Global Journal of Computer Science and Technology: A
Hardware & Computation
Volume 17 Issue 1 Version 1.0 Year 2017
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Encrypted Color Image Transmission in LDPC Encoded MIMO Wireless Communication System with implementation of MP-WFRFT Based

By Laila Naznin, Mohammad Reaz Hossain & Shaikh Enayet Ullah

Rajshahi University

Abstract- This paper emphasizes on comprehensive study for the performance evaluation of LDPC encoded MIMO wireless communication system under implementation of MP-WFRFT based physical layer security scheme. The 4 $\times$4 multi antenna configured simulated system under investigation incorporates LDPC channel coding scheme and various types of modulation (QPSK, DQPSK, and 4-QAM) and signal detection (ZF, MMSE, ZF-SIC and MMSE-SIC) techniques. On considering transmission of encrypted color image in a hostile fading channel, it is noticeable from MATLAB based simulation study that the LDPC channel encoded system is very much robust and effective in retrieving color image under utilization of MMSE-SIC signal detection and 4-QAM digital modulation techniques.

Keywords: 4-weighted fractional fourier transform, MIMO, LDPC, SNR.

GJCST-A Classification: C.2.1, E.3

ENCRYPTEDCOLORIMAGETRANSMISSIONINLDPCENCODEDMIMOWIRELESSCOMMUNICATIONSYSTEMWITHIMPLEMENTATIONOFMPWFRFTBASED

Encrypted Color Image Transmission in LDPC Encoded MIMO Wireless Communication System with implementation of MP-WFRFT Based

Laila Naznin[α], Mohammad Reaz Hossain[σ] & Shaikh Enayet Ullah[ρ]

Abstract- This paper emphasizes on comprehensive study for the performance evaluation of LDPC encoded MIMO wireless communication system under implementation of MP-WFRFT based physical layer security scheme. The 4 ×4 multi antenna configured simulated system under investigation incorporates LDPC channel coding scheme and various types of modulation (QPSK, DQPSK, and 4-QAM) and signal detection (ZF, MMSE, ZF-SIC and MMSE-SIC) techniques. On considering transmission of encrypted color image in a hostile fading channel, it is noticeable from MATLAB based simulation study that the LDPC channel encoded system is very much robust and effective in retrieving color image under utilization of MMSE-SIC signal detection and 4-QAM digital modulation techniques.

Keywords: 4-weighted fractional fourier transform, MIMO, LDPC, SNR.

I. Introduction

Our in perspective of fulfillment of ever-increasing demand for authenticated, confidential and secret data transmission in presence of malicious eavesdroppers over existing and future generation wireless networks, a considerable amount of research is being going on physical layer security which offers an information-theoretic level of secrecy with implementation of various improved cryptographic algorithms under exploitation of important characteristics of wireless channel such as fading, interference and noise. During the past two decades, Multiple-input multiple-output (MIMO) wireless systems have been studied extensively with quantification of their potential gains in throughput, diversity and range. In MIMO linked based 4G wireless networks, cryptographic algorithms are used to maintain physical layer security. With proper designed of powerful error-correction codes called low-density parity-check (LDPC) codes, a high level of data security can be provided at the physical layer[1].The WWWW(Wireless World Wide Web) supportable 5G network has not yet been deployed commercially and its physical layer radio interface technology (RAT) has not been standardized. The Mobile Internet and IoT (Internet of Things) have been considered as two main market drivers for 5G and will be used massively in augmented reality, virtual reality, remote computing, eHealth services, automotive driving etc. In 5G/future generation wireless network, massive MIMO antenna arrays with beamforming techniques would hopefully be implemented with consideration of physical layer security[2,3]. In 2010, Mei and et.al., proposed an approach to carrier scheme convergence based on 4-WFRFT. With utilization of such proposed technique, the authors demanded that communication facilities was capable of switching between multi-carrier (MC) ,OFDM and single-carrier (SC) system with simple parameters controlling and improving the distortion resistance capability of the communication system[4]. In 2016, Xiaojie and et.al., proposed a multiple parameters weighted fractional Fourier transform (MPWFRFT) and constellation scrambling (CS) method based physical layer (PHY) security system executed in two steps. In the first step of such proposed scheme, MPWFRFT was implemented as the constellation beguiling (CB) method to change signal's identity. In the second step, the additional pseudo random phase information regarded as the encryption key was attached to the original signal to enhance the security. The authors mentioned that their proposed physical layer (PHY) security scheme was capable of preventing the exchanging signals from eavesdropper's classification and inception.[5]. In 2017, Chen and et.al. proposed a novel user cooperation scheme based on weighted fractional Fourier transform (WFRFT), to enhance the physical (PHY) layer security of wireless transmissions against eavesdropping. The authors mentioned that the proposed security scheme was capable of creating an identical artificial noise to eavesdroppers and providing information bearing signal to the legitimate receiver. They also demanded that their proposed WFRFT-based user cooperation scheme could achieve significant performance advantage in terms of secrecy ergodic capacity, compared with conventional PHY-layer security oriented user

