universe experiences buccaneering and illicit access to data which persist almost rampant. Copious information hiding proficiencies are pullulating to encumber such threats. To quote some, Cryptography masks the original clandestine information in other signals' stratum; Steganography veils the same in the course of digital files (Al-Azawi and Fadhil, 2010; Karzenbeisser and Perircolas, 2000). Another expertise is digital water marking which watermarks the original file to avert piracy. As far as steganography is concerned, the buried secret is usually held inconspicuous statistically in whichever nature of cover with the intention of dodging the inkling of the intruders (Bender *et al*., 1996; Cheddad *et al*., 2010).

Steganography is a blend of three attributes; correspondingly cover (file adopted for embedding), stego (resultant infixed output) and secret object (file to be rooted) (Amirtharajan and Rayappan, 2012a-d; Al-Frajat *et al*., 2010). The reason behind the notion of choosing images majorly as covers is the fact that they possess prominent redundancy when they get represented digitally. When images are used as covers, such stego systems are named image steganography (Amirtharajan and Rayappan, 2012a- d). There exist myriad mechanisms for screening secrets within a cover file (Zaidan *et al*., 2010; Zanganeh and Ibrahim, 2011; Zhu *et al*., 2011). Salient amongst such are spatial and transform domain expertises (Janakiraman *et al*., 2012a, b). In the former, pixel values get manoeuvred to drive in the secret bits unswervingly of which LSB scheme is the widely used. This modus operandi promises elevated embedding capacity but is evident.

In the latter, pixels are converted to transform domain coefficients only after that secret bits are enrolled in them. The higher the bits entrenched, the superior is the infixing capacity of the given cover (Hmood *et al*., 2010a, b; Kumar *et al*., 2011). It can also consign to the buried message's size in relation with that of the cover (Padmaa *et al*., 2011). The art of sensing and identifying the secret in images and to crack the steganographic construct is nothing but steganalysis (Qin *et al*., 2010, Amirtharajan *et al*., 2012).The means of first spreading the messages in frequency domain followed by embedding is the spread spectrum technique (Thenmozhi *et al*., 2012).

Multiplexing idea is unearthed to cope up the ever increasing requirement of high data rate (Van Nee and

Corresponding Author: Padmapriya Praveenkumar, Department of Electronics and Communication Engineering, School of Electrical, Electronics Engineering, SASTRA University Thanjavur, 613401, India

Prasad, 2000). Bandwidth efficiency is significantly maximised with the help of Frequency Division Multiplexing (Joshi and Saini, 2011; Thenmozhi *et al*., 2011). The whole channel is subdivided to a lot of subcarriers to accommodate countless users simultaneously at different frequencies. State-of-the-art expertises in wireless technology and improvised smart applications necessitate beneficial practices.

The coffers experienced in this mechanism is dealt with the preamble of OFDM, in which Orthogonal frequency, sinusoidal function's harmonic, precludes the want of guard bands to minimise Inter Symbol Interference (ISI) (Liu *et al*., 2006; Salari *et al*., 2008) and Inter Block Interference (IBI) (Kumar *et al*., 2008); not only guard bands but also band limited filters and oscillators required for individual channel. Cyclic prefix is used throughout transmission to shrink IBI (Praveenkumar *et al*., 2012a-c). System complexity is diminished by implementing FFT in OFDM. OFDM finds applications in Digital Audio Broadcasting (DAB), Digital Video Broadcasting (DVB) and Asymmetric Digital Subscriber Line (ADSL). Due to these, transmission speed is enhanced to 50 Mbps.

Like any other expertise, this also has certain limitations. The signal may be weaken at spectral null. OFDM has soaring Peak to Average Power Ratio (PAPR). Interference cancellation, synchronisation and phase noise reduction are very intricate here; moreover, OFDM entails post equalisation leading to bit errors in transmission. This has paved the way to Forward Error Correction (FEC) codes that lend a helping hand in removing those errors (Van Meerbergen *et al*., 2006, 2009).

For having tamper resistant systems, numerous algorithms and techniques are proposed to mask the secret data. After a thorough study of existing literature in steganography and OFDM, this work forefronts a model for secret sharing subsequent to interleaving, in OFDM system, in order to attain security with escalated data rates.

