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): 2061-2064, 2014
ISSN 1812-5638 / DOI: 10.3923/itj.2014.2061.2064

Spread and Hide-A Stego Transceiver

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: We live in an era where hacking and unauthorized access attempts to data are so common. There is a need to secure data before it is transmitted. Addition of overhead bits and modulation techniques decrease the capacity and increase the cost. Both the channel capacity and the cost to set up the communication system have to be optimal. So intimidating is a feature called multiple access used for this purpose. Multiple access also improves capacity by simultaneously transmitting large number of messages. There is very less or no interference between the signals since each of them is polarized orthogonally or encoded using different coding sequences or sent as bursts in different time slots. Particularly Code Division Multiple Access (CDMA) makes it more difficult for the hacker to access the transmitted data. If the message is thrown to all the users only the intended receiver has the same coding sequence to decode it. So, others can't access the message. Even if the message is detected, use of steganography makes it all the more difficult for the hacker to decode the message. This increases the security multifold. The aesthetic appeal of CDMA and steganography together has revolutionized the present world communication systems. In this study, the performance of CDMA is analysed by embedding confidential information at three levels namely after interleaving, spreading and modulator. The Bit Error Rate (BER) performance comparison graphs with and without information hiding at three levels are analysed using BPSK, QPSK and QAM schemes.

Key words: CDMA, steganography, BER, BPSK, QPSK, QAM

INTRODUCTION

The necessity of mankind to communicate to the farthest corners of the world led to the development of wireless networks (Kumar *et al*., 2011). These virtually shrunk the world and reduced the distance between the users. Owing to its perpetual demands, latest technologies are anticipated to gratify the escalating higher data rate (Van Nee and Prasad, 2000). The escalating demand for high speed, noise free wireless communication systems were primitively tackled by the use of Multiple Access techniques like FDMA and TDMA.

Code Division Multiple Access (CDMA) is one such technique ameliorated from multiple access (Baier, 1996) which facilitates overlap of signal without interference and more efficient use of bandwidth , ameliorated security are gratified by CDMA which uses PN sequences to modulate the data into the wide band signal which is larger than minimum bandwidth required for the transmission of the data. Spreading of signal is accomplished by the use of pseudo- random codes which make the signal scatter over the entire bandwidth and appears as noise to unintended users (Hara and Prasad, 1996). The technique of modulating all the data onto same frequency band with different coding sequence is called Spread Spectrum (SS)-CDMA. Here, frequency hopping mechanism is preferred over frequency spreading. This signal is available only to the user with particular coding sequence and as noise to the rest. The entropy and the orthogonality of the codes enhance security multifold and lessen the interference between data placing forth its efficiency. The receiver with same coding sequence can only decipher the data, thus increases the security. Also the cross correlation between any two codes is zero rending them orthogonal.

In direct sequence CDMA, the input multiplied with the PN code is spread over space making it immune to intended and unintended jamming. Thus the extensions of CDMA in communication technologies have devoted several vantages like greater capacity, improved security, privacy, rapid deployment, flexibility and asserting balance in phases of the signal (Amirtharajan and Balaguru, 2011). Amidst several merits, its efficiency is inhibited by the inability to generate perfect orthogonal codes for modulation which still remains a backbreaker.

In order to abnegate even this small amount of data leak, new techniques were developed to embed the

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

message or the cipher text into a multimedia file or a picture (Amirtharajan and Rayappan, 2012a, b, c). Here, the weakness of the human brain to discern minute changes is exploited. The pioneer was the simplest LSB steganography, in which LSB of RGB color pattern is altered. This technique being primitive is simple to be implemented and detected too. In the palette based technique, the data is obscured in any color palettes of the image whereas the co-efficients of the frequency domain of the signal are modified in transform based steganography (Amirtharajan *et al*., 2012d; Janakiraman *et al*., 2012). Steganalysis is used to stop the covert communication.

Cryptography and water marking are consanguineous to steganography. In cryptography, the keys are generated by the transmitter and are intimated only to intended receiver (Schneier, 2007). Only when the keys match, the data is candid. Water marking is exclusively used to uphold the ownership or the copyright of the file (Karzenbeisser and Perircolas, 2000). The proprietor's name is embedded in the file that is even undetectable by steganalysis. While so many techniques have been germinated to protect the data, several new algorithms have also developed to extract the covert file or delete the watermark.

A methodology for hiding data in images was proposed by Mahdi *et al*. (2012) and Marvel *et al*. (1998) has proposed a scheme for hiding authentication using Elliptic Curve Cryptography. Frequency domain based secret data embedding has been concentrated by Praveenkumar *et al*. (2012a, b, c). A survey on information hiding scheme has been proposed by Petitcolas *et al*. (1999). Cox *et al*. (1997) proposed an information hiding scheme using spread spectrum communication. Further a critical review on CDMA based image steganography has been proposed by Thenmozhi *et al*. (2012).

