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): 1985-1991, 2014
ISSN 1812-5638 / DOI: 10.3923/itj.2014.1985.1991

Purposeful Error on OFDM: A Secret Channel

Padmapriya Praveenkumar, 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: Improved Signal to Noise Ratio (SNR) and variable higher data rates will pave a way to a brighter future for the next generation broadband applications of wireless communication. The OFDM system tolerates robustness against the multipath effects encountered by the fading channels. Enhanced system is achieved by using Forward Error Correction (FEC) codes. The attrition of errors in signals will increase the reliability of the system. In this study, secret data has been embedded after encoding the data using Convolutional encoders and passed over OFDM system. At the receiver end, Artificial Neural Network (ANN) helps better BER. The signals are passed over an OFDM receiver and decoded using Viterbi decoders.

Key words: FEC, OFDM, ANN, steganography, viterbi decoders

INTRODUCTION

In order to tackle the intensifying demand for increased data rate and channel capacity of the transmission line, the concept of multiplexing was brought in. The pioneer was the Frequency Division Multiplexing (FDM) which enhanced the bandwidth efficiency of the channel, by dividing the entire channel into many sub carriers. With the progress of wireless technology and their extended smart applications, the users and their demand further more increased calling for an amended technology. Thus, the FDM was extended to OFDM (orthogonal frequency division multiplexing) which is a multicarrier broadband system in which usable bandwidth is divided into a number of narrow bands via which the data is transmitted in parallel (Praveenkumar *et al*., 2012a-c). Each sub carrier has a unique frequency which is an integral multiple of cycles in symbol period and hence inhibits Inter Symbol Interference (ISI) (Kumar *et al*., 2011) and Inter Block Interference (IBI). During transmission, appending cyclic prefix greater than or equal to the channel order 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. Thus, OFDM which was principally developed for wireless communication, is widely preferred nowadays in Digital Audio Broadcasting (DAB), Digital Video Broadcasting (DVB), Asymmetric Digital Subscriber Line (ADSL), high speed internet and proposed to be used in 4G technology (Van Nee and Prasad, 2000).

The advent of wireless communication has revolutionized the world by overcoming the inconveniences caused by wired communication. Though there is no hassle 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 unusable. 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 used to achieve privacy data give clear information to the intruders that it is the message. To deny even that small amount of information technology was developed to embed a message or a cipher text inside an image or a multimedia file called steganography and the file is called stego-image (Amirtharajan and Rayappan, 2012a-c). In Petitcolas *et al*. (1999) released a survey on various information schemes (Thenmozhi *et al*., 2012). By the use of these techniques the intruder is denied the clear cut information of where the message is. The weakness of the human senses is exploited as a minute change due to the embedded message can't be detected. The technique has evolved over the years to a very high level.

The simplest LSB steganography technique (Amirtharajan and Rayappan, 2012a-d; Amirtharajan *et al*., 2012; Padmaa *et al*., 2011; Petitcolas *et al*., 1999), a spatial domain (Janakiraman *et a l*., 2012), changes the LSB of any of the layers of the RGB colour pattern of an image (Ahmed *et al*., 2010). The palette based technique hides the message in one of the colour palettes of the image.

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

Alternatively, the transform based techniques employ an alteration in the coefficients of the frequency domain representation of the image (Thanikaiselvan *et al*., 2011). The LSB, though primitive, is the easiest to implement as well as the easiest one that can be detected.

The steganalysis is a technique used to retrieve the information from the file. Cryptography and watermarking are two techniques that are very closely related to steganography (Amirtharajan and Rayappan, 2012a-d). While watermarking is another type of technology, cryptography uses keys for protecting the messages (Schneier, 2007). Watermarking is used to protect the ownership of a file or a message or simply to copyright a file (Karzenbeisser and Perircolas, 2000).The creator's name is embedded in the file that is undetectable by steganalysis to prevent any other else claim the ownership of that file. Cryptography generates keys that are known only to the sender and the receiver during each transmission to secure the message. Without the knowledge of these keys one cannot open the message.

