Journal of Applied Sciences

ISSN 1812-5654

science alert

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

Journal of Applied Sciences 14 (15): 1728-1735, 2014
ISSN 1812-5654 / DOI: 10.3923/jas.2014.1728.1735

Sub Carriers Carry Secret: An Absolute Stego Approach

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

Abstract: Information security is a prime concern especially when it comes to business and corporate sectors where off the record information should be given utmost importance. Very cooperative especially to business enterprise, modern day expertise has contributed a lot towards sharing a surreptitious data. The field of wireless communication has surmounted many hurdles in the past few years and is now finally capable of supporting higher data rates thanks to the development of Orthogonal Frequency Division Multiplexing (OFDM). It is the most ideal format for broadband communication to meet its need for higher data rates. This study further augment the usefulness of OFDM communication by making it secure to avert data piracy. This study propose an idea of embedding the secret message at the real part of Inverse Fast Fourier Transform (IFFT) output of OFDM system and performance of the system is examined for various modulations. Thus, this study is a conjunction of wireless and data security which serves the purpose of secret sharing and can be applicable and suitable to entrepreneurial activities.

Key words: IFFT, information hiding, OFDM, steganography

INTRODUCTION

Check in order to deal with the increasing demand for higher data rate and channel capacity, the concept of multiplexing was introduced (Van Nee and Prasad, 2000). Frequency Division Multiplexing (FDM) which was the first type of multiplexing scheme, enhanced the bandwidth efficiency of the channel, by dividing the entire channel into many sub carriers (Peled and Ruiz, 1980; Saltzberg, 1967; Scholtz, 1982). With advancements in wireless technology and their several smart applications, the demands of the users increased manifold calling for new and improved technology. Thus, the FDM paved way for OFDM (Chang, 1970) which is a multicarrier broadband system in which usable bandwidth is separated into narrow bands by which serial data is transmitted in parallel (Akansu *et al*., 1998; Akay and Ayanoglu, 2004; Hussain *et al*., 2011; Pickholtz *et al*., 1984; Thenmozhi *et al*., 2012; Sun *et al*., 2013).

Each sub carrier has a unique frequency which is an integral multiple of cycles in symbol period (Chang and Gibby, 1968; Van Nee and Prasad, 2000). Adding cyclic prefix, larger than or almost equal to the channel order, during transmission is primarily used to avoid IBI. The effectuation of FFT in this technique has allowed the use of a set of harmonically related functions as sub carriers, each of which is fed to the single tap equaliser at the receiver end using scalar division (Amirtharajan and Balaguru, 2011; Kumar *et al*., 2011; Peled and Ruiz, 1980; Thenmozhi *et al*., 2011, 2012; Praveenkumar *et al*., 2012a-c, 2013a-l). Thus, OFDM, to-day, is widely preferred in high speed internet and proposed to be used in 4G technology (Al-Kebsi, 2008).

Wireless communication has revolutionized the world by overcoming the inconveniences caused by wired communication. Even though there is no trouble of wires, wireless communication is prone to bit errors while transmission. The packets received are often undetectable or have a very high impact of noise that renders it un-usable. Hence, Forward Error Correction (FEC) is vital in wireless communication systems. These FEC codes add error correction information to the code prior to the transmission that helps in correcting the errors in the signal, if any.

The methods of encoding and decoding data, used to achieve privacy, leak the message out to the intruders. To prevent this, a technology was developed to embed a message or a cipher text inside an image or a multimedia file called steganography (Al-Frajat *et al*., 2010; Ahmed *et al*., 2010; Amirtharajan *et al*., 2013a-e; Amirtharajan and Rayappan, 2012a-d; Ramalingam *et al*., 2014; Janakiraman *et al*., 2012a, b; Marvel *et al*., 1999; Padmaa *et al*., 2011; Thanikaiselvan *et al*., 2011, 2012a, b, 2013) and the file is called stego image.

