Performance Analysis of SC-FDMA Wireless Communication System with Implementation of Chaos-Based Image Encryption Scheme

Joarder Jafor Sadique and Shaikh Enayet Ullah

Department of Applied Physics and Electronic Engineering
Rajshahi University, Rajshahi-6205, Bangladesh

joarderjafor@yahoo.com, enayet67@yahoo.com

Abstract

In this paper, a comprehensive BER performance simulative study has been made on secure color image transmission in a SC-FDMA wireless communication system. The system implements a modified form of Chaos-based image encryption scheme under utilization of three channel equalization techniques (MMSE, ZF and Q-Less QR Decomposition) and three digital modulation schemes (QPSK, DQPSK and QAM).In comparative study, it is noticeable from simulation results that the ½-rated convolutionally encoded system combined with both transmit and receive diversity in Rayleigh multipath fading channel outperforms in QAM and ZF schemes.

Key words: *Single-carrier frequency-division multiple access (SC-FDMA), Minimum Mean Squared Error (MMSE), Zero-forcing (ZF),Q-Less QR decomposition, Rayleigh Fading channel, BER*

1. Introduction

Wireless high-rate data transmission scheme supported long term evolution (LTE) communication system defined by the 3rd generation partnership project (3GPP) deploys multiple-input multiple-output (MIMO) technology with the single carrier-frequency division multiple access (SC-FDMA) radio interface technology. The LTE system with chosen SC-FDMA as a promising uplink transmission technique achieves peak data rates of 75 Mbps. The time-division duplex long-term evolutions (TDD-LTE) system can provide high data rate up to 100 Mbps with a bandwidth of 20 MHz to meet up requirements of high-speed mobile users. Due to deployment of SC-FDMA in TDD-LTE system, a peak to- average power ratio (PAPR) is reduced significantly. The LTE-Advanced, which is an evolution of the LTE, supports single user spatial multiplexing of up to four antennas in theuplink targeted to achieve peak data rates of 500 Mbps [1, 2].

The SC-FDMA is a DFT Spread- OFDM (DFTS-OFDM) technique deployed in LTE system to enhance the power utilization efficiency of the power-constrained mobile transmitterbatteries and to prolong their lifetimes. The SC-FDMA can provide larger cell (macrocell) coverage. It is expected that such SC-FDMA scheme will be effectively implemented in LTE –advanced systems although such LTE-Advanced MSs will use hybrid circuits. The SC-FDMA has better performance with low-order digital modulations.

It is known from present research study that Carrier aggregation has been established as one of the most important technologies to ensure the success of 4G technologies. The Carrier aggregation technique makes efficient use of spectrum already deployed and additionally provides required support for the resource allocation in new frequency bands. In case of uplink transmission, one of the problems caused by carrier aggregation is the loss of efficiency defined by cubic metric parameter for the power amplifier. This is the disadvantage of SC-FDMA scheme for uplink data transmission with Carrier aggregation [3, 4].

The present study focuses on the transmission of secure color image transmission in a MIMO SC-FDMA wireless communication system using a modified form of chaos based image encryption technique.

2. Mathematical Theory

2.1 Chaos based Image Encryption Scheme

We assume a RGB color image, P containing M x N x 3 array of color pixels. The range of the color pixel value is [0, 255] for each of the three M x N sized color image components (Red, Green and Blue), P_r, P_g and P_b. Another synthetically generated M x N x 3 sized matrix, K is used as a key and its three M x N sized matrix components are Kr, Kg and Kb respectively. Each element of matrix component has value in the range [0, 255]. Each pixel/element of color image component/matrix component is represented by 8 bits [0/1].