After carefully reviewing the available literature, this paper proposes a secret data embedding scheme through convolutional encoders in OFDM. On the other side, i.e., the receiver, Artificial Neural Network (ANN) along with Viterbi decoders has been employed to improve the BER performance.

CONVOLUTIONAL ENCODER AND VITERBI DECODER

Convolutional encoders, a type of FEC, are often preferable to encode the digital signals as they are easy to decode. They process data sequentially unlike the block codes which process fixed block of data at a time. The convolutional encoder, a linear Finite State Machine (FSM), generates a code that depends on the input and output states of the FSM (Forney, 1970, 1971, 1973). Hence convolutional encoders are widely used. Even when the data is encoded before transmission, proper decoding of the signals is essential at the receiver. Of the many decoders available, viterbi decoder scores over the others. The efficiency of error detection increases with the constraint length of the convolutional encoder. But that requires complex decoding techniques. Viterbi decoder is very efficient in decoding convolutional codes of considerable length. Also, viterbi decoder adopts Maximum Likelihood (ML) decision rule that reduces the possibility of errors further. This makes the viterbi decoder the default choice for decoding convolutional codes.

Artificial neural network: The Artificial Neural Networks (ANN) is a technology that can be perceived as a network similar to the human nervous systems. The ANN consists of Artificial Neurons (AN) or network nodes analogous to the neurons in the actual nervous system. Each neuron does a simple task. But as a network the total functionality is very complex. It is a network where each AN does a task as dictated by the weight assigned to it (Hebb, 1949). This follows the divide and conquers approach as a complex task is subdivided into many simpler tasks, each done parallely. These weights influence the signals given as input to the ANs (Haykin, 1999). They can be positive or negative depending upon the desired functionality of the AN. Learning or training depends on a cost function which is a measure of how far the derived solution is away from the optimal solution. The categorization of the learning process is based on what the learning algorithm depends upon. ANN sometimes provides state of the art solutions in cognitive sciences and many other engineering and small networks. In many networks the onerous task of breaking a down a complex problem is achieved through ANN.

PROPOSED METHODOLOGY

In this study, the input bits are grouped in to parallel bits before encoding over convolutional encoders as shown in Fig. 1. Besides being simple to implement, these codes process the data based on both the past and present values. This kind of adaptive nature makes it more suitable for wireless communication where the noise signal can be utterly unpredictable. As any other communication systems, the wireless systems are also vulnerable to security issues. Any unauthorized user may access data, steal the privacy of legitimate users and can introduce an error in the transmitted data.

An attempt to introduce robust feature for securing the data has been made to design a secure wireless system unlike the other communication systems. Confidential data has been embedded in the redundant bits after encoding. Then the coded with confidential data has been passed over OFDM system. OFDM involves the use of subcarriers of bandwidth less than the channel coherence bandwidth leading to the sub channels experiencing a relatively flat fading. Each sub channel varies in its data rate and the power with which it is transmitted according to the demand.

OFDM facilitates overlapping of the signal spectrum ensuring the efficient use of channel bandwidth. This reduces the ISI between adjacent symbols. The implementation is made simple by the use of IFFT and FFT pairs. This leads to the use of a set of harmonically related functions as sub carriers. Further, a Cyclic Prefix (CP) of length greater or equal to the channel order is appended during transmission to avoid Inter Block Interference (IBI). At the receiver end perceptron neural network is employed to improve the BER. In ANN, the weights are updated in each iteration based on the learning algorithm. Then the datas are passed over OFDM