The simplest LSB steganography technique a spatial domain, changes the LSB of any of the layers of the RGB colour pattern of an image. The palette based technique hides the message in one of the colour palettes of the image. The transform based techniques employ an alteration in the coefficients of the frequency domain representation of the image. Another classification related to secure communication called spread communication

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

(Pickholtz *et al*., 1982; 1984; Pickholtz *et al*., 1991). Covert communication using CDMA was proposed and carried out in (Amirtharajan and Balaguru, 2011; Praveenkumar *et al*., 2012a-c, 2013a-j) and a detailed survey on image steganography was illustrated in (Amirtharajan *et al*., 2012a; Cheddad *et al*., 2010; Karzenbeisser and Perircolas, 2000; Rajagopalan *et al*., 2012).

The LSB, though primitive, is the easiest way to implement but also easily detectable. Cryptography and watermarking are two techniques that are very strongly correlated to steganography. While watermarking is another type of technology, Cryptography uses keys for protecting the messages (Karzenbeisser and Perircolas, 2000; Schneier, 2007). Watermarking is used to protect the ownership of a file or a message or simply to copyright a file. The creator's name is embedded in the file that cannot be detected by steg analysis thus preventing any one else claiming the ownership of that file. Cryptography generates keys that are acknowledged merely to the sender and the receiver alone during each transmission to secure the message, without whose knowledge one cannot open the message. Cheddad *et al*. (2010) presented a detailed survey on image steganography and steg analysis and there are several information hiding schemes for secret data embedding.

After reviewing the available literature carefully, this study proposes the data embedding scheme after the IFFT block of OFDM to ensure secure data transmission and reception over wireless medium. The next section explains the proposed method followed by results and discussion. The final section conclude that BPSK modulation is preferred compared to other two QPSK and QAM modulation schemes.

METHODOLOGY

The OFDM block diagram with data embedding and extraction is shown in the Fig. 1. In this system, the symbols are produced with symbol rate and these serial data streams are converted in to parallel data's with symbol rate of $\bar{N}$ where N denotes the sub carriers and TS represents the symbol period. Modulation schemes like Binary Phase Shift Keying (BPSK), Quadrature Phase Shift Keying (QPSK) and Quadrature Amplitude Modulation (QAM) schemes are used to produce the constellation points. The complex parallel data symbols are modulated by an Inverse Fast Fourier Transform (IFFT) for converting the symbols from frequency to time domain waveforms. Then separating the real and imaginary parts of the IFFT outputs and then embedding the secret data in the real part of the IFFT output as in Fig. 2. Because embedding in the phase value of IFFT degrades the output performance. This increases the security level of the hidden information and increases the complexity in extracting the information by the intruder.

The FFT and IFFT equations are given in Eq. 1 and 2, respectively:

$$X(f) = \sum_{m=1}^{N} x(m) e^{-J2\pi(f-1)\frac{m-1}{N}} \quad 1 \le f \le m \tag{1}$$

$$X(m) = \frac{1}{N} \sum_{f=1}^{N} X.(f)\ e^{-J2\pi(f-1)(\frac{m-1}{N})} \quad 1 \le m \le N \tag{2}$$

$$X(m) \Rightarrow \text{real}$$

then X(m) can be represented as Eq. 3:

