Advances in Networks
2016; 4(2): 13-20
http://www.sciencepublishinggroup.com/j/net
doi: 10.11648/j.net.20160402.11
ISSN: 2326-9766 (Print); ISSN: 2326-9782 (Online)

Performance Analysis of Encrypted Color Image in a D-BLAST Aided LDPC Encoded MC-CDMA Wireless Communication System

Tonusree Saha[1], Md. Sarwar Hosain[1], Shafi Ahmed Istiaq[2]

[1]Department of Information and Communication Engineering, Pabna University of Science and Technology, Pabna, Bangladesh
[2]Department of Information and Communication Technology, Bogra Cantonment Public School and College, Bogra, Bangladesh

Email address:
tonusree.ice@gmail.com (T. Saha), sarwar@ice.pust.ac.bd (Md. S. Hosain), shafi.ice@gmail.com (S. A. Istiaq)

To cite this article:
Tonusree Saha, Md. Sarwar Hosain, Shafi Ahmed Istiaq. Performance Analysis of Encrypted Color Image in a D-BLAST Aided LDPC Encoded MC-CDMA Wireless Communication System. *Advances in Networks.* Vol. 4, No. 2, 2016, pp. 13-20.
doi: 10.11648/j.net.20160402.11

Received: October 6, 2016; **Accepted**: November 2, 2016; **Published**: December 16, 2016

Abstract: In this paper, a comprehensive MATLAB simulation based study has been presented for the performance evaluation of LDPC encoded MC-CDMA wireless communication system. The investigated system implements various signal detection techniques such as Minimum mean square error (MMSE), Zero-Forcing (ZF), Zero-Forcing successive interference cancellation (ZF-SIC) Minimum mean square error successive interference cancellation (MMSE-SIC) under different digital modulation schemes (QPSK, DPSK, QAM). Simulation results show that the system shows quite **s**atisfactory and robust performance under scenario of MMSC-SIC signal detection and QAM digital modulation schemes.

Keywords: MC-CDMA, MIMO, LDPC, Signal Detection Scheme, Signal to Noise Ratio (SNR), D-BLAST

1. Introduction

Progressive involvement in technology development is vital for a government if it hopes to keep its own country competitive in the rapidly changing field of wireless personal communications. Wireless communications is enjoying its fastest growth period in history, due to enabling technologies which permit wide spread deployment. Multi-Carrier Code Division Multiple Access (MC-CDMA) is a multiple access scheme used in OFDM-based telecommunication systems, allowing the system to support multiple users at the same time [1]. The basic MC-CDMA signal is generated by a serial concatenation of classical DS-CDMA and OFDM. MC-CDMA can handle *N* simultaneous users with good BER, using standard receiver techniques. This system has been adopted as the uplink physical layer radio access technique for the 3GPP Long Term Evolution (LTE) and 4G LTE-Advanced. The main advantages of the MC-CDMA system are that improve the reliability and performance of wireless radio links and the signal offered to the receiver contains not only a direct line-of-sight radio wave, but also a large number of reflected radio waves [2].

Multiple-input multiple-output, or MIMO, is a radio communications technology or RF technology, is used by Wi-Fi, LTE; Long Term Evolution, and many other radio, wireless and RF technologies to provide increased link capacity and spectral efficiency combined with improved link reliability using what were previously seen as interference paths [3]. Such technologies incorporate different types of multi-antenna techniques such as Alamouti space-time coding for transmit diversity, Eigen beam forming spatial multiplexing, BLAST spatial multiplexing architectures, Conventional beam and null forming and Conventional receive diversity. Under BLAST spatial multiplexing(SM) architectures, three Bell Laboratory layered space-time (BLAST) SM techniques have been known as: Vertical BLAST (V-BLAST), Horizontal BLAST (H-BLAST) and Diagonal BLAST (D-BLAST) [4], [5]. The present study investigates the performance of D-BLAST architecture with 4 x 4 antenna configuration for a LDPC encoded MC-CDMA wireless communication system on secure color image transmission.

2. Signal Processing and Detection Techniques

For signal detection if transmitted signal X=[x_1, x_2, x_3, x4]^T, received signal Y=[y_1,y_2 y_3,y_4]^T, white Gaussian noise N= [n_1, n_2, n_3, n_4]^T with variance σ_n^2 and the channel matrix H=[h_1 h_2 h_3 h_4] have been considered. The signal model in terms of transmitted and received signals, Noise and channel coefficients can be written as:

$$Y = HX + N \tag{1}$$

As the interference signals from other transmitting antennas are minimized to detect the desired signal, the detected desired signal from the transmitting antenna withinverting channel effect by a weight matrix W is given by

$$\tilde{X} = [\tilde{x}_1, \tilde{x}_2, \tilde{x}_3, \tilde{x}_4]^T = WY \tag{2}$$