A diffusion operation is performed to produce cipher image C with components as [5]

$$\begin{aligned} C_r &= P_r \oplus K_r \\ C_g &= P_g \oplus K_g \\ C_b &= P_b \oplus K_b \end{aligned} \tag{1}$$

Where $\oplus$ is the bite level XOR operation between each pixel and element of color image and matrix components.The binary to decimally converted values of C_r, C_g and C_b form the chaos based encrypted image. To retrieve the transmitted color image P, reverse diffusion operation is performed to decrypt the color images with components as:

$$\begin{aligned} P_{r\,(retrieved)} &= C_r \oplus K_r \\ P_{g\,(retrieved)} &= C_g \oplus K_g \\ P_{b\,(retrieved)} &= C_b \oplus K_b \end{aligned} \tag{2}$$

2.2 Channel Equalization Schemes

In the 2 x 2 MIMO SC FDMA system, the transmitted and received signals are represented by $\mathbf{x=[x_1, x_2]^T}$ and $\mathbf{y= [y_1, y2]^T}$ respectively. If $\mathbf{n}= [n_1, n_{2R}]^T$ denotes the white Gaussian noise with a variance$\boldsymbol{\sigma_n^2}$and the channel matrix is represented by$\mathbf{H}$= [h1 h_2**],** we can write

$$y = Hx + n = h_1 x_1 + h_2 x_2 \tag{3}$$

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

$$\tilde{\mathbf{x}} = [\tilde{\mathbf{x}}_1, \tilde{\mathbf{x}}_2]^{\mathbf{T}} = \mathbf{Wy} \tag{4}$$

2.2.1. Minimum Mean Square Error (MMSE) Scheme: In Minimum mean square error (MMSE) scheme, the MMSE weight matrix is given by

$$\mathbf{W_{MMSE}} = (\mathbf{H^H H} + \sigma_{\mathbf{n}}{}^2 \mathbf{I})^{-1} \mathbf{H^H} \tag{5}$$

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

$$\tilde{\mathbf{x}}_{\mathbf{MMSE}} = \mathbf{W_{MMSE}} \mathbf{y} \tag{6}$$

2.2.2. Zero-Forcing (ZF) Scheme: In Zero-Forcing (ZF) scheme, the ZF weight matrix is given by

$$\mathbf{W_{ZF}} = (\mathbf{H^H H})^{-1} \mathbf{H^H} \tag{7}$$

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

$$\tilde{\mathbf{x}}_{\mathbf{ZF}} = \mathbf{W_{ZF}} \mathbf{y} \tag{8}$$

2.2.3. Q-Less QR Decomposition Scheme: With Q-less QR Decomposition scheme, the detected signal $\tilde{\mathbf{x}}$ can be found based on the least squares approximate solution to $\tilde{\mathbf{H}} * \tilde{\mathbf{x}} = \tilde{\mathbf{y}}$ where, $\tilde{\mathbf{H}}$ and $\tilde{\mathbf{y}}$ are the channel matrix and received signal respectively. From $\tilde{\mathbf{H}}$ channel matrix, an upper triangular matrix $\tilde{\mathbf{R}}$ of the same dimension as $\tilde{\mathbf{H}}$ is estimated and using the following steps, the detected desired signal $\tilde{\mathbf{x}}$ is computed [6-8].

$$\begin{aligned}
\tilde{\mathbf{x}} &= \tilde{\mathbf{R}} \backslash (\tilde{\mathbf{R}}^{\mathbf{H}} \backslash (\tilde{\mathbf{H}}^{\mathbf{H}} * \tilde{\mathbf{y}})) \\
\tilde{\mathbf{r}} &= \tilde{\mathbf{y}} - \tilde{\mathbf{H}} * \tilde{\mathbf{x}} \\
\tilde{\mathbf{e}} &= \tilde{\mathbf{R}} \backslash (\tilde{\mathbf{R}}^{\mathbf{H}} \backslash (\tilde{\mathbf{H}}^{\mathbf{H}} * \tilde{\mathbf{r}})) \\
\tilde{\mathbf{x}} &= \tilde{\mathbf{x}} + \tilde{\mathbf{e}}
\end{aligned} \tag{9}$$