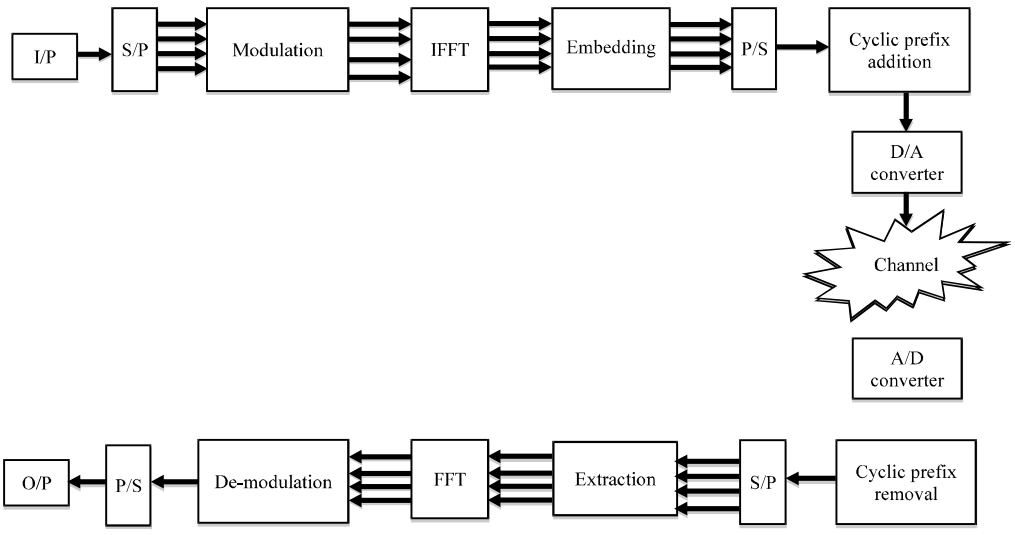

Fig. 1: Proposed block diagram

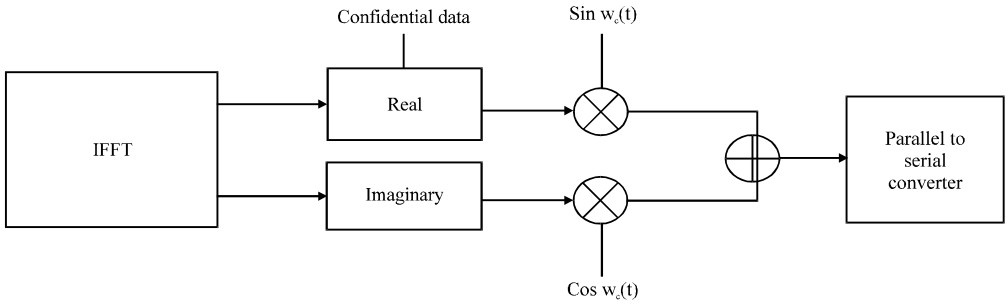

Fig. 2: Embedding in real part of IFFT

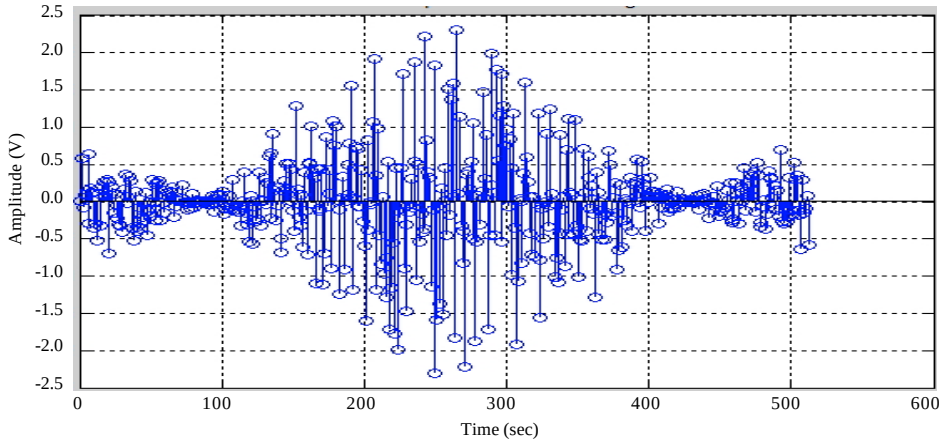

Fig. 3: IFFT output using BPSK modulation scheme before embedding the secret data bits

$$X(m) = \frac{1}{N}\sum_{f=1}^{N} a(f)\cos\left(\frac{2\pi(f-1)(m-1)}{N}\right) + b(f)\sin\left(\frac{(2\pi(f-1)(m-1))}{N}\right) \quad (3)$$

Then one fourth of the total symbol is added to the actual OFDM symbol which is termed as cyclic prefix which is maintained to eradicate Inter Symbol Interference (ISI) and Inter Carrier Interference (ICI). By maintaining the orthogonality condition between the sub carriers of the OFDM system more number of subcarriers can be accommodated without interference. Then finally the orthogonal symbols are converted in to equivalent. As final stage in transmitter section, the digital signal is transformed into its equivalent analog form and then transmitted over the Additive White Gaussian Noise (AWGN) channel.