Author α σ: Assistant Professor, Department of Information and Communication Engineering, University of Rajshahi, Rajshahi-6205, Bangladesh. e-mails: lipy.naznin.ice.ru@gmail.com, mrh.ice.ru@gmail.com

Author ρ: Professor, Department of Information and Communication Engineering, University of Rajshahi, Rajshahi-6205, Bangladesh. e-mail: enayet_apee@ru.ac.bd

cooperation schemes such as relay-jamming and cluster-beamforming[6]. In this paper, we have presented information on suitability of signal detection scheme in performance evaluation of 4-WFRFT based physical layer security scheme implemented channel encoded system under consideration of color image transmission.

II. Signal Processing Techniques

In our present study various signal processing schemes have been used. A brief overview of these schemes is given below with special emphasis on Four -Weighted Fractional Fourier Transform (4-WFRFT) physical layer security scheme:

a) Four -Weighted Fractional Fourier Transform (4-WFRFT)

We assume that the binary data extracted from color image are channel coded and interleaved and subsequently digitally modulated using 4-QAM, QPSK and DQPSK mapping constellation. The complex digitally modulated symbols are rearranged block wise with each block containing 1024(L=1024) symbols. Under scenario of block wise signal processing, the 4-Weighted Fractional Fourier Transform (4-WFRFT) of a digitally modulated complex sequence

$X_0(n)$ (n=0,1,2,3……………L-1) is defined as:

$$\begin{aligned} S_0(n) &= F^{\alpha, m_k, n_k}[X_0(n)] \\ &= w_0(\alpha, m_k, n_k) X_0(n) + w_1.(\alpha, m_k, n_k) X_1(n) \\ &+ w_2(\alpha, m_k, n_k) X_2(n) + w_3.(\alpha, m_k, n_k) X_3(n) \\ &= w_0 X_0(n) + w_1.\frac{1}{\sqrt{L}} \sum_{l=0}^{l=L-1} X_0(l) e^{-j\frac{2\pi}{L} ln} \\ &+ w_2 X_0(-n) + w_3.\frac{1}{\sqrt{L}} \sum_{l=0}^{l=L-1} X_0(l) e^{-j\frac{2\pi}{L} ln} \end{aligned} \tag{1}$$

where, k= 0, 1, 2, 3 ; $\{X_0(n), X_1(n), X_2(n), X_3(n)\}$ are the 0~3 times normalized DFT of $X_0(n)$ separately and the weighting coefficients w_p(p =0, 1, 2, 3) are defined by[7]

$$w_p = \frac{1}{4} \sum_{k=0}^{k=3} \exp\{\pm \frac{2\pi j}{4} [(4m_k + 1)\alpha(k + 4n_k) - pk]\} \quad (p = 0,1,2,3) \tag{2}$$

b) LDPC Channel Coding

The low-density parity-check (LDPC) code has been considered as one of the useful modern channel codes. It was invented as early as 1962 by Gallager. It is a linear block code whose parity-check matrix H_{parity} contains only a few 1's in comparison to 0's (i.e., sparse matrix). In our study, we have used linear block code with coding rate ½ defined by 64× 128 sized parity-check matrix H_{parity}. The LDPC code can be represented by the bilateral Tanner graph containing two kinds of nodes(bit nodes or variable nodes are associated with a column and check nodes or parity nodes are associated with a row of the parity-check matrix H_{parity}. In case of merely any elemental value of the H_{parity} matrix is of 1, a parity node will be connected to a bit node[8].In each LDPC channel encoded 1×128 matrix sized codeword c, the first 64 bits of the codeword matrix are the parity bits and the last 64 bits are the information bits. The LDPC decoding adopts an iterative approach and operates alternatively on the bit nodes and the check nodes to find the most likely codeword c that satisfies the condition $cH^T_{parity}=0$. In iterative Log Domain Sum-Product LDPC decoding, various steps are followed with estimation of various parameters. Primarily, the 128×1 sized received bit sequence $rx_{i,\ i=1,2,3.................128}$ are converted from (0/1) format into (-1/1) format and passed through AWGN channel of noise variance of N0. The log-likelihood ratio (LLR) of transmitted codeward $c=[c_1c_2c_3c_4.......c_{128}]$ is given by