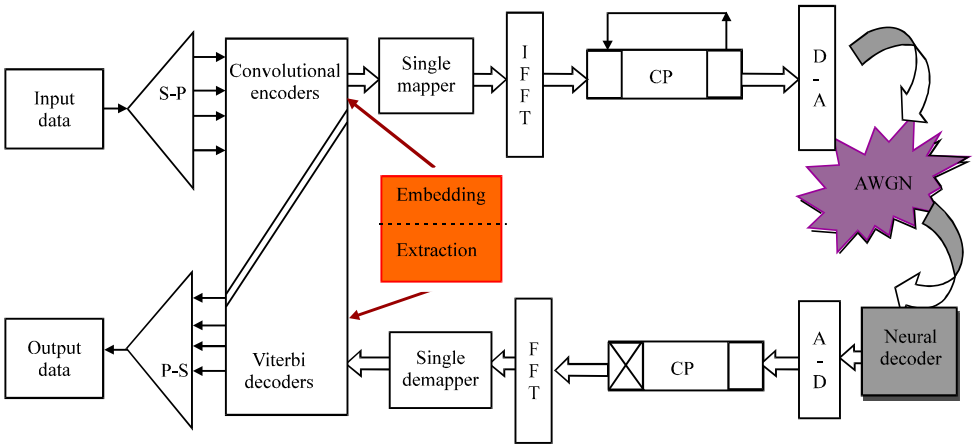

Fig. 1: Block diagram representation of proposed methodology

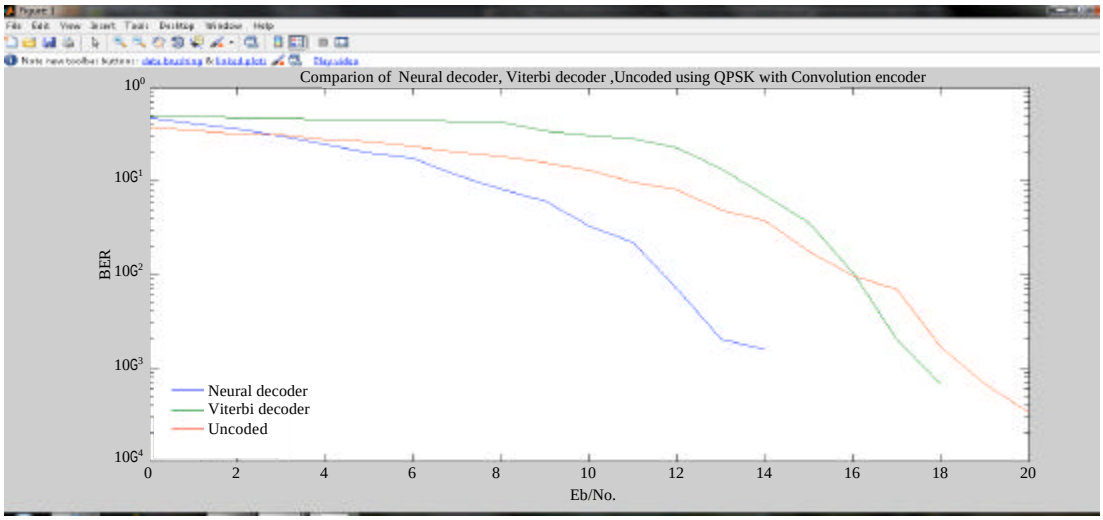

Fig. 2: Comparison of uncoded, viterbi decoder and viterbi decoder with neural network using QPSK modulation in OFDM

receiver and by knowing the exact key at the receiver side, confidential data extraction has been made then decode using viterbi decoder to produce the output bits.

RESULTS AND DISCUSSION

The comparison graph between Uncoded, Convolutional encoder with Viterbi decoder and Viterbi decoder with Neural network using QPSK in OFDM system and its performance plot using Neural networks are shown in Fig. 2 and 3, respectively. From the results, BER of Viterbi decoder with Neural network supersede the other two.

Uncoded, Convolutional encoder with viterbi decoder and Viterbi decoder with Neural network using QAM and its performance plot using Neural networks in OFDM system are compared and depicted in Fig. 4 and 5, respectively. From the Fig. 2 and 3, Viterbi decoder with Neural network is found to be superior compared to uncoded and Convoutional coded systems.

