Journal of Applied Sciences

ISSN 1812-5654

science alert

ANSInet
an open access publisher
http://ansinet.com

Journal of Applied Sciences 14 (16): 1836-1843, 2014
ISSN 1812-5654 / DOI: 10.3923/jas.2014.1836.1843

Multi (Carrier+Modulator) Adaptive System-an Anti Fading Stego Approach

Padmapriya Praveenkumar, Rengarajan Amirtharajan, R. Sai Janani,
K. Thenmozhi and J.B.B. Rayappan
School of Electrical and Electronics Engineering, SASTRA University, Thanjavur,
Tamil Nadu, India

Abstract: There are numerous criteria in running an enterprise. Apart from trading goods and services, or may be both to clients, emphasis should be laid on maintaining the business model that comprises of maintenance of intellectual properties and decisive testimonials as well. In this regard, up to date technological proficiencies be of great assist as everything is now digital and online. Though sound different, technology and administrative terms go hand in hand. Of all one domain that catch the attention instantly is secret sharing and secret communication. This study is one such work. Digital multimedia applications, coming into the limelight in the recent years have impacted the bandwidth requirements and caused an ever soaring demand for broadband wireless application. On the other hand, wireless communication that uses fixed modulation fails to satisfy the needs as its efficiency is stultified by the fading channels. This stydy proposes the adaptive modulation scheme in OFDM (Orthogonal Frequency Division Multiplexing) system to counteract fading in the transmission power and the transfer function of frequency selective channel. The prime aim is to maximise the total capacity and transmit power without vitiating the quality of service at the receiver. It can be achieved by making the system smart and subsume some intelligence into it. We make the system adapt itself to the channel conditions and choose the well-suited service at that instant. Simulation results have made it clear that adaptive modulation in OFDM system offers the choice of modulation and FEC (Forward Error Control Codes) with variable rates. The essence of adaptation is maintained even while embedding in wireless transmission to serve the security purposes. Bit Error Rate (BER) graph plotted prior to embedding is analyzed and compared with the one plotted for embedded data.

Key words: Adaptive modulation, BER, FEC, information hiding, OFDM, steganography

INTRODUCTION

In the current scenario, wireless communication has become a mandatory constituent of everybody's life. The enhanced efficiency, greater flexibility and mobility, reduced cost altogether contributes to the heightened demand of wireless techniques in current trend. OFDM is a technique adopted in wireless systems to enhance the efficiency of the spectrum countenancing signal overlap. In OFDM, the entire channel is divided into large number of closely spaced sub-carriers that are orthogonal to each other and the data is transmitted parallel via the channels (Van Nee and Prasad, 2000). The signal on the carrier is modulated by either methods- Binary Phase Shifting Keying (BPSK), Quadrature Phase Shifting Keying (QPSK) or Quadrature Amplitude Modulation (QAM).

Formatting that is done later is grounded on these modulation schemes. The formatted data in the form of bits is subjected to interleaving to avoid burst errors. Also, OFDM efficiently forbids ISI and IFI through its cyclic prefix which also helps in maintaining orthogonality between the sub carriers (Peled and Ruiz, 1980; Saltzberg, 1967). Dividing the channel into a number of flat fading sub carriers makes OFDM robust to frequency fading. FFT and IFFT techniques are usually hired for modulation and demodulation of the data (Hwang *et al*., 2009).

A pragmatic approach to conceal the data in a multimedia file withholding the smallest information about the existence of the message is called steganography (Al-Azawi and Fadhil, 2010; Zhu *et al*., 2011). This technique offers covert communication by camouflaging data into a multimedia file, known as cover image. Embedding secret data and transmission through OFDM systems was carried (Kumar *et al*., 2011; Thenmozhi *et al*., 2012; Stefan and Fabin, 2000; Praveenkumar *et al*., 2012a, b, c) out to ensure security and confidentiality over wireless data transmission systems. The vulnerability of the human auditory and visual senses against a minute

Corresponding Author: Padmapriya Praveenkumar, School of Electrical and Electronics Engineering, SASTRA University, Thanjavur, Tamil Nadu, India

changes due to the concealment of data was exploited. Then various techniques like spatial domain techniques, transform based techniques, cover generation techniques and Spread Spectrum Image Steganography (SSIS) were developed (Amirtharajan and Rayappan, 2012a, b, c, d, 2013; Amirtharajan *et al*., 2011, 2012a, b, c, 2013a, b, c, d, e).