$$Lc_i = -4rx_i/N0 \tag{3}$$

Taking transposed form of Equation (3) and considering all its sampled values and inserting in each of 64 rows, a 64× 128 sized [LCI] matrix is formed. As the Lqij are considered to be the messages sent from bit nodes i to check nodes j, initially, 64× 128 sized [LQIJ] matrix is formed from the element wise product of two matrices $[H_{parity}]$ and[LCI] as:

$$[LQIJ] = [H_{parity}] \odot [LCI] \tag{4}$$

From matrix [LQIJ], α_{ij} and β_{ij} are estimated using the following relation:

$$\alpha_{ij} \triangleq \text{sign}[LQIJ] \quad \beta_{ij} \triangleq |LQIJ|$$

Initially, a 64× 128 sized [LRJI] matrix is considered as null matrix. In horizontal stepping for finding non zero in the column of H_{parity} matrix, the Pibetaij parameter values at the position(r,l) are estimated using the relation:

$$\text{Pibetaij}(r,l) = \ln[(\exp(\beta_{ij}(r,l)+1)/[(\exp(\beta_{ij}(r,l)-1)] \tag{5}$$

At each position of non zero element, new values Pibetaij(i,c1) are estimated from the summation of all column wise Pibetaij values- previous Pibetaij value at that position where, i=1,2, …….64, c1 is the non zero elemental position in the column for a row identified by i. With estimated values of Pibetaij(i,c1), PiSum(i,c1) are estimated as:

$$\text{PiSum}(i,c1) = \ln[(\exp(\text{Pibetaij}(i,c1)+1)/[(\exp(\text{Pibetaij}(i,c1)-1)] \tag{6}$$

Similarly, another parameter prodOf(i,c1) values are estimated from the product of all column wise multiplied α_{ij} values with α_{ij} value at that position. The previously considered [LRJI] matrix is upgraded through inserting the parameter Lrji(i,c1) values as:

$$\text{Lrji}(i,c1) = \text{prodOf}(i,c1) * \text{PiSum}(i,c1) \tag{7}$$

In vertical stepping for finding non zero in the row of H_{parity}matrix, the Lqij parameter values at the position (r1,j) are updated using the relation:

$$\mathrm{Lqij(r1,j)=Lc_i+sum(Lrji(r1,j))-Lrji(r1,j)} \quad (8)$$

where, i=1,2.........128, j=1,2.........128
Finally, a new parameter value is estimated as:

$$\mathrm{LQi = Lc_i + sum(Lrji(r1, j))} \quad (9)$$

If LQi is less than zero, the transmitted bit is 1, otherwise the transmitted bit is 0. The above mentioned steps in iterative Log Domain Sum-Product LDPC decoding algorithm have been executed in MATLAB source codes available in the website at[9]. Generation of different sized parity-check matrix and estimation of parity bits corresponding to information bits have also been presented in the cited website.

c) Signal detection scheme

In our 4 x 4 simulated LDPC encoded MIMO wireless communication system, the transmitted and received signals are represented by $x=[x_1, x_2, x_3, x_4]^T$ and $y=[y_1, y_2, y_3, y_4]^T$ respectively. If $n= [n_1, n_2, n_3, n_4]^T$ denotes the white Gaussian noise with a variance $\boldsymbol{\sigma}_n^2$ and the channel matrix is represented by $H=[\,h_1\ h_2\ \ h_3\ h_4\,]$, we can write

$$\mathbf{y} = \mathbf{Hx} + n = \mathbf{h}_1 x_1 + \mathbf{h}_2 x_2 + \mathbf{h}_3 x_3 + \mathbf{h}_4 x_4 \quad (10)$$

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

$$\tilde{x} = [\tilde{x}_1, \tilde{x}_2, \tilde{x}_3, \tilde{x}_4]^T = Wy \quad (11)$$