PROPOSED METHODOLOGY

OFDM is a technique where the serial data with higher data rates are made to carve up into parallel streams with subsequently lower data rates. The data are then canalized into separate sub- carriers for modulation and formatting that is done later is grounded on those modulating schemes. BPSK, QPSK, QAM adopts 1, 2, 3 bits/word respectively which shrinks the bandwidth of the subcarriers lesser than the channel.

Then the bits are subjected to interleaving, to avoid burst errors that occur within a code word and to stipulate interleaving algorithm. These interleaved bits are commuted into constellation points by the time the jumbled data with its embedded coveted data undergoes phase modulation as shown in Fig. 1, thus making the symbol period of the sub streams.

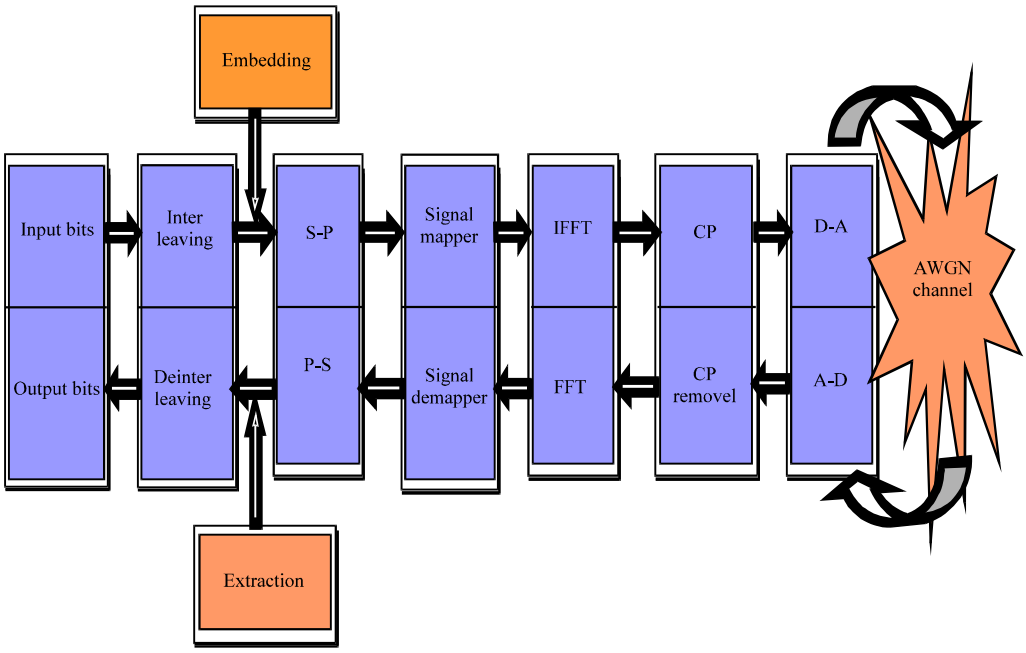

Fig. 1: Proposed OFDM Block diagram with Interleaving

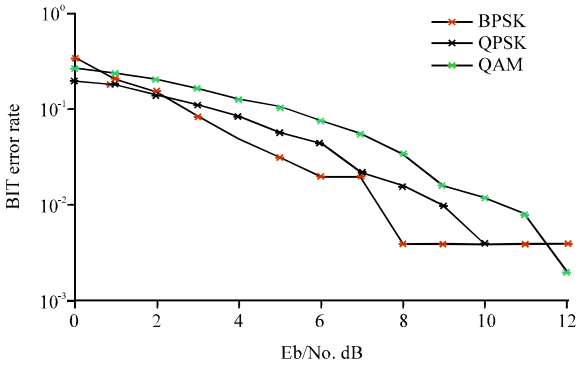

Fig. 2: BER comparison of modulation schemes like BPSK, QPSK and QAM in OFDM system without interleaving

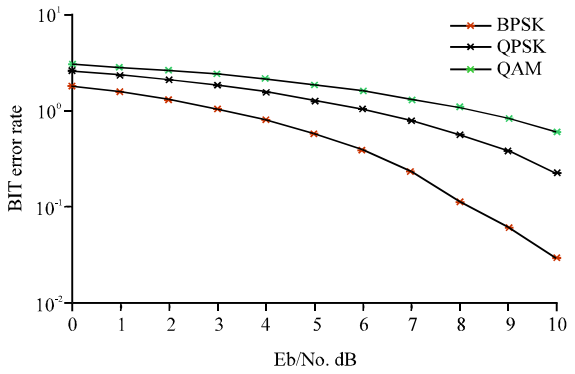

Fig. 3: BER comparison of modulation schemes like BPSK, QPSK and QAM in OFDM system with interleaving

longer than the delay spread of the time dispersive radio channel. While the mutual influence among the sub carriers is hard to avoid, higher efficiency can still be obtained by proper selection of orthogonal frequencies. FFT and IFFT techniques are usually hired for modulating and demodulating the data constellations.