The transform based techniques convert the image into frequency domain and then the message is written onto it. The simplest method insists on changing the LSB (Padmaa *et al*., 2011; Amirtharajan and Rayappan, 2012a) of the image in the RGB domain. The SSIS is very efficient and recent technology. It has its roots in the spread spectrum technology used in communication as the message is subjected to an spreading and interleaving before embedding on to the cover image (Cox *et al*., 1997; Marvel *et al*., 1999; Amirtharajan and Balaguru, 2011). This technique is also used in watermarking which is a form of steganography that lays emphasis on protecting the copyright and prevents the unauthorized modification in the file. Nowadays the signature is interleaved and written onto the whole of the image that can be extracted to prove its creator when necessary.

Digital image steganography survey and its various techniques used to embed data has been discussed (Amirtharajan *et al*., 2012a; Cheddad *et al*., 2010; Petitcolas *et al*., 1999). Cryptography is a technique which is often combined and confused with steganography. It employs the use of the public or private keys of the receiver to encrypt the data without the knowledge of which retrieval of data is not possible (Schneier, 2007). It converts data into a cipher text before transmission. Often to improve the secrecy of the message in a steganography, the message is subjected to cryptography and embedded as a cipher text which may demand larger capacity of the stego system. There have been various methods deployed to detect, extract or destroy the message without affecting the cover image (Amirtharajan and Rayappan, 2012a; Rajagopalan *et al*., 2012; Janakiraman *et al*., 2012a, b; Luo *et al*., 2011; Zhao and Luo, 2012).

The process used to identify the occurrence of a message is known as stego analysis. The effectiveness of a stego scheme lies in the imperceptibility of the message failing which the entire system is said to have failed (Amirtharajan *et al*., 2012a, b, 2013a, b, c, d, e; Thanikaiselvan *et al*., 2012a, b, 2013). Of late, researches are being done to use audio and video files instead of an image to cover data (Al-Frajat *et al*., 2010; Zhu *et al*., 2011).

Convolutional coding is a type of FEC in which the input message bits will be serial rather than blocks and it utilizes shift register with modulo 2 adders and multiplexers that provides the decoded output bits (Summerfield, 1996; Sudhakar *et al*., 2000). It accepts K input bits from 2 k combination bits and then outputs n bits from the set of 2n output symbols (Benedetto *et al*., 2003). The output of the decoder depends on the present and sometimes on the previous set of inputs also.

To provide the demanding need for the future generation, adaptive modulation has come to the rescue. By knowing the Channel State Information (CSI) (Goldsmith and Chua, 1998; Seiichi and Hiroshi, 2007; Toni and Conti, 2011) the type of modulation, FEC can be varied to adopt the channel conditions to provide better BER and to utilize the spectrum efficiently.

After reviewing the available literature on adaptive modulation in OFDM and steganography, this study proposes an adaptive choice of modulation and FEC based on AWGN, Rayleigh and Rician fading channel's state information. Then confidential data bits have entrenched subsequent to modulation using the phase value of the modulated output as secret key. BER graphs are plotted using different modulation schemes after embedding.

METHODOLOGY

A linear stream of 256 binary bits is given as inputs to the proposed system. The forward error control block generates convolutional encoder utilizing 1/2 and 1/3 code rates. Then data's are encoded using the FEC earlier to transmission. The confidential information is added as an additional phase value at the output of the signal mapper.