3. System model

The block diagram of the simulated FEC encoded MIMO SC-FDMA wireless communication system is shown in Figure 1. A RGB color image in JPEG format is encrypted using chaos based image encryption technique and channel encoded using convolutional coding scheme **.**The channel encoded bits are interleaved for the minimization of burst error. The interleaved and channel encoded bits are digitally modulated using QPSK, DQPSK and QAM [9]. The digitally modulated symbols are then applied to 64-point FFT block and subsequently sent into STBC encoder. The output of the STBC encoder are fed into two channels for executing various steps (subcarrier mapping, 1024 point IFFT and Cyclic prefixing) in OFDM section. At the receiver side, the transmitted signals are detected using channel equalization schemes. The detected signals are fed into OFDM section to execute various tasks (CP removing, 1024 point FFT and subcarrier de-mapping). The signals are fed into STBC decoder and the decoded signal is further processed for digital demodulation, de-interleaving, channel decoding and decryption. Eventually, the transmitted color image is retrieved [10].

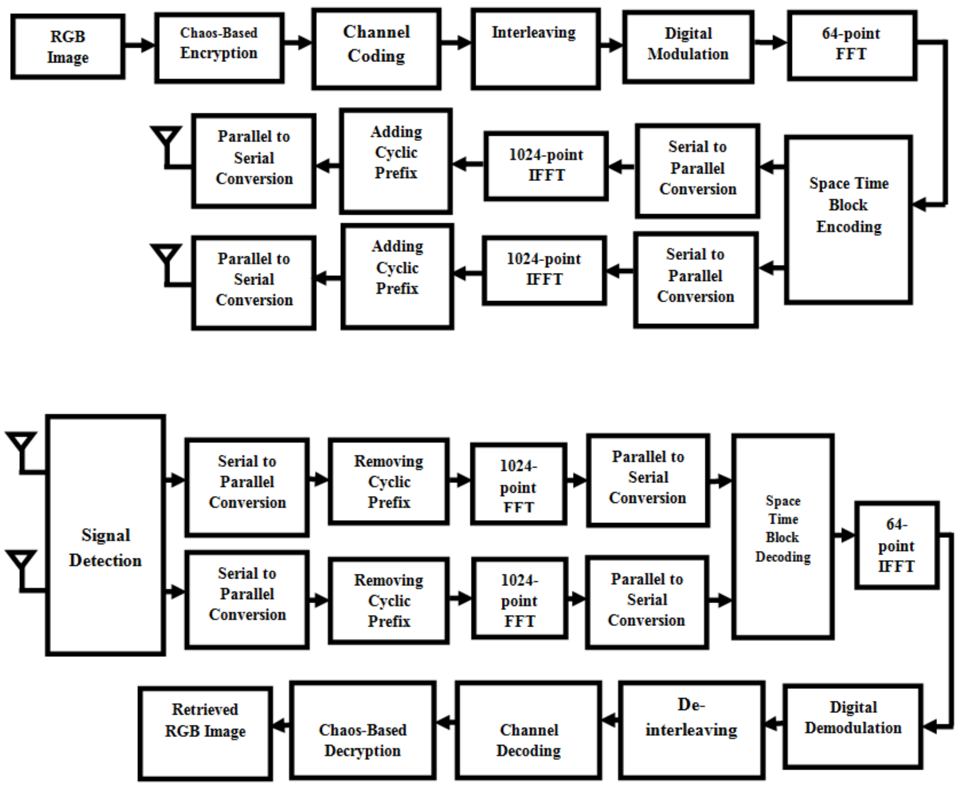

Figure 1. Block diagram of FEC encoded MIMO SC-FDMA wireless communication

4. Results and Discussion

We have investigated BER performance of the SC-FDMA aided wireless communication system with simulation parameters tabulated in Table 1.