A. Minimum Mean Square Error (MMSE)

In Minimum mean square error (MMSE) scheme, the MMSE weight matrix is given by

$$W_{MMSC} = (H^H H + {\sigma_n}^2 I)^{-1} H^H \tag{3}$$

and the detected desired signal from the transmitting antenna is given by

$$\tilde{X}_{MMSC} = W_{MMSC} Y \tag{4}$$

Let us now try to understand the math for extracting the two symbols which interfered with each other. In the first time slot, the received signal on the first receive antenna is,

$$y_1 = h_{1,1}x_1 + h_{1,2}x_2 + n_1 = \begin{bmatrix} h_{1,1} h_{1,2} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} + n_1 \tag{5}$$

The received signal on the second receive antenna is,

$$y_2 = h_{2,1}x_1 + h_{2,2}x_2 + n_2 = \begin{bmatrix} h_{2,1} h_{2,2} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} + n_2 \tag{6}$$

We assume that the receiver knows$h_{1,1}, h_{1,2}, h_{2,1}$ and $h_{2,2}$. The receiver also knows above equation can be represented in matrix notation as follows: y_1 and y_2. For convenience, the above equation can be represented in matrix notation as follows:

$$\begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} h_{1,1} & h_{1,2} \\ h_{2,1} & h_{2,2} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} + \begin{bmatrix} n_1 \\ n_2 \end{bmatrix} \tag{7}$$

Equivalently,

$$y = Hs + n \tag{8}$$

The Minimum Mean Square Error **(**MMSE**)** approach tries to find a coefficient W which minimizes the criterion,

$$E\{[Wy - x][Wy - x]^H\} \tag{9}$$

Solving,

$$\mathrm{W} = [\mathrm{H^H H} + \mathrm{N_0 I}]^{-1} \mathrm{H^H} \tag{10}$$

When comparing to the equation in Zero Forcing equalizer, apart from the $\mathrm{N_0 I}$ term both the equations are comparable. Infact, when the noise term is zero, the MMS Equalizer reduces to Zero Forcing equalizer.

B. Zero-Forcing (ZF)

In Zero-Forcing (ZF) scheme, the ZF weight matrix is given by

$$W_{ZF} = (H^H H)^{-1} H^H \tag{11}$$

and the detected desired signal from the transmitting antenna is given by

$$\tilde{X}_{ZF} = W_{ZF} Y \tag{12}$$

Let us now try to understand the math for extracting the two symbols which interfered with each other. In the first time slot, the received signal on the first receive antenna is,

$$y_1 = h_{1,1}x_1 + h_{1,2}x_2 + n_1 = \begin{bmatrix} h_{1,1} h_{1,2} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} + n_1 \tag{13}$$

The received signal on the second receive antenna is

$$y_2 = h_{2,1}x_1 + h_{2,2}x_2 + n_2 = \begin{bmatrix} h_{2,1} h_{2,2} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} + n_2 \tag{14}$$

We assume that the receiver knows$h_{1,1}$, $h_{1,2}, h_{2,1}$ and $h_{2,2}$. The receiver also knows above equation can be represented in matrix notation as follows: y_1 and y_2. The unknown s are$x_1$and x_2. For convenience, the above equation can be represented in matrix notation as follows:

$$\begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} h_{1,1} & h_{1,2} \\ h_{2,1} & h_{2,2} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} + \begin{bmatrix} n_1 \\ n_2 \end{bmatrix} \tag{15}$$

Equivalently

$$y = Hs + n \tag{16}$$

To solve for x, we know that we need to find a matrix W,which satisfiesWH=1. TheZero Forcing (ZF) linear detector for meeting this constraint is given by

$$W = (H^H H)^{-1} H^H \tag{17}$$

H^H is a Hermitian matrix which is the conjugate transpose of matrix H

This matrix is also known as the pseudo inverse for a general m x nmatrix

$$H^H H = \begin{bmatrix} h_{1,1}^* & h_{2,1}^* \\ h_{1,2}^* & h_{2,2}^* \end{bmatrix} \begin{bmatrix} h_{1,1} & h_{1,2} \\ h_{2,1} & h_{2,2} \end{bmatrix}$$

$$= \begin{bmatrix} |h_{1,1}|^2 + |h_{2,1}|^2 & h_{1,1}^* h_{1,2} + h_{2,1}^* h_{2,2} \\ h_{1,2}^* h_{1,} + h_{2,2}^* h_{2,1} & |h_{1,2}|^2 + |h_{2,2}|^2 \end{bmatrix} \tag{18}$$