. To maintain orthogonality, cyclic prefix is added to IFFT time domain sample outputs that forms the baseband signal with the data symbols on the set of orthogonal sub carriers. The data is transformed to analog form to be sent over the AWGN channel. At the receiver end, with the legitimate de-interleave key and the other key for the embedded data, the coveted data is extracted. This enhances security multi-fold.

RESULTS AND DISCUSSION

The BER of various modulation schemes like BPSK, QPSK and QAM in OFDM without interleaving is given in Fig. 2. From the graph, it can be illustrated that BPSK provides better BER as mentioned in (Praveenkumar *et al*., 2012a, b,) compared to QPSK and QAM. It is clear that the errors are random and unpredictable without interleaving.

Figure 3 provides the BER of various modulation schemes like BPSK, QPSK and QAM in OFDM with interleaving. From the graph, it can be illustrated that BPSK provides better BER as mentioned in (Praveenkumar *et al*., 2012a, b,) and the errors are predictable and reduced with interleaving.

The BER comparison between BPSK, QPSK and QAM with and without embedding after interleaving is given in Fig. 4.

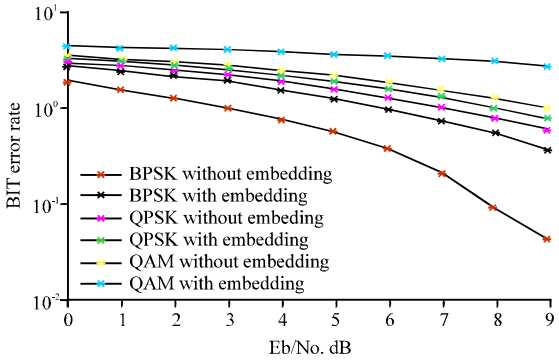

Fig. 4: BER comparison of modulation schemes like BPSK, QPSK and QAM in OFDM system with embedding after interleaving. From the BER comparison between BPSK, QPSK and QAM with and without embedding after interleaving, there is no appreciable deviation in BER graph after including additional confidential data to ensure wireless security

CONCLUSION

The OFDM technology is most suitable for Wireless communication as it manages the higher data rate with more spectrum efficiency with the use of orthogonal subcarriers. In this study, BPSK, QPSK and the QAM become the modulation schemes along with interleaving to control burst errors in the channels. It is further proved that even after the injection of data embedding after interleaving, the three modulations viz. BPSK, QPSK and QAM are not deviating more from actual BER. Among the modulations, QAM is considered more suitable even with secret additional data. From the BER graphs, the burst

errors are reduced very much in OFDM with the help of interleaving algorithm key which has become an security measure before decoding. With the second key the secret embedded data is extracted, otherwise it is not possible to uncover the secret data. As for as the data rate is considered, QAM scheme is preferred after embedding the data with additional information. However when the error rate is taken into account BPSK is more preferred.

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, 2012e. 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.

Cheddad, A., J. Condell, K. Curran and P.M. Kevitt, 2010. Digital image steganography: Survey and analysis of current methods. Signal Process., 90: 727-752.

Hmood, A.K., B.B. Zaidan, A.A. Zaidan and H.A. Jalab, 2010a. An overview on hiding information technique in images. J. Applied Sci., 10: 2094-2100.

Hmood, A.K., H.A. Jalab, Z.M. Kasirun, B.B. Zaidan and A.A. Zaidan, 2010b. On the Capacity and security of steganography approaches: An overview. J. Applied Sci., 10: 1825-1833.

Janakiraman, S., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2012a. Firmware for data security: A review. Res. J. Inform. Technol., 4: 61-72.

Janakiraman, S., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2012b. Pixel forefinger for gray in color: A layer by layer stego. Inform. Technol. J., 11: 9-19.

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.