FEC codes determines the ability of the receiver to correct and detect errors with no reverse channel to demand retransmission of data, but at the rate of a fixed, privileged forward channel bandwidth. Here FEC used is convolutional encoder and viterbi decoder of rate ½ and 1/3. Then the coded outputs are 512 and 768, respectively with punctured pattern of [1 0] and [1 1 0] are utilised with 64 point IFFT and ¼ CP is considered.The channel considered are AWGN, Rayleigh and Rician. The signal mapper block is a modulator that can modulate the encoded data in to complex constellation points by making use of BPSK, QPSK and 8 QAM schemes, thus enabling long distance transmission as shown in Fig. 1.

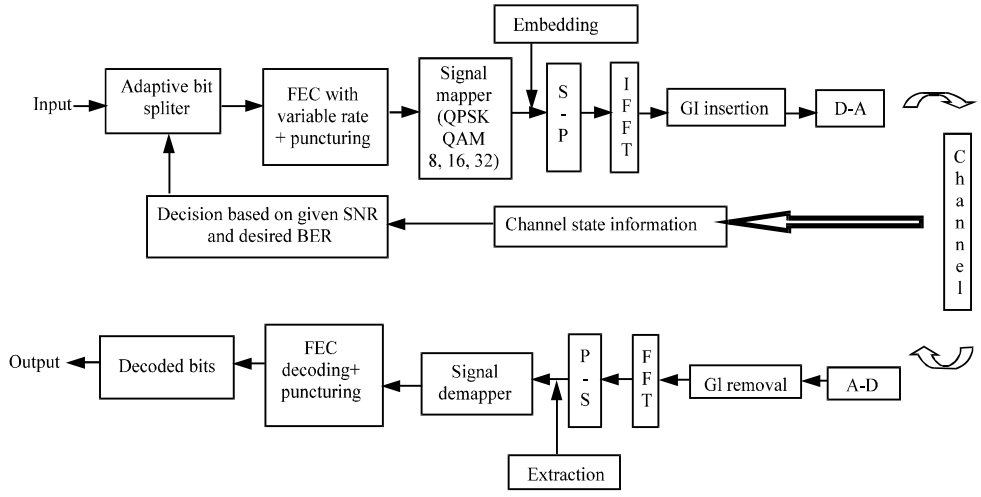

Fig. 1: Proposed methodology

Secret data bits have been embedded along with the original information which adds security and confidentiality to the system. This is can be done by embedding the secret data after modulation using the phase value as key. Then, serial-to-parallel conversion takes place for grouping the bits to Inverse Fast Fourier Transform (IFFT). This is done to insert orthogonal sub-carriers into the symbols obtained by modulation, to obtain OFDM symbols. A safeguard band is inserted among the OFDM symbols to eradicate Inter Symbol Interference (ISI). The digital data is converted into analog form and transmitted through fading channels.

The channels are the models of real-world phenomena like scattering, dispersion, fading etc. The Rayleigh channel characterizes the non-line-of-sight path and Rician channel simulates the line-of-sight path. AWGN is used to add uniform white Gaussian noise.Then the received information, is again converted back to digital form for further processing. Then the guard interval inserted earlier is removed. Then Fast Fourier Transform (FFT) operation is carried out to separate all the carriers of the OFDM signal and the parallel data stream is converted into serial bits. Then the secret data embedded during the transmission is extracted by knowing the phase value and the number of bits embedded and their locations. This maintains immense security over the channel. Depending on the type of encoding procedure used, corresponding decoding is carried out.

After the decoding, the original information bits can be retrieved. The output of the system can be compared with the input to check its accuracy and reliability. Simultaneously, the data being sent over the channel is tapped to obtain the Channel State Information (CSI). This information describes how a signal propagates through the channel and the combined effect of fading, scattering, dispersion etc.