C. Zero-Forcing Successive Interference Cancellation (ZF-SIC)

In ZF-SIC channel equalization scheme with 4× 4 antenna configuration, the channel matrix H undergoes QR factorization as

$$H = QR = Q\begin{bmatrix} R_{1,1} & R_{1,2} & R_{1,3} & R_{1,4} \\ 0 & R_{2,2} & R_{2,3} & R_{2,4} \\ 0 & 0 & R_{3,3} & R_{3,4} \\ 0 & 0 & 0 & R_{4,4} \end{bmatrix} \quad (19)$$

where, Q and R are the unitary and upper triangular matrix respectively. Equation (1) can be rewritten on multiplying$Q^H$by as

$$X = Q^H Y = RX + Q^H N \quad (20)$$

where, $Q^H$is a zero-mean complex Gaussian random vector. Since $Q^H N$ and N havethe same statistical properties, $Q^H N$ can be used to denote N. We get Equation (21)

$$X = RX + N$$

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = \begin{bmatrix} r_{1,1} & r_{1,2} & r_{1,3} & r_{1,4} \\ 0 & r_{2,2} & r_{2,3} & r_{2,4} \\ 0 & 0 & r_{3,3} & r_{3,4} \\ 0 & 0 & 0 & r_{4,4} \end{bmatrix} \begin{bmatrix} \tilde{x}_1 \\ \tilde{x}_2 \\ \tilde{x}_3 \\ \tilde{x}_4 \end{bmatrix} + \begin{bmatrix} n_1 \\ n_2 \\ n_3 \\ n_4 \end{bmatrix} \quad (21)$$

the detected desired signal $\tilde{X}_S$ from the four transmitting antennas can written on neglecting noise term from Equation (21)as

$$\tilde{x}_4 = \frac{x_4}{r_{4,4}}$$

$$\tilde{x}_3 = \frac{(x_3 - r_{3,4}\tilde{x}_4)}{r_{3,3}} \quad (22)$$

$$\tilde{x}_2 = \frac{(x_2 - r_{2,3}\tilde{x}_3 - r_{2,4}\tilde{x}_4)}{r_{2,2}}$$

$$\tilde{x}_1 = \frac{(x_1 - r_{1,2}\tilde{x}_2 - r_{1,3}\tilde{x}_3 - r_{1,4}\tilde{x}_4)}{r_{1,1}}$$

D. Minimum Mean Square Error Successive Interference Cancellation (MMSE-SIC)

The received signal, channel matrix and noise are extendedas

$$H_{ex} = \left[H^T \sqrt{\frac{{\sigma_n}^2}{{\sigma_n}^2}} I \right]^T$$

$$Y_{ex} = [Y^T \quad O^T] \text{ and}$$

$$N_{ex} = \left[N^T - \sqrt{\frac{{\sigma_n}^2}{{\sigma_n}^2}} X^T \right]^T \quad (23)$$

Where, is $\sqrt{\frac{{\sigma_n}^2}{{\sigma_n}^2}}$ the ratio of average noise power to average signal power (1/SNR). On QR factorization of extended channel H_{ex}matrix, we get

$$H_{ex} = Q_{ex} \cdot R_{ex} \quad (24)$$

Where, Q_{ex} and R_{ex} represent a unitary matrix and an upper triangular matrix respectively. We assume that Y, H, N, Q and R are replaced by Y_{ex} , H_{ex} , Q_{ex} , and R_{ex} respectively and correspondingly the resulting system takes the following form

$$X_{ex} = {Q_{ex}}^H \cdot Y_{ex} = R_{ex} \cdot X_S + {Q_{ex}}^H \cdot N_{ex} \quad (25)$$

Neglecting term ${Q_{ex}}^H \cdot N_{ex}$ from Equation (25), the detected desired signal $\tilde{X}_{S_{ex}}$ from the four transmitting antennas can written as

$$\tilde{x}_{ex4} = \frac{x_{ex4}}{r_{ex4,4}}$$

$$\tilde{x}_{ex3} = \frac{(x_{ex3} - r_{ex3,4}\tilde{x}_{ex4})}{r_{ex3,3}}$$

$$\tilde{x}_{ex2} = \frac{(x_{ex2} - r_{ex2,3}\tilde{x}_{ex3} - r_{ex2,4}\tilde{x}_{ex4})}{r_{ex2,2}} \quad (26)$$

$$\tilde{x}_{ex1} = \frac{(x_{ex1} - r_{ex1,2}\tilde{x}_{ex2} - r_{ex1,3}\tilde{x}_{ex3} - r_{ex1,4}\tilde{x}_{ex4})}{r_{ex1,1}}$$

Using identical formulas presented in Equation (22), the transmitted signals are detected [6], [7].