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

$$W_{MMSE} = (H^H H + \sigma_n^2 I)^{-1} H^H \quad (12)$$

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

$$\tilde{x}_{MMSE} = W_{MMSE}\, y \quad (13)$$

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

$$W_{ZF} = (H^H H)^{-1} H^H \quad (14)$$

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

$$\tilde{x}_{ZF} = W_{ZF}\, y \quad (15)$$

In MMSE-SIC based signal detection scheme, the received signal, channel matrix and noise are extended as

$$\overleftrightarrow{\mathbf{H}}_{ex} = \left[\overleftrightarrow{\mathbf{H}}^{\mathrm{T}} \sqrt{\frac{\boldsymbol{\sigma}^2_n}{\boldsymbol{\sigma}^2_s}}\mathbf{I} \right]^{\mathrm{T}},\ \mathbf{Y}_{ex} = \left[\mathbf{Y}^{\mathrm{T}} \quad \mathbf{0}^{\mathrm{T}} \right] \text{ and}$$

$$\mathbf{N}_{ex} = \left[\mathbf{N}^{\mathrm{T}} - \sqrt{\frac{\boldsymbol{\sigma}^2_n}{\boldsymbol{\sigma}^2_s}}\mathbf{X}^{\mathrm{T}} \right]^T \quad (16)$$

Where, $\frac{\sigma^2_n}{\sigma^2_s}$ is the ratio of average receive noise power to average receive signal power.

The signal model in terms of transmitted and received signals, noise and channel coefficients can be written as

$$Y_{ex} = \overleftrightarrow{H}_{ex} X + N_{ex} \quad (17)$$

On QR factorization of 8 × 4 sized extended channel matrix $\overleftrightarrow{\mathrm{H}}_{ex}$, we get

$$\overleftrightarrow{H}_{ex} = \overleftrightarrow{Q}_{ex}.\overleftrightarrow{R}_{ex} \quad (18)$$

where, $\overleftrightarrow{\mathrm{Q}}_{ex}$. and $\overleftrightarrow{\mathrm{R}}_{ex}$ represent 8 × 8 sized unitary matrix and 8 × 4 sized upper triangular matrix respectively. Substituting the values of $\overleftrightarrow{\mathrm{H}}_{ex}$ in Equation (17) and multiplying with $\overleftrightarrow{\mathrm{Q}}^{H}_{ex}$, we get

$$\overleftrightarrow{Y}_{ex} = \overleftrightarrow{R}_{ex}.X + \overleftrightarrow{Q}^{H}_{ex}.N_{ex} \quad (19)$$

Equation(19) can be rewritten with neglecting $\mathrm{Q}^{H}_{ex}.\mathrm{N}_{ex}$ term as:

$$\overleftrightarrow{Y}_{ex} = \begin{bmatrix} \overleftrightarrow{\mathbf{Y}}_{\mathbf{ex1}} \\ \overleftrightarrow{\mathbf{Y}}_{\mathbf{ex2}} \\ \overleftrightarrow{\mathbf{Y}}_{\mathbf{ex3}} \\ \overleftrightarrow{\mathbf{Y}}_{\mathbf{ex4}} \\ \overleftrightarrow{\mathbf{Y}}_{\mathbf{ex5}} \\ \overleftrightarrow{\mathbf{Y}}_{\mathbf{ex6}} \\ \overleftrightarrow{\mathbf{Y}}_{\mathbf{ex7}} \\ \overleftrightarrow{\mathbf{Y}}_{\mathbf{ex8}} \end{bmatrix} = \begin{bmatrix} \overleftrightarrow{\mathbf{R}}_{\mathbf{ex}}(1,1) & \overleftrightarrow{\mathbf{R}}_{\mathbf{ex}}(1,2) & \overleftrightarrow{\mathbf{R}}_{\mathbf{ex}}(1,3) & \overleftrightarrow{\mathbf{R}}_{\mathbf{ex}}(1,4) \\ 0 & \overleftrightarrow{\mathbf{R}}_{\mathbf{ex}}(2,2) & \overleftrightarrow{\mathbf{R}}_{\mathbf{ex}}(2,3) & \overleftrightarrow{\mathbf{R}}_{\mathbf{ex}}(2,4) \\ 0 & 0 & \overleftrightarrow{\mathbf{R}}_{\mathbf{ex}}(3,3) & \overleftrightarrow{\mathbf{R}}_{\mathbf{ex}}(3,4)) \\ 0 & 0 & 0 & \overleftrightarrow{\mathbf{R}}_{\mathbf{ex}}(4,4) \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} \overleftrightarrow{\mathbf{X}}_{\mathbf{1}} \\ \overleftrightarrow{\mathbf{X}}_{\mathbf{2}} \\ \overleftrightarrow{\mathbf{X}}_{\mathbf{3}} \\ \overleftrightarrow{\mathbf{X}}_{\mathbf{4}} \end{bmatrix} \quad (20)$$