In Receiver, analog signal is converted into its digital form. After the cyclic prefix removal, the data's are passed over FFT block, where by knowing the exact key value the secret data has been extracted. Then the data's are demodulated to get the desired output. If the key value is known the secret data can be extracted, if unknown secret remains secret and the original data alone can be extracted.

RESULTS AND DISUSSION

The various output waveforms of the time domain signal outputs at the IFFT of the OFDM system previous to and behind embedding the secret data using modulation schemes like BPSK, QPSK and QAM are shown below.

Figure 3 and 4, shows the variation of the IFFT output using BPSK modulation before and after embedding are shown.

Figure 5 and 6, shows the variation of the IFFT output using QPSK modulation before and after embedding are shown.

Figure 7 and 8, shows the variation of the IFFT output using QAM modulation before and after embedding is shown.

From the output plots, BPSK is preferred compared to the other two modulation schemes, because the number of modulated output bits are larger compared to the other two modulation schemes and the number of IFFT output points is also more. So, the numbers of confidential bits that is being fixed and extracted are more. Figure 9 provides the comparison between various modulation schemes like BPSK, QPSK, 8, 16, 32 and 64 QAM,

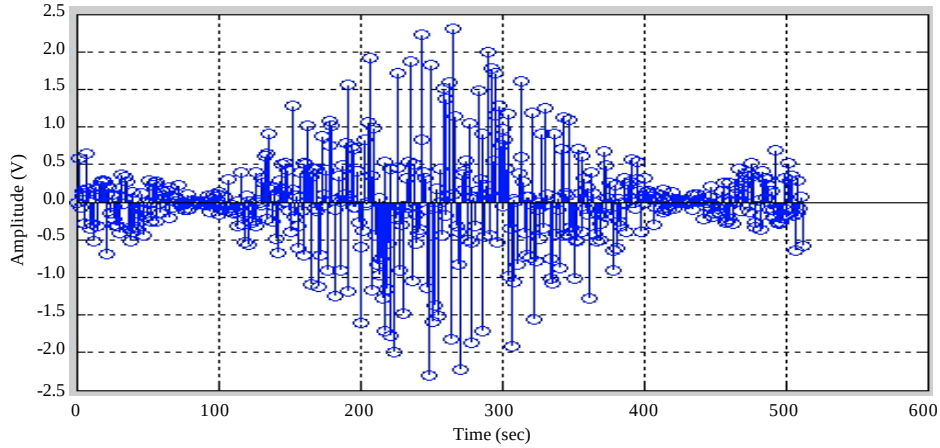

Fig. 4: Embedding done before and after IFFT block using BPSK modulation

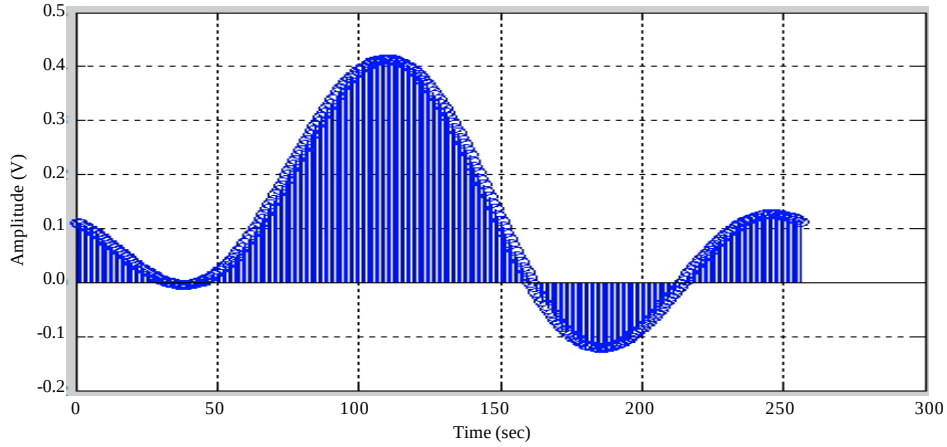

Fig. 5: IFFT output using QPSK modulation scheme before embedding secret data bits