The BER values and EB/No can be plotted for ½ and 2/3 rates of convolutional encoder using BPSK, QPSK and QAM over AWGN, Rayleigh and Ricin fading channels. From the BER plots, adequate information regarding the reliability of the channel and system can be obtained. This helps in making the system adaptive to current channel conditions, thus improving the system efficiency. QPSK is preferred for more noisy channels because its more prone to interference produced by fading channels than QAM. QAM requires stronger error control codes compared to QPSK which means lower information rate and more number of redundant bits.

RESULTS AND DISCUSSION

Input data bits of 256 is taken with convolutional encoder of rate ½ and 1/3 are used with punctured pattern of [1 0] and [1 1 0] are utilised with 64 point IFFT and ¼ CP is considered. The channel considered are AWGN, Rayleigh and Rician. The BER comparison between AWGN, Rayleigh and Rician fading channels using convolutional encoder of rates ½ in OFDM system after embedding secret data bits using BPSK, QPSK and QAM are given in Fig. 2, 3 and 4, respectively.

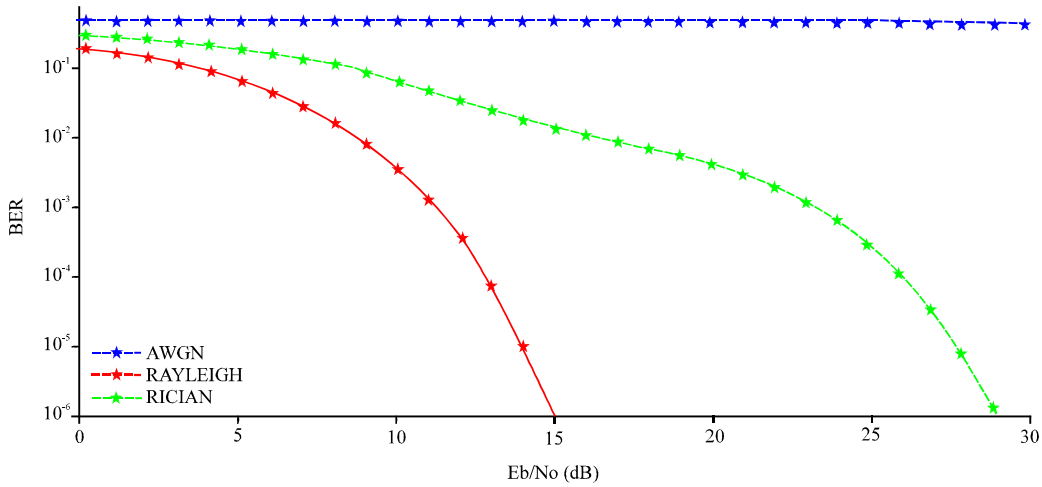

Fig. 2: Comparison between AWGN, rayleigh and rician channels using convolutional encoder of rate ½ using BPSK in OFDM