After carefully reviewing the available literature, this study proposes spread spectrum based steganography by embedding confidential data at three levels of the OFDM system and the analysis is done based on BER graph utilising BPSK, QPSK and QAM.

PROPOSED METHODOLOGY

CDMA uses orthogonal or PN codes which maintains cross correlation property between any two codes. Here the input data bits are multiplied by the PN sequence code which is unique to each user as shown in Fig. 1. Then they are modulated by signal mapper. Here the modulation scheme can be BPSK or QPSK or QAM. Since the data has been spreaded by PN sequence and modulated, it results in a wide band spectrum. Then its passed over AWGN channel. The same unique PN sequence is necessary at the demodulator to decode the data ouput bits otherwise receiver decodes noise signal.

Three levels of embedding has been done additional to CDMA encoding. The first level will be done after interleaving, then after spreading and the final embedding is done after modulation. IF any one of the key value is decoded wrongly, then at the receiver it results in noise signal rather than the desired output bits. The system is said to be efficient when the data is embedded with the least probability of alteration and remains concealed from unintended users.

RESULTS AND DISCUSSION

The comparison graphs between BPSK, QPSK and QAM before and after embedding confidential data after modulation is shown in Fig. 2. From the performance plot, there is no significant change has been analyzed before and after embedding the confidential data over all the

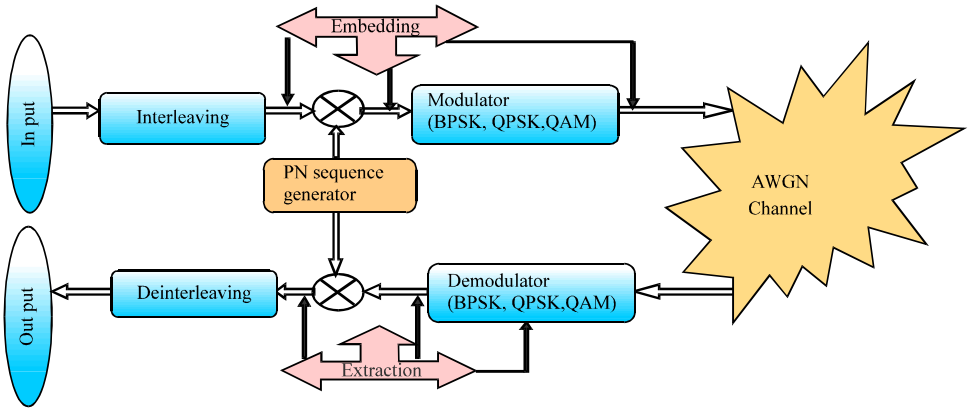

Fig. 1: Proposed methodology

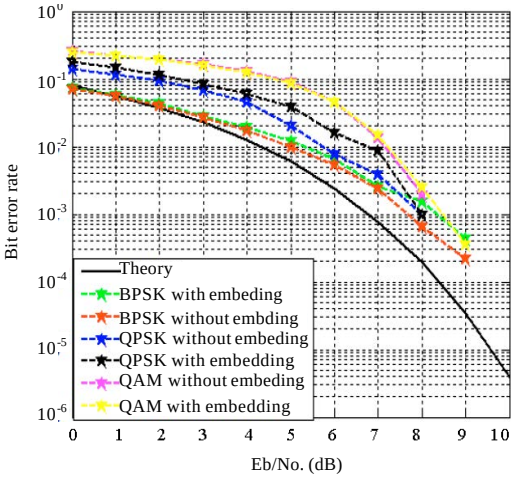

Fig. 2: Comparison between BPSK, QPSK and QAM before and after embedding, confidential data after modulation

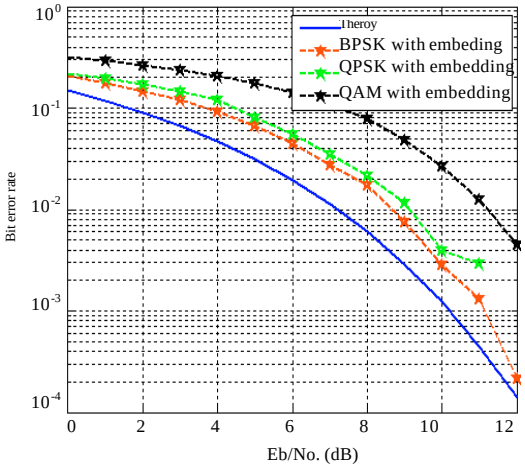

Fig. 4: Comparison between BPSK, QPSK and QAM after embedding confidential, data after interleaving and PN sequence generator