Table 1. Summary of the simulated model parameters

Data type	Color image (96 × 96× 3 pixels)
Antenna configuration	2-by-2
Channel Coding /Decoding	½-rated Convolutional
DataModulation	DQPSK, QPSK and QAM
FFT/IFFT block size	1024
CP length	103
No of symbols per block	64

Channel Equalization Scheme	Mean square error (MMSE), Zero-forcing (ZF) and Q-less QR decomposition
Channel	AWGN and Rayleigh fading
Cryptographic algorithm	Chaos based image encryption
Signal to noise ratio, SNR	0 to10 dB

Firstly, it is noticeable that the BER curves depicted in Figure 2 through Figure-4 are clearly indicative of showing distinguishable difference between system performance under various channel equalization and digital modulation schemes. In all cases, the simulated system shows worst performance in DQPSK digital modulation.

In Figure 2, it is observable that the MIMO FEC encoded SC FDMA system exhibits better bit-error rate (BER) performance with deployment of MMSE channel equalization in QPSK digital modulation as compared to QAM and DQPSK. At 1×10^{-1} BER, a system performance gain of 4 dB is achieved in QPSK as compared to DQPSK. Additionally, a system performance improvement of 4.89 dB has been achieved in QPSK on comparison with DQPSK (BER values: 0.1619 and 0.4988) at a low SNR value of 1 dB. It is noticeable that at low SNR value region, noise enhancement effect is significant causing reduction of system performance. In Figure 3, the estimated BER with ZF equalization at a low SNR value (1 dB) for QAM and DQPSK are found to have values of 0.0645 and 0.4366 which implies a system performance enhancement of 8.31dB. On critical examination of graphical illustrations presented in Figure 2 and Figure 3, it is observable that the noise enhancement effect is significant in MMSE as compared to ZF at low SNR value area for QAM and QPSK digital modulations. In Figure 4, it is quite obvious that the system shows almost identical and worst performance over a wide area of SNR values with DQPSK and Q-Less QR decomposition based channel equalization schemes. The system shows quite satisfactory performance in QAM digital modulation and a performance improved of 7.83 dB is provided as compared to DQPSK for BER values of 0.0823 and 0.4994 at 1dB SNR value.

In Figure 5, it has been confirmed that the encrypted image is highly uncorrelated with the original image. At a comparatively low SNR value of 6dB, the retrieved image has a significant resemblance with the original transmitted image. In Figure 6, the histograms of RGB to Gray converted transmitted, encrypted and retrieved color images at various SNR values for the simulated MIMO SC FDMA wireless communication system have been presented. The x-axis of each image histogram comprises of the intensity values (0-255) and the height of the bar displays the number of pixels with that intensity value. As evident from the original image, it is noticeable that the majority of the pixels have their grayscale values ranging from 0-10,130-140 and 250-255. In case of encrypted image, majority of the pixels have their grayscale values ranging from 75-175. On critical inspection, additionally it is found that the histogram for the Gray converted encrypted image is highly uncorrelated with other images. With increase in SNR value, the histogram is getting similarity with that of the original image.

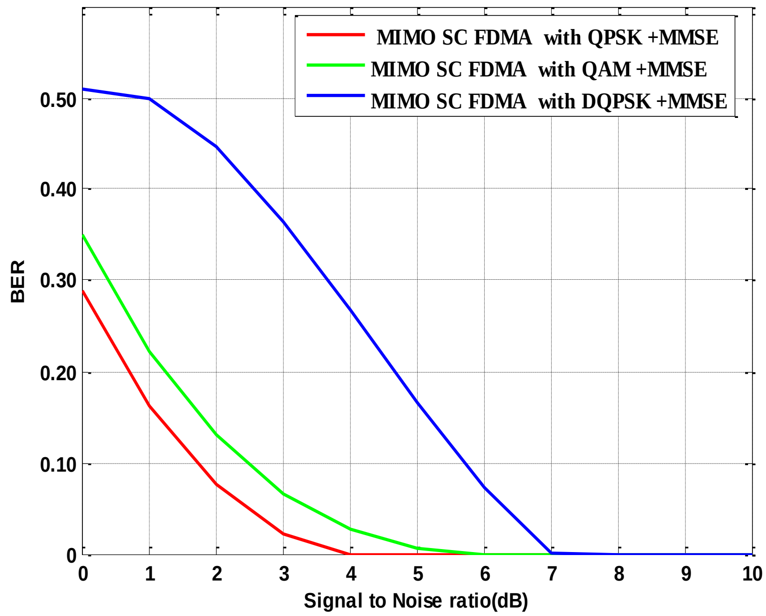

Figure 2. BER performance of channel encoded MMSE equalization based MIMO SC-FDMA wireless communication system under employment of various digital modulation schemes