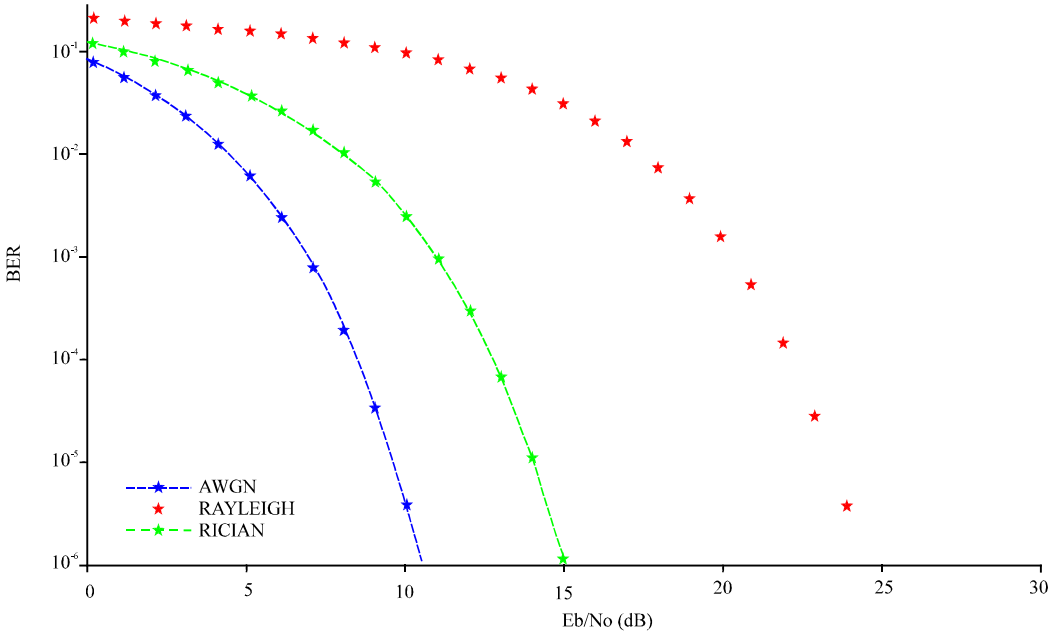

Fig. 3: Comparison between AWGN, rayleigh and rician channels using convolutional encoder of rate ½ using QPSK in OFDM

From the BER values obtained using Fig. 2, 3 and 4, AWGN provides better BER compared to other two channels using convolutional encoder with QPSK of rate 1/2. The BER comparison between AWGN, Rayleigh and Rician fading channels using convolutional encoder of rates 1/3 in OFDM system after embedding secret data bits using BPSK, QPSK and QAM are given in Fig. 5, 6 and 7, respectively. From the BER values obtained using Fig. 5, 6 and 7, AWGN provides better BER compared to other two channels using Convolutional encoder with QPSK of rate 1/3. In QPSK modulation with convolutional encoder of rate 1/3 Rician outperforms Rayleigh, but in QAM modulation with convolutional encoder of rate 1/3 Rayleigh outperforms Rician channel. But comparatively code rate of 1/3 convolutional encoder provides better BER than ½ for OFDM systems employing QPSK modulation.

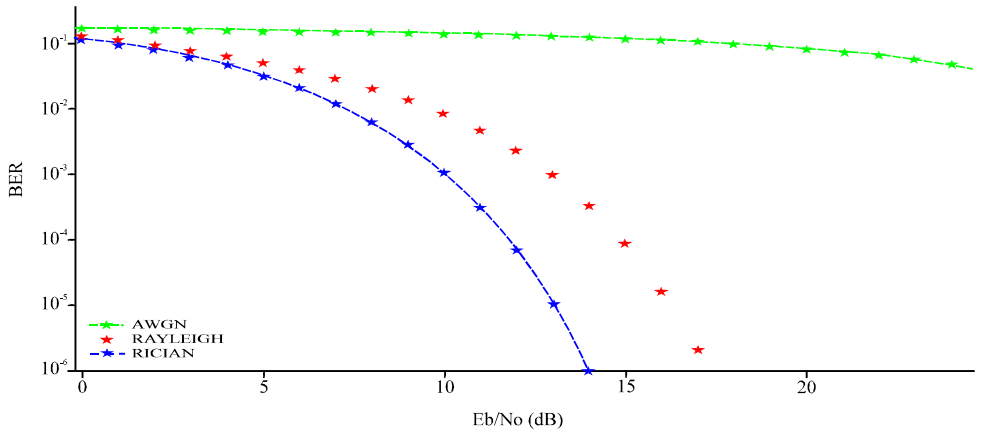

Fig. 4: Comparison between AWGN, Rayleigh and Rician channels using convolutional encoder of rate ½ using QAM in OFDM