From Equation (20), the primarily estimated detected signal $\overleftrightarrow{X}$ from the four transmitting antennas can written as:

$$\begin{aligned}
\ddot{X}_4 &= \frac{\ddot{Y}_{ex4}}{\ddot{R}_{ex}(4,4)} \\
\ddot{X}_3 &= \frac{(\ddot{Y}_{ex3} - \ddot{R}_{ex}(3,4)\ddot{X}_4)}{\ddot{R}_{ex}(3,3)} \\
\ddot{X}_2 &= \frac{(\ddot{Y}_{ex2} - \ddot{R}_{ex}(2,3)\ddot{X}_3 - \ddot{R}_{ex}(2,4)\ddot{X}_4)}{\ddot{R}_{ex}(2,2)} \\
\ddot{X}_1 &= \frac{(\ddot{Y}_{ex1} - \ddot{R}_{ex}(1,2)\ddot{X}_2 - \ddot{R}_{ex}(1,3)\ddot{X}_3 - \ddot{R}_{ex}(1,4)\ddot{X}_4)}{\ddot{R}_{ex}(1,1)}
\end{aligned} \tag{21}$$

With ML decoding, the digitally modulated detected signals can be written using the following relation,:

$$\ddot{\hat{x}}_m = \arg\min_{\hat{x}^{(k)} \in \vec{x}} \left|\hat{x}^{(k)} - \ddot{x}_m\right|^2 \tag{22}$$

where, $\vec{\mathbf{X}}$ is the digitally modulated complex symbols.

In ZF-SIC channel equalization scheme, the channel matrix H undergoes QR factorization as

$$H = QR = Q\begin{bmatrix} R_{1,1} & R_{1,2} & R_{1,3} & R_{1,4} \\ 0 & R_{2,2} & R_{2,3} & R_{2,4} \\ 0 & 0 & R_{3,3} & R_{3,4} \\ 0 & 0 & 0 & R_{3,4} \end{bmatrix} \tag{23}$$

where, Q and R are the unitary and upper triangular matrix respectively. Equation (10) can be rewritten on multiplying by Q^H as

$$\bar{y} = Q^H y = Rx + Q^H n \tag{24}$$

where, $Q^H N$ is a zero-mean complex Gaussian random vector. Since $Q^H n$ and n have the same statistical properties, $Q^H n$ can be used to denote **n**. We get Equation (24) as

$$\bar{y} = Rx + n$$

$$\Downarrow$$

$$\begin{bmatrix} \bar{\mathbf{y}}_1 \\ \bar{\mathbf{y}}_2 \\ \bar{\mathbf{y}}_3 \\ \bar{\mathbf{y}}_4 \end{bmatrix} = \begin{bmatrix} \mathbf{r}_{1,1} & \mathbf{r}_{1,2} & \mathbf{r}_{1,3} & \mathbf{r}_{1,4} \\ \mathbf{0} & \mathbf{r}_{2,2} & \mathbf{r}_{2,3} & \mathbf{r}_{2,4} \\ \mathbf{0} & \mathbf{0} & \mathbf{r}_{3,3} & \mathbf{r}_{3,4} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{r}_{4,4} \end{bmatrix} \begin{bmatrix} \tilde{\mathbf{x}}_1 \\ \tilde{\mathbf{x}}_2 \\ \tilde{\mathbf{x}}_3 \\ \tilde{\mathbf{x}}_4 \end{bmatrix} + \begin{bmatrix} \mathbf{n}_1 \\ \mathbf{n}_2 \\ \mathbf{n}_3 \\ \mathbf{n}_4 \end{bmatrix} \tag{25}$$

the primarily estimated detected signal $\tilde{X}$ from the four transmitting antennas can written on neglecting noise term from Equation (25) as