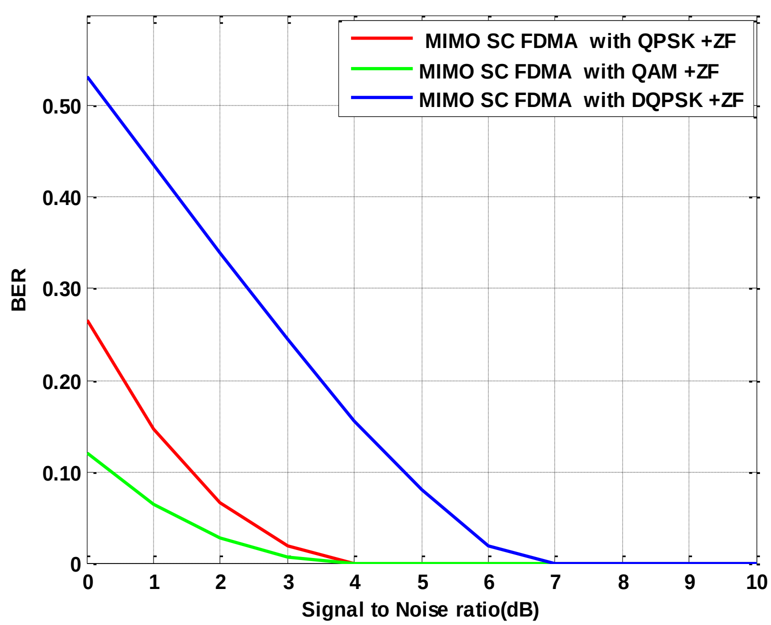

Figure 3. BER performance of channel encoded ZF equalization based MIMO SC-FDMA wireless communication system under employment of various digital modulation schemes

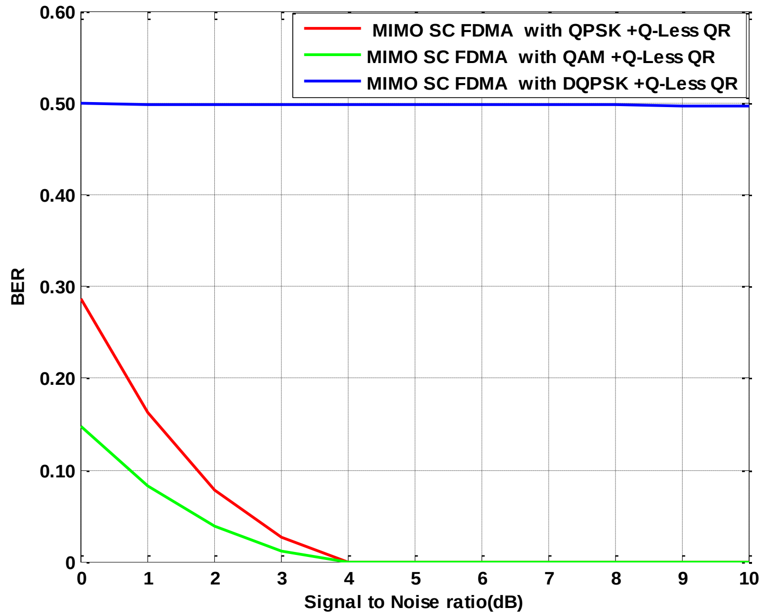

Figure 4. BER performance of channel encoded Q-Less QR Decomposition aided equalization based MIMO SC-FDMA wireless communication system under employment of various digital modulation schemes