Performance plot of Neural network QPSK is better than QAM modulation in OFDM system. Comparison of BPSK, QPSK and QAM with data embedding in OFDM system is given in Fig. 6. From the results BPSK provides better BER even after embedding additional data.

Figure 7 and 8 shows the comparison of QPSK and QAM modulation schemes in OFDM system without encoding, Viterbi decoding and Viterbi decoding using Neural network with confidential data embedding, respectively.

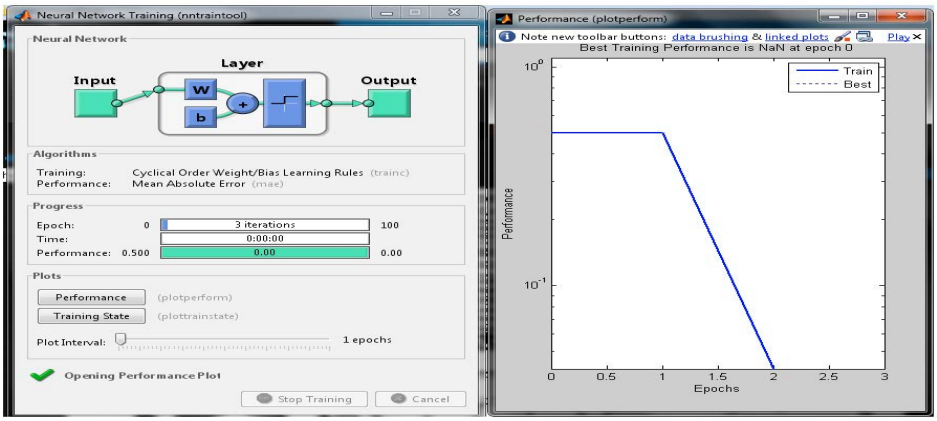

Fig. 3: Performance plot of neural network using QPSK modulation

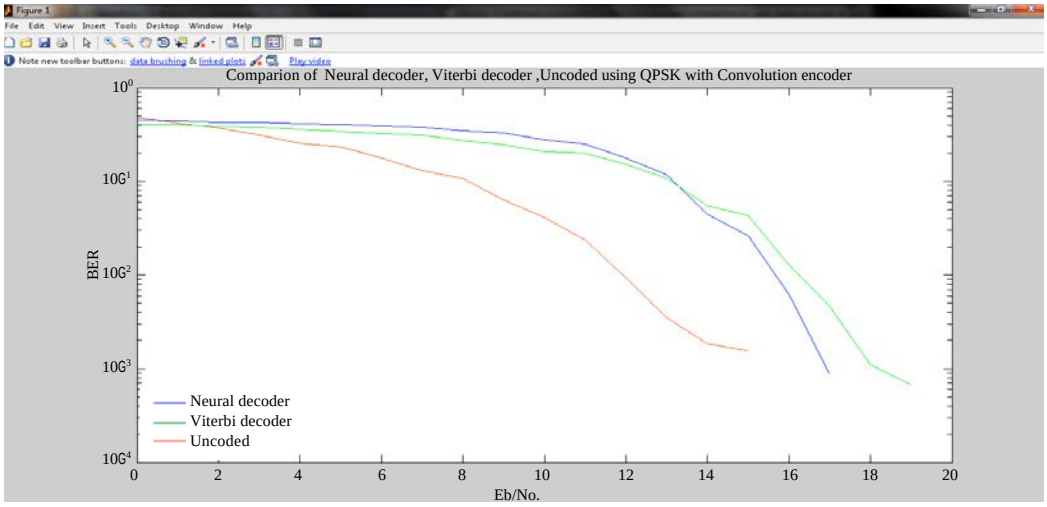

Fig. 4: Comparison of uncoded, viterbi decoder and viterbi decoder with Neural network using QAM modulation in OFDM