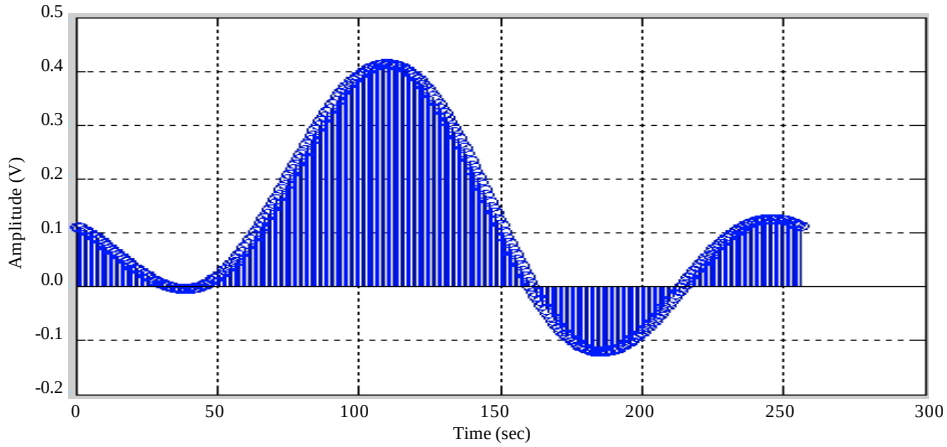

Fig. 6: Embedding done before and after IFFT block using QPSK modulation

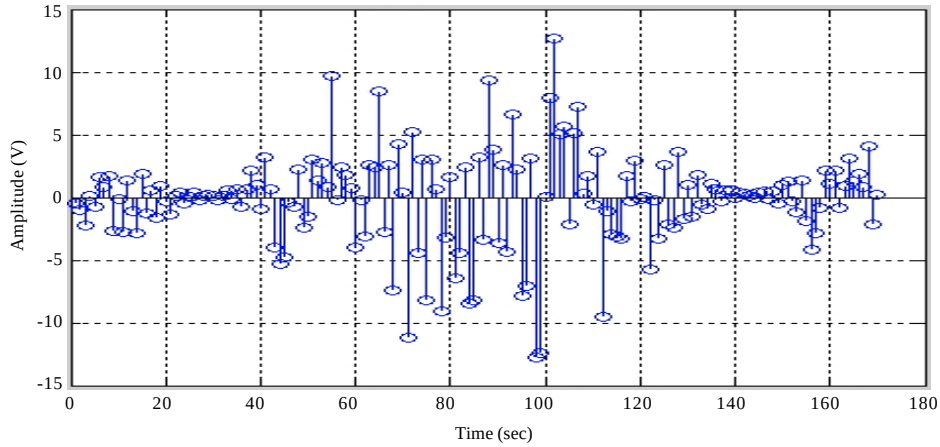

Fig. 7: IFFT output using QAM modulation scheme before embedding secret data bits