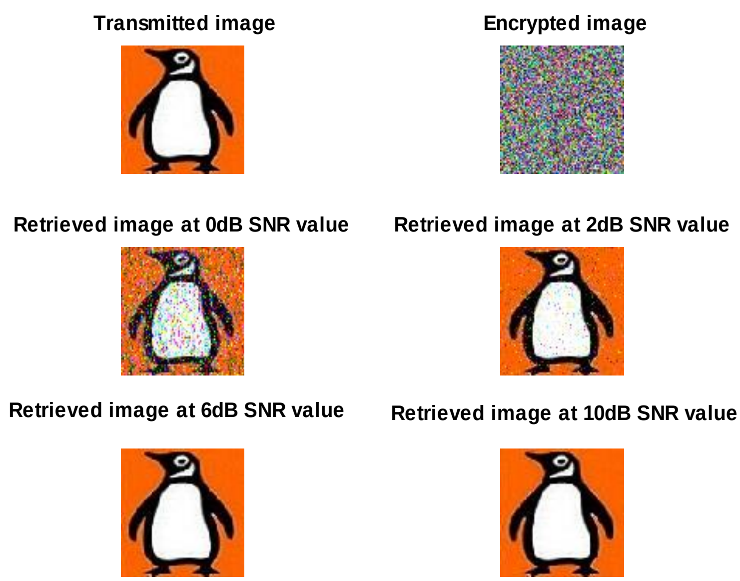

Figure 5. Transmitted, Encrypted and Retrieved color images at various SNR Values in a MIMO SC-FDMA wireless communication system

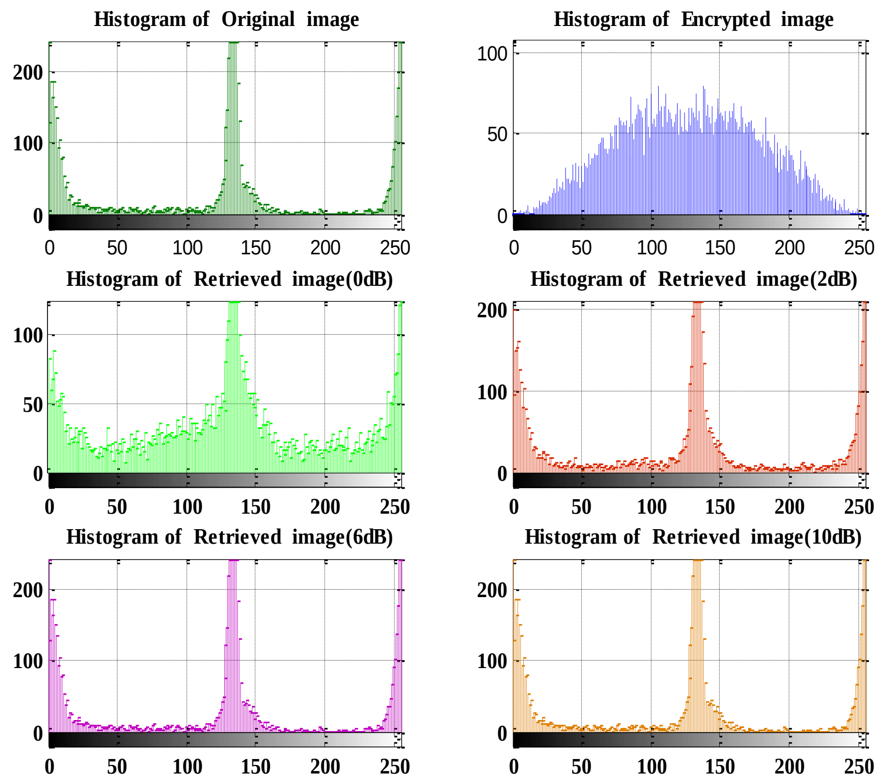

Figure 6. Histogram of Gray converted Transmitted, Encrypted and Retrieved Color images at various SNR values in a MIMO SC-FDMA wireless communication system

5. Conclusion

In this paper, simulation results for a convolutionally encoded MIMO SC-FDMA wireless communication system on encrypted color image transmission have been presented. In the context of system performance, it can be concluded that the implementation of QAM digital modulation technique with ZF channel equalization provides satisfactory result for convolutionally encoded MIMO SC- FDMA wireless communication system.