3. Description of the Simulation Model

A simulated single-user 4 x 4 D-BLAST spatially multiplexed LDPC encoded MC-CDMA Wireless Communication System as depicted in Figure 1 utilizes various signal detection schemes. In such a communication system, a color image is encrypted with Chaos-Based Image Encryption Scheme [8].

A RGB image png format is kept in C drive of the computer. The resolution of the image is of 96 pixels (width) × 96 pixels (height). The selected image are processed in a MIMO MC-CDMA system depicted in Figure 1. The captured color image are converted into their respective three Red, Green and Blue components with each component is of96 pixels ×96pixels in size. The encrypted data are channel encoded using low density parity check coding technique [9],[10]and interleaved for minimization of burst errors. The interleaved bits are digitally modulated using various types of digital modulations and spatially multiplexed using D-BLAST scheme to produce four independent data streams. Each data stream are serial to parallel converted, DFT-spreader/preceded and subsequently subcarriers are mapped prior to OFDM modulation through implementation as an inverse Fast Fourier transform (IFFT) on a block of information symbols followed by an analog-to-digital converter (ADC). To mitigate the effects of inter-symbol interference (ISI) caused by channel time spread, each block of IFFT coefficients is typically preceded by a cyclic prefix.. The modulated complex symbols are parallel to serial converted and transmitted. In receiving section, the transmitted signals are detected and processed cyclic prefix removal, serial to parallel conversion, OFDM demodulation, subcarrier de-mapping, DFT-de-spreaded/decoded, parallel to serial conversion and subsequently spatially de-multiplexed under D-BLAST scheme. The de-multiplexed

data are digitally demodulated, de-interleaved, channel decoded and decrypted to recover the transmitted color image[11], [12].