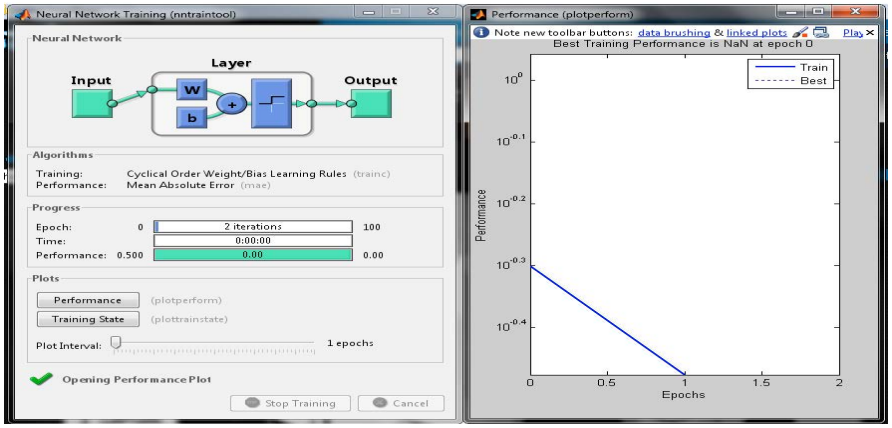

Fig. 5: Performance plot of neural network using QAM modulation

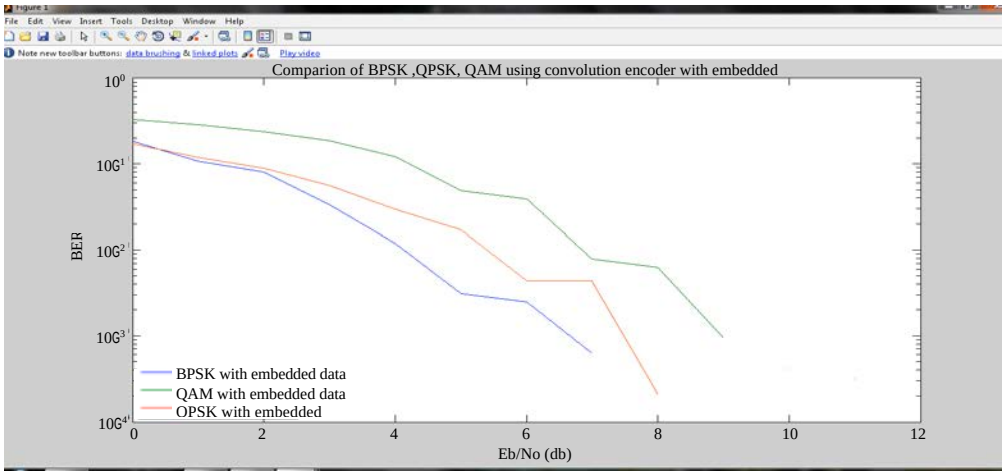

Fig. 6: Comparison of BPSK, QPSK and QAM with data embedding

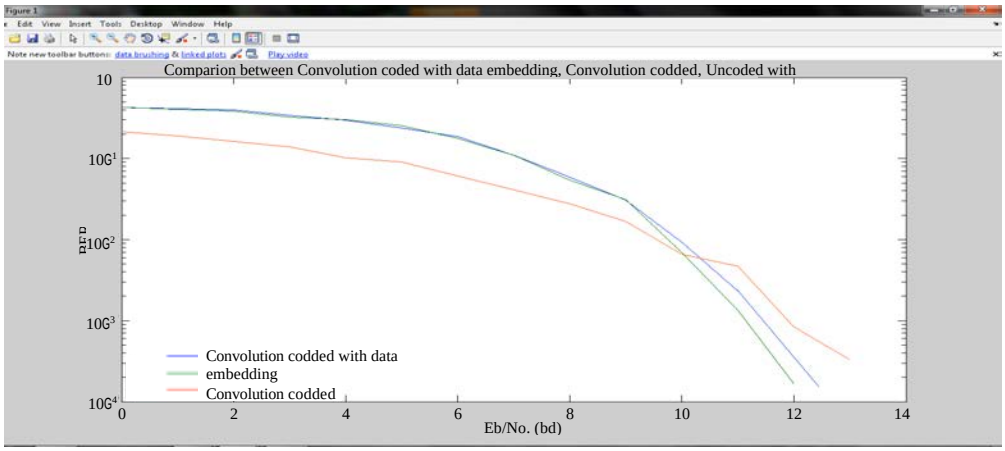

Fig. 7: Comparison of uncoded, convolution coded, convolution coded with data embedding using QPSK

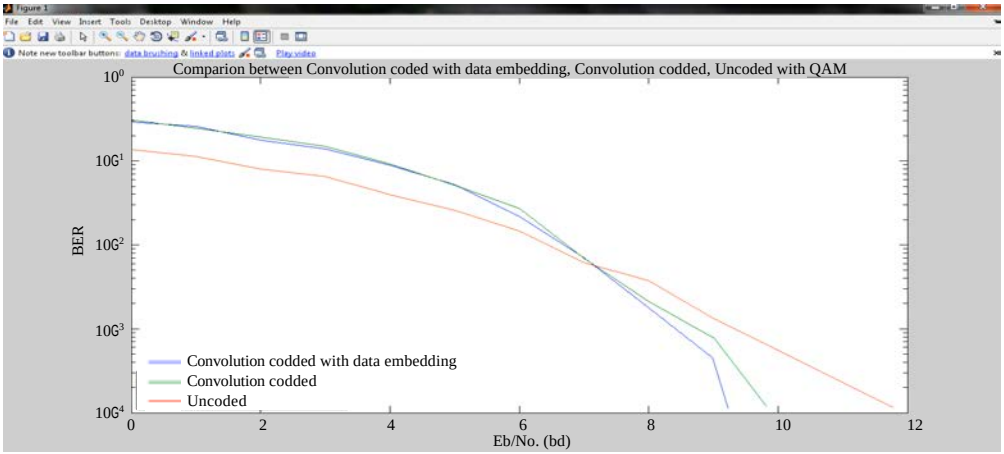

Fig.8: Comparison of uncoded, convolution coded, convolution coded with data embedding using QAM

From the results it is clear that BER of Viterbi decoder with Neural networks even after data embedding is comparatively low with respect to Viterbi decoded and uncoded systems.

CONCLUSION

In this study, confidential data has been embedded after encoding the serial input bits using convolutional encoder. Then its being modulated using signal mapper either by QPSK or QAM. Then the Modulated data has been transmitted over OFDM transmission. At the receiver end Perceptron neural network has been trained to improve the BER at the receiver before passing through OFDM receiver system. Then by knowing the confidential data at the Viterbi decoder, output can be decoded. From the results, it is seen that BER Viterbi decoder with neural network provides better performance than convolutional coded OFDM system which is in turn superior than un-coded system. Even embedding confidential data, Viterbi decoder with neural network using QPSK modulation provides better BER.

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.

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.

Forney, D.D. Jr., 1970. Convolutional codes I: Algebraic structure. IEEE Trans. Inform. Theory, 16: 720-738.

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

Forney, G.D. Jr., 1973. The viterbi algorithm. Proc. IEEE, 61: 268-278.

Haykin, S., 1999. Neural Networks a Comprehensive Foundation. Prentice-Hall, New Jersey.

Hebb, D.O., 1949. The Organization of Behavior: A Neuropsychological Theory. 1st Edn., Wiley, New York, ISBN: 0805843000.

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

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.

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

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, pp: 1-6.

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

Thanikaiselvan, V., S. Kumar, N. Neelima and R. Amirtharajan, 2011. Data battle on the digital field between horse cavalry and interlopers. J. Theor. Applied Inform. Technol., 29: 85-91.

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: 260.