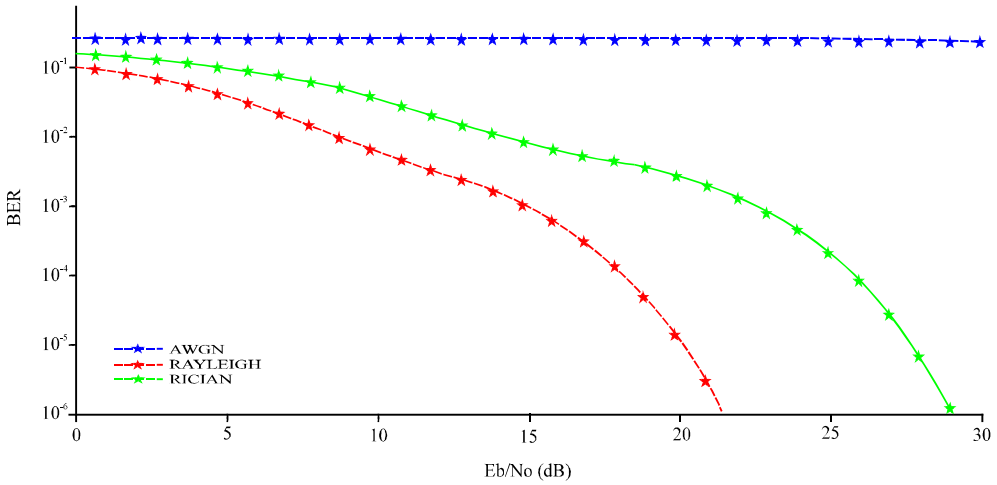

Fig. 5: Comparison between AWGN, Rayleigh and Rician channels using convolutional encoder of rate 1/3 using BPSK in OFDM

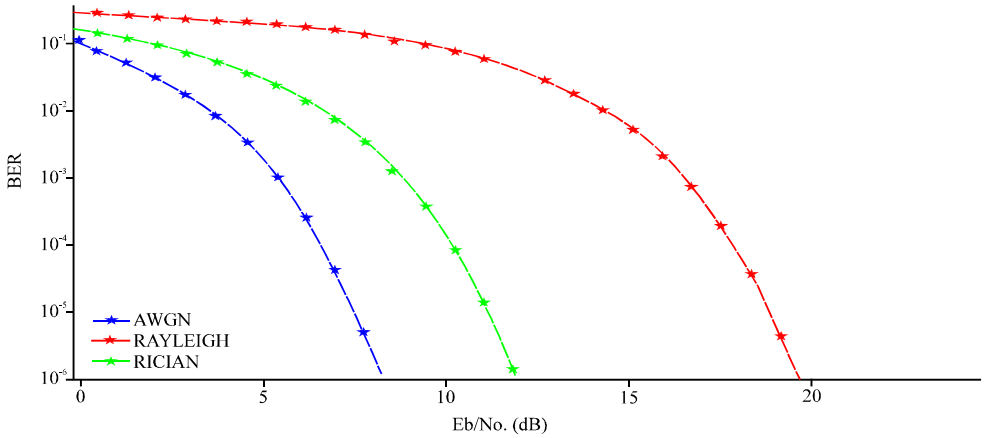

Fig. 6: Comparison between AWGN, Rayleigh and Rician channels using convolutional encoder of rate 1/3 using QPSK in OFDM