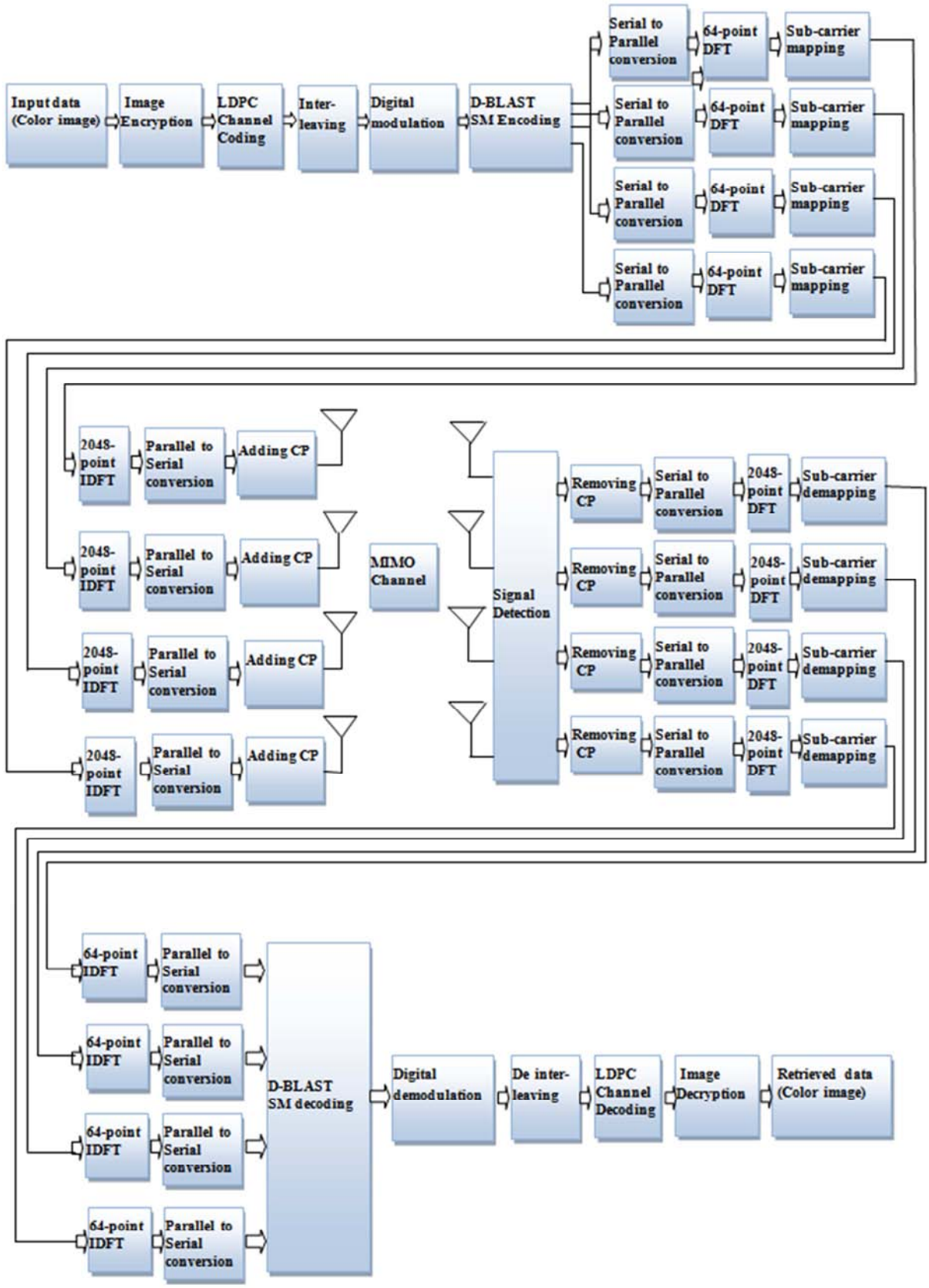

Figure 1. *Conceptual Block diagram of D-BLAST aided LDPC encoded MC-CDMA Wireless Communication System.*

4. Result and Discussion

This section presents all of the results obtained by the computer simulation program written in Matlab following the analytical approach of a wireless communication system considering the following simulation parameters shown below in the Table 1. The results are represented in terms of signal to noise ratio (SNR) and the bit error rate (BER) for practical values of system parameters. The graphical illustrations presented in Figure 2 and Figure 8 show system performance comparison with implementation of Minimum Mean Square Error (MMSE), Zero-Forcing (ZF), Mean Square Error Successive Interference Cancellation (MMSE-SIC) and Zero-Forcing Successive Interference Cancellation(ZF-SIC) based channel equalization schemes under various low order digital modulations. In all cases, the system outperforms in QAM and shows worst performance in DPSK digital modulation. The BER performance difference is quite obvious in lower SNR areas and the system's BER declines with increase in SNR values. In Figure 2, the BER values in case of QAM and DPSK are 0.1418 and 0.3098 for a 3 dB SNR value that is indicative of achievable system performance by 3.40 dBfor QAM modulated MC-CDMA employing Minimum Mean Square Error(MMSE) channel equalization scheme. Figure 3 illustrates the achievable performance of QAM-modulated system under deployment of Zero-Forcing(ZF), the system achieves a gain of 2.14dB at SNR value of 3 dB.(BER values: 0.2764 and 0.4526 in case of QAM and DPSK. In Figure 4, it is noticeable that for a typically assumed SNR value of 3 dB, the BER values are 0.0956 and 0.3588 in case of QAM and DPSK digital modulations and the system achieves a gain of 5.74 dB in QAM as compared to DPSK under deployment of Minimum Mean Square Error Successive Interference Cancellation (MMSE-SIC). Figure 5 present that the system achieves a gain of 1.87dB at SNR value of 3 dB for BER values: 0.2399 and 0.3691 in case of QAM and DPSK. From Figure 6 to Figure 8 shows performance of QAM, QPSK and DPSK modulated system under deployment of for equalization techniques. Here it is observable that for SNR value of 3 dB, the system gain is 6.20dB, 5.38 dB and 1.14dB using QAM, QPSK and DPSK modulation schemes respectively with implementation of different channel equalization technique and it is seen that MMSE-SIC provides best result among four equalization techniques with three digital modulation techniques individually. Figure 9 shows pictorial views of transmitted, encrypted and retrieved images with a typically assumed SNR value of 10dB and estimated bit error rate zero, image retrieval with transmitted image encryption are quite satisfactory.

Table 1. *Summary of the simulated model parameters.*

Data type	Color image: 96 × 96× 3 pixels
Modulation Scheme	QPSK,BPSK,QAM, DBPSK
Channel coding	½.-rated irregular LDPC
No of complex modulated symbols in OFDM block	2048
No of complex modulated symbols in DFT-spreading/precoding	64
Size of parity-check matrix used in LDPC coding	64 × 128
Length of Cyclic prefixing in number of complex symbols	205
SNR	0-10 dB
LDPC decoding Algorithm	Log Domain Sum-Product
Signal detection	(MMSE, ZF, ZF-SIC and MMSE-SIC)
Channel	AWGN and Rayleigh
Spreading Code	Walsh-Hadamard