$$\begin{aligned}
\tilde{\mathbf{x}}_4 &= \frac{\bar{\mathbf{y}}_4}{\mathbf{r}_{4,4}} \\
\tilde{\mathbf{x}}_3 &= \frac{(\bar{\mathbf{y}}_3 - \mathbf{r}_{3,4}\tilde{\mathbf{x}}_4)}{\mathbf{r}_{3,3}} \\
\tilde{\mathbf{x}}_2 &= \frac{(\bar{\mathbf{y}}_2 - \mathbf{r}_{2,3}\tilde{\mathbf{x}}_3 - \mathbf{r}_{2,4}\tilde{\mathbf{x}}_4)}{\mathbf{r}_{2,2}} \\
\tilde{\mathbf{x}}_1 &= \frac{(\bar{\mathbf{y}}_1 - \mathbf{r}_{1,2}\tilde{\mathbf{x}}_2 - \mathbf{r}_{1,3}\tilde{\mathbf{x}}_3 - \mathbf{r}_{1,4}\tilde{\mathbf{x}}_4)}{\mathbf{r}_{1,1}}
\end{aligned} \tag{26}$$

With ML decoding, the digitally modulated detected signals can be written using the following relation,:

$$\tilde{\tilde{x}}_m = \arg\min_{\hat{x}^{(k)} \in \vec{x}} \left|\hat{x}^{(k)} - \tilde{x}_m\right|^2 \tag{27}$$

where, $\vec{\mathbf{X}}$ is the digitally modulated complex symbols[10,11].

d) 2D Median Filtering

2D median filtering is widely used as an effective technique for removing various types of noises (salt and pepper and Gaussian) from noise contaminated image. In such filtering operation, the pixel values in the neighborhood window are generally ranked according to intensity and the middle value (the median) becomes the output value for the pixel under evaluation. In this paper, 2D Median Filtering scheme with a 3×3 neighborhood windowing mask is preferably used to make sorting of all the pixel values within the window and finding the median value and replacing the original pixel value with the median value [12].

III. System Description

The simulated LDPC encoded MIMO Wireless Communication System with Implementation of MP-WFRFT based physical layer security scheme is depicted in Figure 1.A RGB color image with 96 pixels width and 96 pixels height has been considered. The color image is converted into its respective three Red, Green and Blue components with each component is of 96 × 96 pixels in size. The pixel integer values are converted into 8 bits binary form and channel encoded using LDPC and interleaved and subsequently digitally modulated using QPSK, DQPSK and 4-QAM[13]. The digitally modulated complex data sequence are transformed using 4-Weighted Fractional Fourier Transform (4-WFRFT) for encryption. The encrypted data symbols are fed into spatial multiplexing encoder section for production of four data series to be transmitted simultaneously from four antennas. In receiving section, the transmitted signals are detected using various signal detection techniques. The detected signals are decrypted and fed into spatial multiplexing decoder, digitally demodulated, deinterleaved and channel decoded. The estimated binary data are now converted into integer form and processed for 2-D image filtering. The filtered data are entered into R,G and B components and eventually, color image is retrieved.