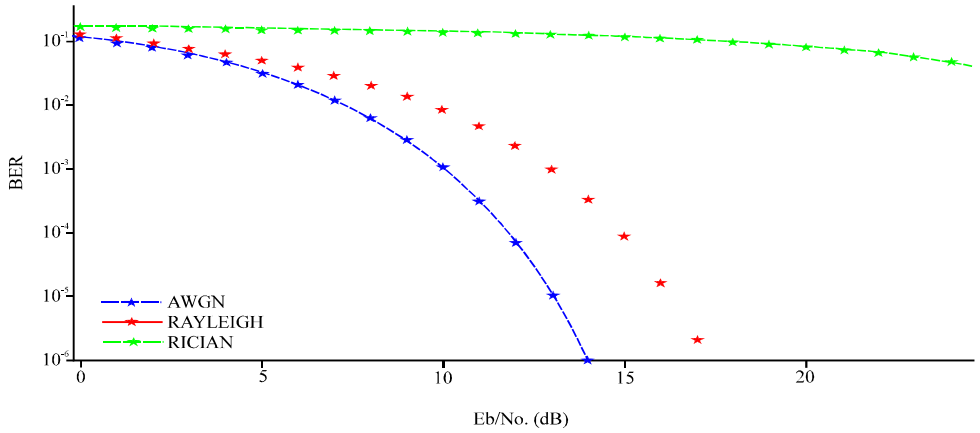

Fig. 7: Comparison between AWGN, Rayleigh and Rician channels using convolutional encoder of rate 1/3 using QAM in OFDM

CONCLUSION

Business data security's endeavors and goals sound somewhat diverse as that of conventional security courses. At the minute, focus is on design and development of innovative security technologies.As enterprises are unable to meet the expense of security risks, economical but complex expertise is now the most wanted. This is to validate the optimal sum of expenses to make certain that the information assets are adequately cosseted. This study does this job more effectively with the help of modern day technology. Adaptive modulation is preferred in OFDM wireless system to improve the transmission efficiency by knowing the CSI. In this study adaptive modulation utilizing BPSK, QPSK and QAM modulation schemes using Convolutional encoder of rate ½ and 1/3 are passed over AWGN/Rayleigh/ Rician fading channels .The secret data bits has been embedded after modulation to ensure security and confidentiality of the transmitted data. By knowing the exact phase value (key), the secret data bits can be retrieved. From the BER graphs, convolutional encoder of rate 1/3 with QPSK is preferred for Rician fading channels and QAM is preferred for Rayleigh fading channels. In both the sytmes with convolutional encoder of rate ½ and 1/3 QPSK system is superior in performance as compared with BPSK and QAM and in all the techniques adopted, AWGN provides superior BER than Rayleigh and Rician fading channels.

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 R.J.B. Balaguru, 2011. Covered CDMA multi-user writing on spatially divided image. Proceedings of the 2nd International Conference on Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology, February 28-March 3, 2011, Chennai, India, pp: 1-5.

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, 2012a. Random image steganography and steganalysis: Present status and future directions. Inform. Technol. J., 11: 566-576.

Amirtharajan, R., K. Ramkrishnan, M.V. Krishna, J. Nandhini and J.B.B. Rayappan, 2012b. Who decides hiding capacity? I, the pixel intensity. Proceedings of the International Conference on Recent Advances in Computing and Software Systems, April 25-27, 2012, Chennai, India, pp: 71-76.

Amirtharajan, R., V. Mahalakshmi, N. Sridharan, M. Chandrasekar and J.B.B. Rayappan, 2012c. Modulation of hiding intensity by channel intensity-Stego by pixel commando. Proceedings of the International Conference on Computing, Electronics and Electrical Technologies, March 21-22, 2012, Kumaracoil, pp: 1067-1072.

Amirtharajan, R. and J.B.B. Rayappan, 2013. Steganography-time to time: A review. Res. J. Inform. Technol., 5: 53-66.

Amirtharajan, R., K. Karthikeyan, M. Malleswaran and J.B.B. Rayappan, 2013a. Kubera kolam: A way for random image steganography. Res. J. Inform. Technol., 5: 304-316.

Amirtharajan, R., M.V. Abhiram, G. Revathi, J.B. Reddy, V. Thanikaiselvan and J.B.B. Rayappan, 2013b. Rubik's cube: A way for random image steganography. Res. J. Inform. Technol., 5: 329-340.

Amirtharajan, R., P. Archana and J.B.B. Rayappan, 2013c. Why image encryption for better steganography. Res. J. Inform. Technol., 5: 341-351.

Amirtharajan, R., S. Sulthana, P.S. Priya, G. Revathi, A.K. Infant and J.B.B. Rayappan, 2013d. Seeable visual but not sure of it-A visual cryptographic perspective for TAMIL characters. Int. J. Eng. Technol., 5: 2000-2007.