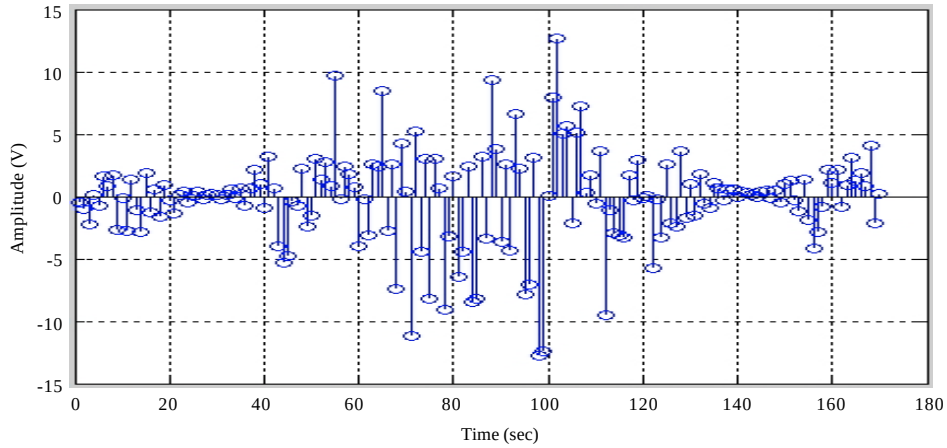

Fig. 8: Embedding done after IFFT block using QAM modulation

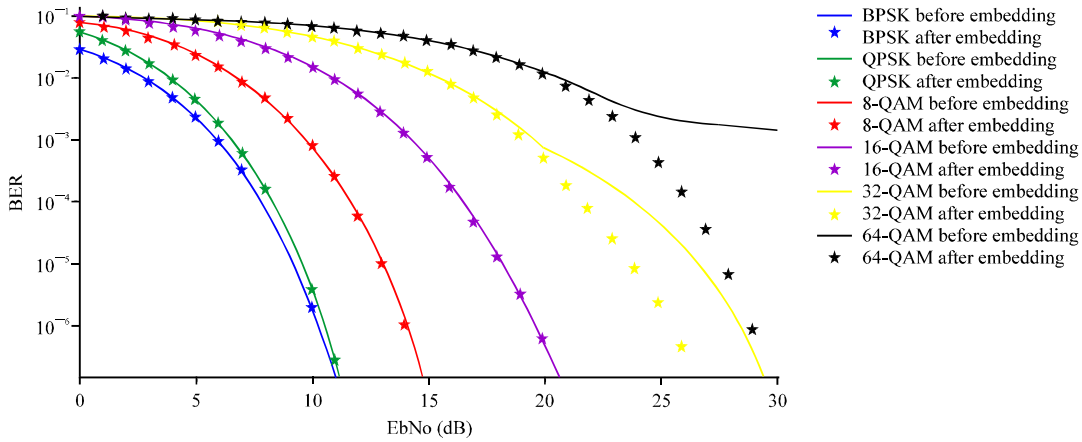

Fig. 9: BER comparison between various modulation schemes before and after embedding secret data bits at the output of IFFT

respectively. From the figure, there is no change in BER graph before and after embedding the secret data bits till 20 dB for all modulation schemes.

CONCLUSION

In this study, the performance of secure communication in OFDM system is analyzed for various modulation schemes like BPSK, QPSK and QAM. From the IFFT output plots, embedding secret data in the real part of the IFFT output shows better results even after embedding. The input bits are meager and the IFFT output points are also lesser for QAM modulation compared to QPSK and BPSK modulation schemes. So, the number of confidential bits that can be entrenched in QAM should be less compared to the other two schemes, otherwise it deteriorates the output performance by reducing the orthogonality between subcarriers. So, for better embedding, BPSK modulation is preferred compared to other two modulation schemes. This study has all the practical implementation possibilities which lend a helping hand in maintaining and safeguarding important testimonials and credentials.

REFERENCES

Ahmed, M.A., M.L.M. Kiah, B.B. Zaidan and A.A. Zaidan, 2010. A novel embedding method to increase capacity and robustness of low-bit encoding audio steganography technique using noise gate software logic algorithm. J. Applied Sci., 10: 59-64.

Akansu, A.N., P. Duhamel, X.M. Lin and M. de Courville, 1998. Orthogonal transmultiplexers in communication: A review. IEEE Trans. Signal. Process., 46: 979-995.

Akay, E. and E. Ayanoglu, 2004. High performance Viterbi decoder for OFDM systems. Proceedings of the IEEE 59th Vehicular Technology Conference, Volume 1, May 17-19, 2004, Irvine, CA., USA., pp: 323-327.

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.

Al-Kebsi, I.I.M., 2008. The impact of modulation adaptation and power control on peak to average power ratio clipping technique in orthogonal frequency division multiplexing of fourth generation systems. J. Applied Sci., 8: 2776-2780.

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. 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. 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. Brownian motion of binary and gray-binary and gray bits in image for stego. J. Applied Sci., 12: 428-439.

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., V. Mahalakshmi, N. Sridharan, M. Chandrasekar and J.B.B. Rayappan, 2012b. 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., K. Ramkrishnan, M.V. Krishna, J. Nandhini and J.B.B. Rayappan, 2012c. 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. and J.B.B. Rayappan, 2013. Steganography-time to time: A review. Res. J. Inform. Technol., 5: 53-66.

Amirtharajan, R., S. Sulthana and J.B.B. Rayappan, 2013a. Seeing and believing is a threat: A visual cryptography schemes. Res. J. Inform. Technol., 5: 435-441.