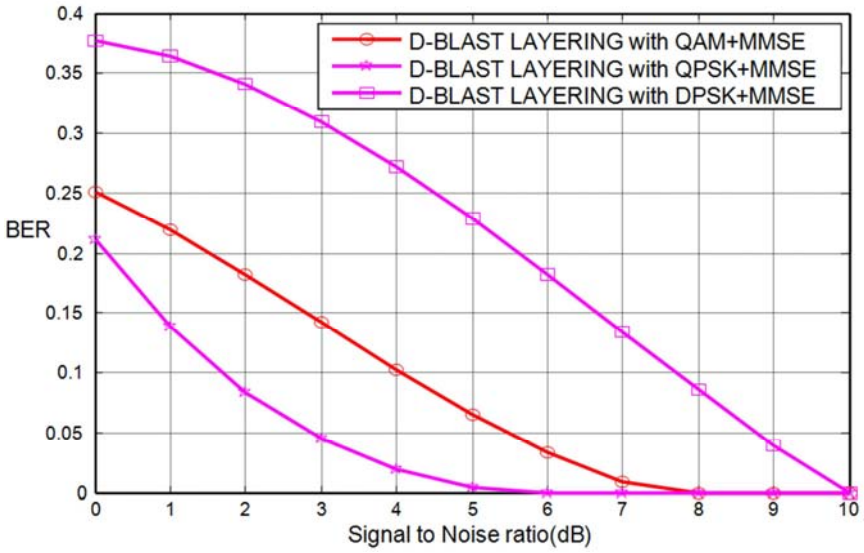

Figure 2. *BER evaluation in a channel equalization based MC–CDMA wireless communication system under implementation of different digital modulation schemes and MMSE channel equalization scheme.*

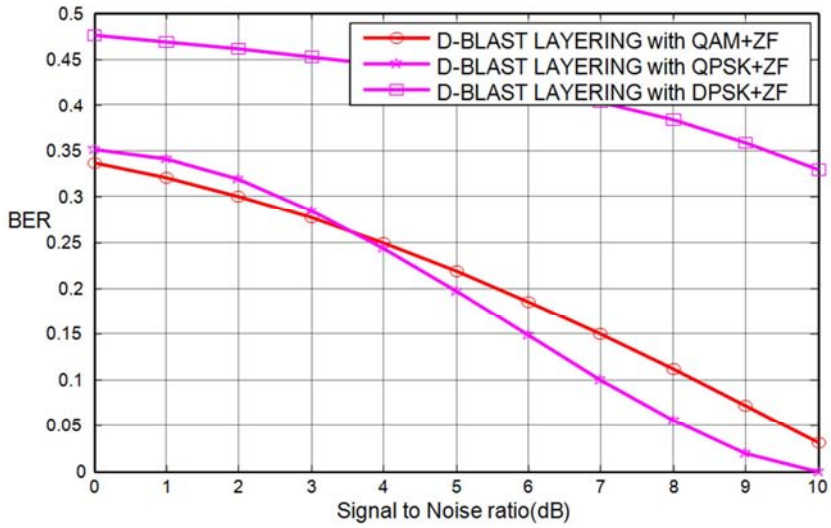

Figure 3. *BER evaluation in a channel equalization based MC–CDMA wireless communication system under implementation of different digital modulation schemes and ZF channel equalization scheme.*

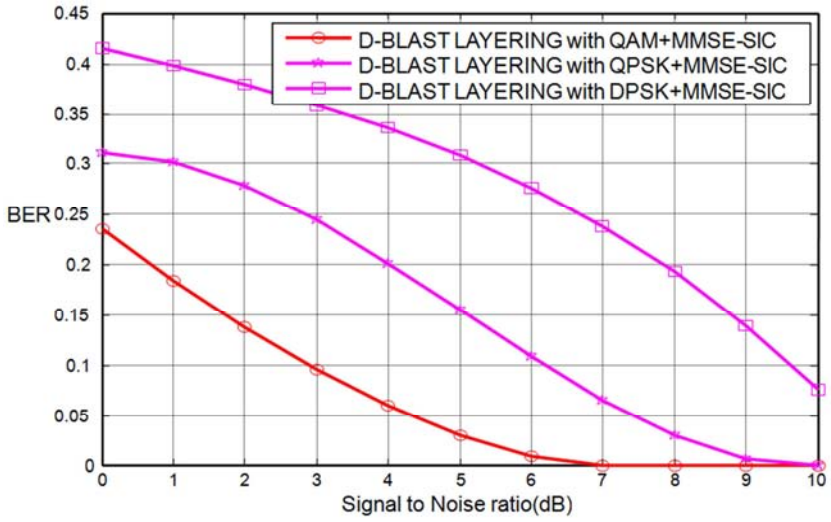

Figure 4. *BER evaluation in a channel equalization based MC–CDMA wireless communication system under implementation of different digital modulation schemes and MMSE-SICchannel equalization scheme.*