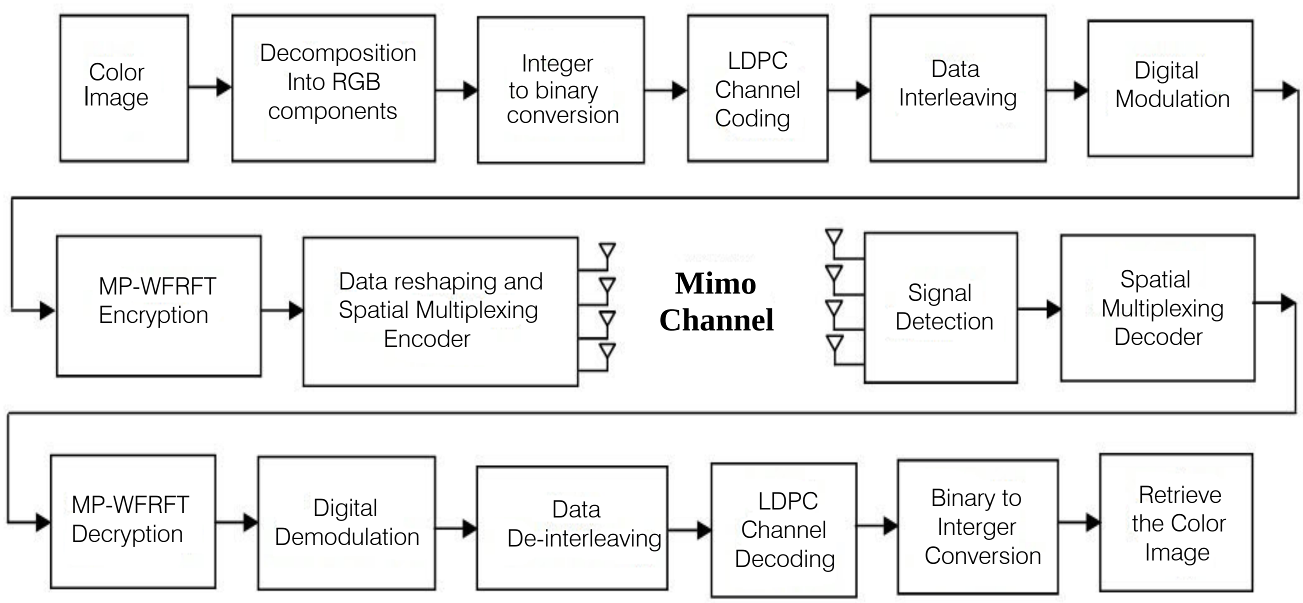

Figure 1: Block Diagram Of Physical Layer Security Scheme Implemented LDPC Encoded MIMO Wireless Communication System

IV. Result and Discussion

In this section, we present a series of simulation results using MATLAB R2014a to illustrate the significant impact of various types of signal detection and modulation techniques on performance of LDPC encoded and MP-WFRFT based physical layer security scheme implemented .MIMO wireless communication system in terms of bit error rate (BER). It is assumed that the channel state information (CSI) of the MIMO fading channel is available at the receiver and the fading channel coefficients are constant during simulation. The proposed model is simulated to evaluate the quality of the system performance with considering the following parameters presented in the Table 1.

Table 1: Summary of the simulated model parameters

Parameters	Types
Data Type	Color image
Image Size	(96 x 96 x 3) pixels
Physical Layer Security scheme	Multiple parameters weighted fractional Fourier transform (MPWFRFT) with constellation scrambling (CS)
WFRFT modulation order	0.2
Arbitrary real parameters [m] and [n] considered in estimation of weighting coefficients	[1,3,7,0] and [8,3,1,5]
Noise reduction image filter	2D-Median filter
Antenna configuration	4 x 4 MIMO Channel

Channel Coding	LDPC
LDPC Channel decoding	Log-domain sum product
Digital Modulation	QPSK, DQPSK and 4-QAM
Signal Detection Scheme	ZF,MMSE,ZF-SIC and MMSE-SIC
SNR	0 to 15 dB
Channel	AWGN and Rayleigh

Graphical illustrations presented in Figure 2 through Figure 5 are clearly indicative that our considered LDPC channel encoded simulated system shows comparatively better performance in QAM digital modulation as compared to QPSK and DQPSK. The system performance in terms of bit error rate (BER) is very much well defined in all cases.