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., K. Karthikeyan, M. Malleswaran and J.B.B. Rayappan, 2013e. Kubera kolam: A way for random image steganography. Res. J. Inform. Technol., 5: 0-316.

Chang, R. and R. Gibby, 1968. A theoretical study of performance of an orthogonal multiplexing data transmission scheme. IEEE Trans. Commun. Technol., 16: 529-540.

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

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.

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.

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

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

Karzenbeisser, S. and F.A.P. 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, Chennai, India, pp: 1-5.

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.

Pickholtz, R.L., D.L. Schilling and L.B. Milstein, 1982. Theory of spread-spectrum communications-a tutorial. IEEE Trans. Commun., 30: 855-884.

Pickholtz, R.L., D.L. Schilling and L.B. Milstein, 1984. Revisions to Theory of spread-spectrum communications-a tutorial. IEEE Trans. Communi., 32: 211-212.

Pickholtz, R.L., L.B. Milstein and D.L. Schilling, 1991. Spread spectrum for mobile communications. IEEE Trans. Vehicular Technol., 40: 313-322.

Praveenkumar, P., R. Amirtharajan, Y. Ravishankar, K. Thenmozhi, J. Bosco and B. Rayappan, 2012a. 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.

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, K. Thenmozhi and J.B.B. Rayappan, 2012c. Phase for face saving-a multicarrier stego. Proc. Eng., 30: 790-797.

Praveenkumar, P., G.S. Hemalatha, B. Reddy, K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2013a. Secret link through Simulink: A stego on OFDM channel. Inform. Technol. J.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2013b. Data puncturing in OFDM channel: A multicarrier stego. Inform. Technol. J.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2013c. Inserted embedding in OFDM channel: A multicarrier stego. Inform. Technol. J.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2013d. Purposeful error on OFDM: A secret channel. Inform. Technol. J.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2013e. Reversible steganography on OFDM channel-a role of RS coding. Inform. Technol. J.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2013f. Spread and hide: A stego transceiver. Inform. Technol. J.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2013g. Stego in multicarrier: A phase hidden communication. Inform. Technol. J.

Praveenkumar, P., K. Thenmozhi, M.N. Dinesh and R. Amirtharajan, 2013h. Fixing, padding and embedding: A modulated stego. Int. J. Eng. Technol., 5: 2257-2261.

Praveenkumar, P., K. Thenmozhi, S. Vivekhanandan, J.B.B. Rayappan and R. Amirtharajan, 2013i. Intersect embedding on OFDM channel-a stego perspective. Proceedings of the IEEE Conference on Information and Communication Technologies, April 11-12, 2013, JeJu Island, pp: 1211-1214.

Praveenkumar, P., M. Nagadinesh, P. Lakshmi, K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2013j. Convolution and viterbi EN(DE)coders on OFDM hides, rides and conveys message-A neural STEGO. Proceedings of the International Conference on Computer Communication and Informatics, January 4-6, 2013, Coimbatore, pp: 1-5.

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2013k. Can we reduce PAPR? OFDM+PTS+SLM+STEGO: A novel approach. Asian J. Sci. Res., 6: 38-52.

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2013l. OFDM with low PAPR: A novel role of partial transmit sequence. Res. J. Inform. Technol., 5: 35-44.

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.

Ramalingam, B., R. Amirtharajan and J.B.B. Rayappan, 2014. Stego on FPGA: An IWT approach. Sci. World J. 10.1155/2014/192512

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.

Scholtz, R.A., 1982. The origins of spread-spectrum communications. IEEE Trans. Commun., 30: 822-854.

Sun, Z., F. Zeng and X. Ling, 2013. Research of OFDM system ICI suppression method based on orthogonal wavelet. Inform. Technol. J., 12: 7704-7708.

Thanikaiselvan, V., P. Arulmozhivarman, R. Amirtharajan and J.B.B. Rayappan, 2011. Wave (let) decide choosy pixel embedding for stego. Proceedings of the International Conference on Computer, Communication and Electrical Technology, March 18-19, 2011, India, pp: 157-162.

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

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

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