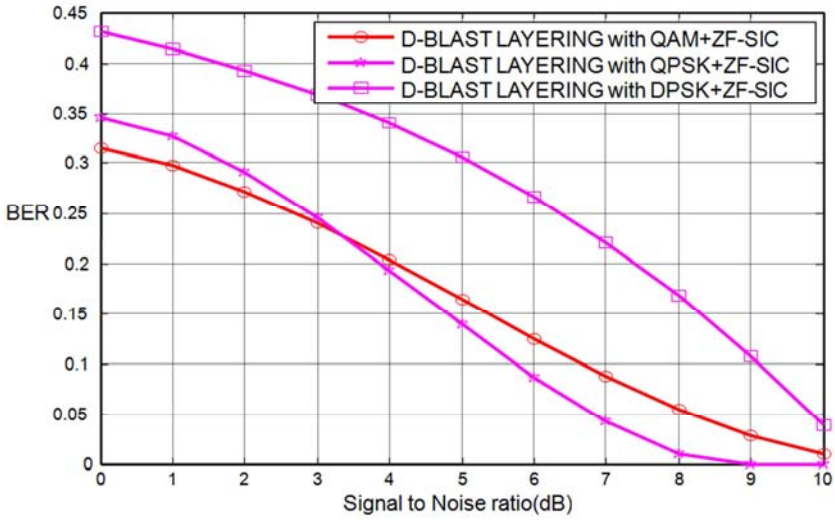

Figure 5. *BER evaluation in a channel equalization based MC–CDMA wireless communication system under implementation of different digital modulation schemes and ZF-SIC channel equalization scheme.*

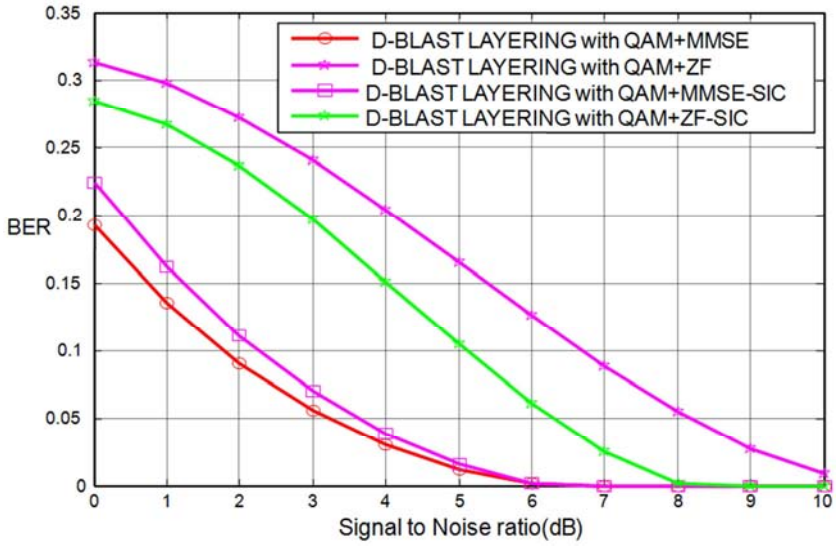

Figure 6. *BER evaluation in a channel equalization based MC–CDMA wireless communication system under implementation of QAM modulation schemes and different channel equalization scheme.*

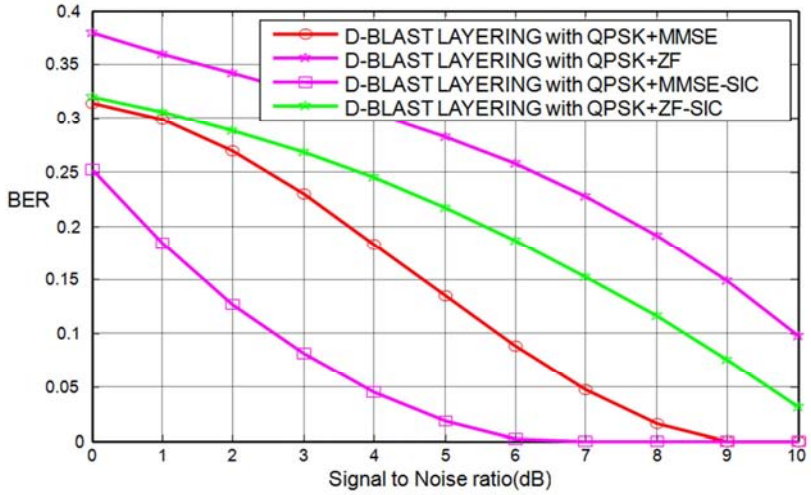

Figure 7. *BER evaluation in a channel equalization based MC–CDMA wireless communication system under implementation of QPSK modulation schemes and different channel equalization scheme.*