References

[1] L. Yang, G. Ren, B. Yang and Z. Qiu, "Fast Time-Varying Channel Estimation Technique for LTE Uplink in HST Environment", IEEE Transactions on Vehicular Technology, vol. 61, no. 9, **(2012)**, pp. 4009-4019.
[2] K. Neshatpour, M. Mahdavi and M. Shabany, "A Low-Complexity High-throughput ASIC for the SCFDMA MIMO Detectors", **(2010)**, pp. 3065-3068.
[3] A. -E. M. Taha and H. S. Hassanein and N. A. Ali, "LTE, LTE-advanced and WiMAX towards IMT-advanced Networks", John Wiley and Sons Limited, United Kingdom, **(2012)**.
[4] G. de la Roche, A. Glazunov and B. Allen, "LTE-advanced and next generation wireless networks Channel modelling and propagation", John Wiley and Sons Limited, United Kingdom, **(2013)**.
[5] N. A. Al-Romema1, A. S. Mashat and I. AlBidewi, "New Chaos-Based Image Encryption Scheme for RGB Components of Color Image", Computer Science and Engineering, vol. 2, no. 5, **(2012)**, pp. 77-85.
[6] Y. S. Cho, J. Kim, W. Y. Yang and C. G. Kang, "MIMO-OFDM Wireless Communications with Matlab", John Wiley and Sons (Asia) Pte Limited, Singapore, **(2012)**.

[7] S. T. Karris, "Numerical Analysis Using MATLAB and Spreadsheets", Second Edition, Orchard Publications California, USA, **(2004)**.
[8] J. J. Sadique and S. E. Ullah, "Encrypted Data Transmission in STBC Transmission Scheme Based Turbo Encoded SC- FDMA Wireless Communication System, International Journal of Applied Science and Technology (IJAST**)**, vol. 50, **(2013)**, pp. 1-10, Australia.
[9] T. S. Rappaport, "Wireless communications: Principles and Practices", Second Edition, Prentice Hall Inc., New Jersey, USA, **(2004)**.
[10] H. G. Myung and D. J. Goodman, "Single CarrierFDMA - A New Air Interface forLong Term Evolution", John Wiley and Sons, Limited, United Kingdom, **(2008)**.

Authors

Joarder Jafor Sadique received his B.Sc. (Hons.) and M.Sc. degree both in Applied Physics and Electronic Engineering department from University of Rajshahi, Bangladesh in 2010 and 2011 respectively. During his post graduate study, he has completed a research work on MIMO SC-FDMA Wireless Communication System. His research interest includes Channel Equalization, Radio Interface technologies (OFDMA and SC-FDMA) and Antenna Diversity. Concurrently, He is working as a Lecturer in the Department of Electrical and Electronic Engineering (EEE), University of Information Technology and Sciences (UITS), Dhaka, Bangladesh.

Shaikh Enayet Ullah is a Professor of the Department of Applied Physics and Electronic Engineering, Faculty of Engineering, University of Rajshahi, Rajshahi, Bangladesh. He received his B.Sc. (Hons.) and M.Sc degree both in Applied Physics and Electronics from University of Rajshahi in 1983 and 1985 respectively. He received his PhD degree in Physics from Jahangirnagar University, Bangladesh in 2000. He has earned US equivalent Bachelor's and Master's degree in Physics and Electronics and PhD degree in Physics from a regionally accredited institution of USA from New York based World Education Services on the basis of his previously received degrees and academic activities (Teaching and Research), in 2003. He worked as a Professor and Chairman (on deputation) in the Department of Information and Communication Engineering, University of Rajshahi from 2009 to 2012. He has published more than 60 articles in multidisciplinary fields. His main research interests include Cooperative communications, MIMO-OFDM, WiMAX, Cognitive radio and LTE radio interface technologies.