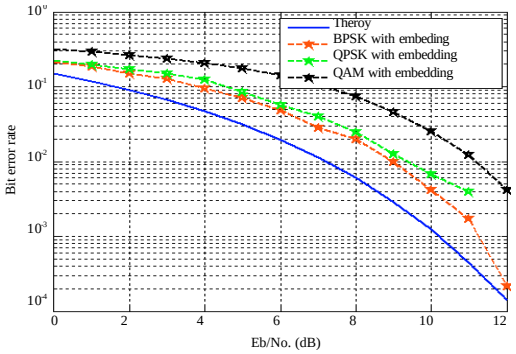

Fig. 3: Comparison between BPSK, QPSK and QAM after embedding confidential, data after spreading

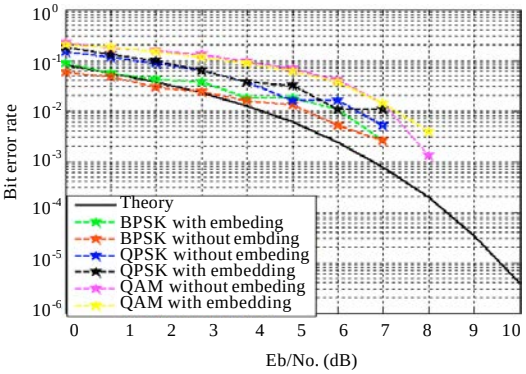

Fig. 5: Comparison between BPSK, QPSK and QAM before and after embedding, Confidential data after Interleaving, PN sequence generator and modulator

three modulation schemes. BER of BPSK is close to the theoretical computed one compared to other two modulation schemes.

BER comparison graphs between BPSK, QPSK and QAM after embedding additional data after spreading is shown in Fig. 3. From the results, after embedding BPSK and QPSK shows almost similar BER curves and they are close to the theoretical one as compared to QAM modulation scheme.

Figure 4 gives the comparison graph between BPSK, QPSK and QAM after embedding the confidential data after interleaving and PN sequence generator. BPSK provides better BER as compared to QPSK and QAM even after embedding additional data.

Figure 5 shows the overall BER comparison between BPSK, QPSK and QAM before and after embedding confidential data after Interleaving, PN sequence generator and modulator. From the results, in BPSK and QAM there is no significant changes before and after embedding confidential data as compared to QPSK.

CONCLUSION

In this proposed methodology, embedding confidential data has been done at three levels. First level of embedding is done after interleaver. Then the scrambled datas are multiplied by the unique PN sequence code assigned to each user to spread the input sequence. Then the second level of embedding has been carried out. Then they are being modulated by BPSK or QPSK or QAM. Then the third level of embedding has taken place after modulation. Then the datas are passed over AWGN channel. At the receiver end, same PN sequence is required t o decode the CDMA output data. Additionally

three keys are required to decode the data outputs, out of the three keys if any one of the key value is not known, then the receiver decodes noise rather than getting confidential output datas. Comparison graphs are plotted, based on the three levels of embedding. One is after interleaving (ie) before spreading, then the other one is after spreading and the final one is done after modulation. Confidential data embedding after spreading provides better results as compared with the theoretical one as analysed with the other two types of embedding. From the Bit Error Rate(BER) graphs, BPSK has better BER compared to other two modulation schemes. For transmitting large number of datas QAM provides improved BER at the cost of noise.

REFERENCES

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. and R.J.B. Balaguru, 2011. Covered CDMA multi-user writing on spatially divided image. Proceedings of the Wireless ViTAE Conference, February 28-March 3, 2011, IEEE, Chennai, India, pp: 1-5.

Baier, P.W., 1996. A critical review of CDMA. Porceedings of the IEEE 46th Vehicular Technology Conference on Mobile Technology for the Human Race, Volume 1, 28 April-1 May, 1996, Atlanta, GA., pp: 6-10.

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.

Hara, S. and R. Prasad, 1996. DS-CDMA, MC-CDMA and MT-CDMA for mobile multi-media communications. Proceedings of the IEEE 46th Vehicular Technology Conference on Mobile Technology for the Human Race, Volume 2, 28 April-1 May, 1996, Atlanta, GA., pp: 1106-1110.

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.

Mahdi, M.A., M.M. Abd-Eldayem, S.S. Elgamal and T.C. Wan, 2012. Security analysis and enhancement of authentication in cdma based on elliptic curve cryptography. Res. J. Inf. Technol., 4: 106-123.

Marvel, L.M., C.T. Retter and C.G. Jr. Boncelet, 1998. A methodology for data hiding using images. Proceedings of the IEEE on Military Communications Conference, October 18-21, 1998, Boston, MA , USA., pp: 1044-1047.

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.

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: 284.