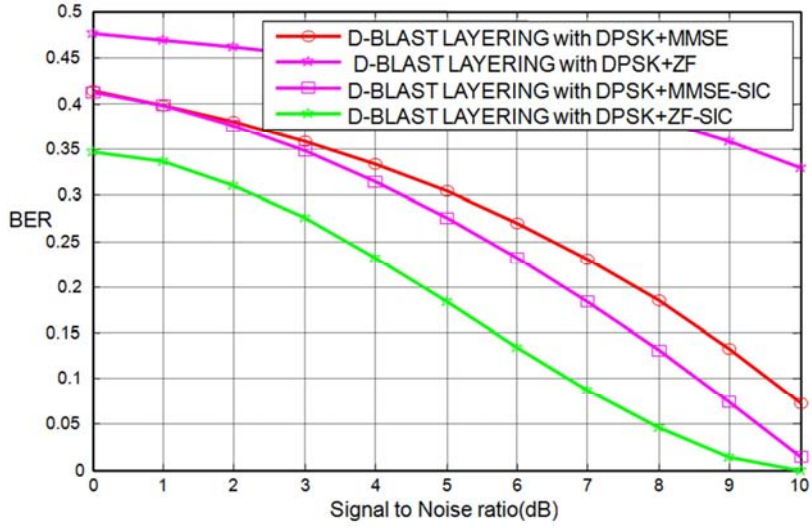

Figure 8. *BER evaluation in a channel equalization based MC–CDMA wireless communication system under implementation of DPSK modulation schemes and different channel equalization scheme.*

Figure 9. *Pictorial views of Transmitted, Encrypted and Retrieved image in a simulated D-BLAST aided LDPC encoded MC-CDMA Wireless Communication system under implementation of different digital modulation schemes and MMSE-SIC channel equalization scheme.*

5. Conclusions

In this work, simulation results concerning the adaptation of various equalization techniques in a LDPC encoded MC-CDMA wireless communication system has been presented. A range of system performance results highlights the impact of various signal detection techniques under different digital modulations scheme. A comparison on the MMSE, ZF, MMSE-SIC and ZF-SIC has been made based on their bit error rates and signal-to-noise ratio. In the context of system performance, it can be concluded that the implementation of QAM digital modulation technique with deployment of MMSE-SIC channel equalization technique provides satisfactory result for such a LDPC encoded MC-CDMA wireless communication system as compared with MMSE, ZF,and ZF-SIC for such a LDPC encoded MC-CDMA wireless communication system.

References

[1] Lohninger, Hans (2005-12-17). "Direct Sequence CDMA Simulation".

[2] Viterbi A. J., CDMA: Principles of Spread Spectrum Communication. Reading: Addison-Wesley, 1995.

[3] Jerry R. Hampton, "Introduction to MIMO Communications", Cambridge University Press, United Kingdom, 2014

[4] D. Gesbert et al., “From Theory to Practise: An Overview of MIMO Space-Time Coded Wireless Systems”, *IEEE Journal on Selected Areas in Communication*, Vol. 21, No. 3, pp 281-302, April 2003.

[5] Md. SarwarHosain, ShaikhEnayetUllah and RubaiyatYasmin, "Performance analysis of D-BLAST aided Turbo Encoded SC-FDMA wireless communication system", International Journal of Scientific & Engineering Research, vol. 5, Issue: 7, pp.744-749, 2014.

[6] V. Jagan Naveen, K. Murali Krishna, K. RajaRajeswari,” Performance analysis of equalization techniques for MIMO systemsin wireless communication” International Journal of Smart HomeVol.4, No.4, October, 2010.

[7] Md. SarwarHosain, ShaikhEnayetUllah and RubaiyatYasmin, " Quality Assessment of Encrypted Color Image in a D-BLAST aided LDPC encoded SC-FDMA Wireless Communication System”, International Journal of Emerging Technologies in Computational and Applied Sciences, 12(1), March-may, 2015, pp. 58-64.

[8] N. A. Al-Romema1, A. S. Mashat and I. Al Bidewi, "New Chaos-Based Image Encryption Scheme for RGB Components of Color Image", Computer Science and Engineering, vol. 2, no. 5, pp. 77-85, 2012.

[9] Amin Shokrollahi*LDPC Codes: An Introduction* Digital Fountain, Inc.39141 Civic Center Drive, Fremont, CA 94538 April 2, 2003.

[10] Bagawan Sewu Nugroho, https://sites.google.com/site/bsnugroho/ldpc.

[11] MahmudulHaqueKafi, Md. SarwarHosain and Sk. Shifatul Islam,” Impact of MGSTC BLAST spatial multiplexing scheme on performance assessment of MCCDMA wireless communication system”, International Journal of Emerging Technologies in Computational and Applied Sciences, 12(1), March-May 2015, pp. 08-14.

[12] Theodore S. Rappaport, ―Wireless Communication Principles and Practice‖, Second Edition, Pearson Education, Inc, 2004, ISBN 81-7808-648-4.