Amirtharajan, R., S.D. Roy, N. Nesakumar, M. Chandrasekar, R. Sridevi and J.B.B. Rayappan, 2013e. Mind game for cover steganography: A refuge. Res. J. Inform. Technol., 5: 137-148.

Amirtharajan, R., R.R. Subrahmanyam, P.J.S. Prabhakar, R. Kavitha and J.B.B. Rayappan, 2011. MSB over hides LSB: A dark communication with integrity. Proceedings of the IEEE 5th International Conference on Internet Multimedia Systems Architecture and Application, December 12-14, 2011, Bangalore, Karnataka, India, pp: 1-6.

Benedetto, S., G. Montorsi and D. Divsalar, 2003. Concatenated convolutional codes with interleavers. IEEE Commun. Mag., 41: 102-109.

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.

Cox, I.J., J. Kilian, F.T. Leighton and T. Shamoon, 1997. Secure spread spectrum watermarking for multimedia. IEEE Trans. Image Process., 6: 1673-1687.

Goldsmith, A.J. and S.G. Chua, 1998. Adaptive coded modulation for fading channels. IEEE Trans. Commun., 46: 595-602.

Hwang, T., C.Y. Yang, G. Wu, S.Q. Li and G.Y. Li, 2009. OFDM and its wireless applications: A survey. IEEE Trans. Veh. Technol., 58: 1673-1694.

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.

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, Chennai, India, pp: 1-5.

Luo, H., Z. Zhao and Z.M. Lu, 2011. Joint secret sharing and data hiding for block truncation coding compressed image transmission. Inform. Technol. J., 10: 681-685.

Marvel, L.M., C.G. Jr. Boncelet and C.T. Retter, 1999. Spread spectrum image steganography. IEEE Trans. Image Process., 8: 1075-1083.

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

Peled, A. and A. Ruiz, 1980. Frequency domain data transmission using reduced computational complexity algorithms. Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing, April 19-24, 1980, Taipei, Taiwan, pp: 964-967.

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. Proc. 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, J. Bosco and 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.

Saltzberg, B., 1967. Performance of an efficient parallel data transmission system. IEEE Trans. Commun. Technol., 15: 805-811.

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

Seiichi, S. and H. Hiroshi, 2007. System design issues and performance evaluations for adaptive modulation in new wireless access systems. Proc. IEEE, 95: 2456-2471.

Stefan, K. and A. Fabin, 2000. Information Hiding Techniques for Steganography and Digital Watermarking. Artech House, London, UK.

Sudhakar, R., A. Mukhtar and Z. Gu, 2000. Low-complexity error selective Viterbi decoder. Electron. Lett., 36: 147-148.

Summerfield, S., 1996. Analysis of convolutional encoders and synthesis of rate-2/n Viterbi decoders. IEEE Trans. Inform. Theory, 42: 1280-1285.

Thanikaiselvan, V., P. Arulmozhivarman, J.B.B. Rayappan and R. Amirtharajan, 2012a. Graceful graph for graceful security-towards a STE (G) Raph. Res. J. Inform. Technol., 4: 220-227.

Thanikaiselvan, V., P. Arulmozhivarman, R. Amirtharajan and J.B.B. Rayappan, 2012b. Horse riding and hiding in image for data guarding. Proc. Eng., 30: 36-44.

Thanikaiselvan, V., P. Arulmozhivarman, S. Subashanthini and R. Amirtharajan, 2013. A graph theory practice on transformed image: A random image steganography. Sci. World J. 10.1155/2013/464107

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.

Toni, L. and A. Conti, 2011. Does fast adaptive modulation always outperform slow adaptive modulation? IEEE Trans. Wireless Commun., 10: 1504-1513.

Van Nee, R. and R. Prasad, 2000. OFDM for Wireless Multimedia Communications. Artech House, Norwell, MA., USA., ISBN-13: 9780890065303, Pages: 260.

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.