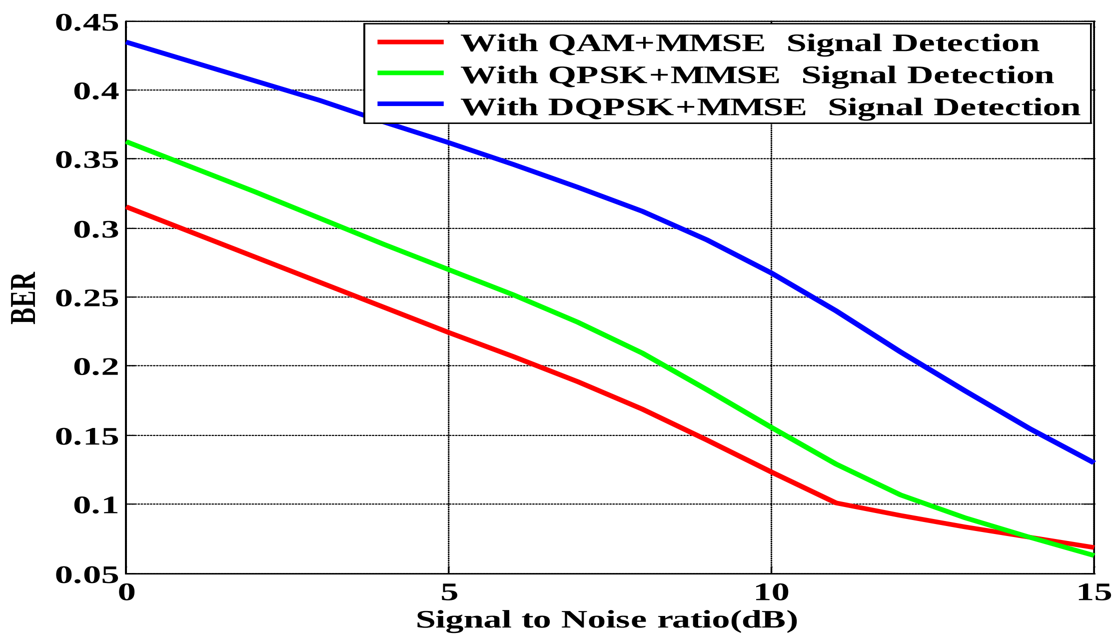

Figure 2: BER performance of LDPC channel encoded MP-WFRFT based Physical Layer Security Scheme implemented MIMO wireless communication under utilization of various digital modulation and MMSE signal detection technique

It is seen from Figure 2 that the estimated BER values at a typically assumed SNR value of 5dB are 0.2247 and 0.3616 in case of QAM and DQPSK which is indicative of system performance improvement of 2.07 dB in QAM as compared to DQPSK. At 15% BER, SNR gain of 1.41dB and 5.39dB are achieved in QAM as compared to QPSK and DQPSK .

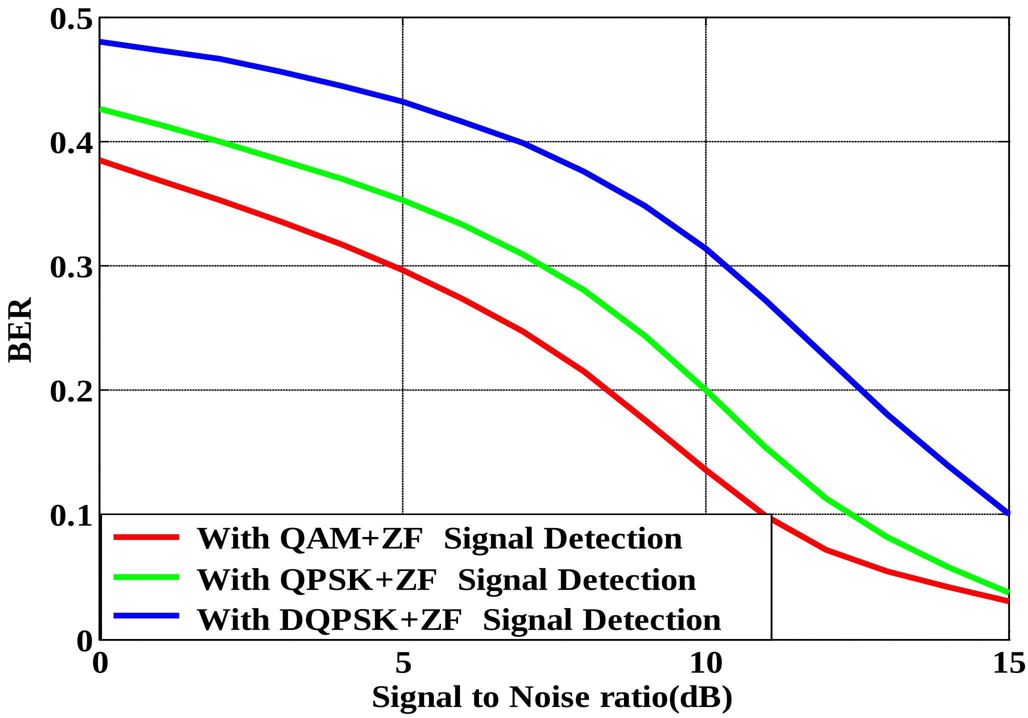

Figure 3: BER performance of LDPC channel encoded MP-WFRFT based Physical Layer Security Scheme implemented MIMO wireless communication under utilization of QAM and ZF signal detection technique

At 5dB SNR value, the estimated BER values are 0.2968 and 0.4315 in case of QAM and DQPSK (Figure 3) which is indicative of system performance improvement of 1.63 dB in QAM as compared to DQPSK. It is noticeable from Figure 3 that at 15% BER, SNR gain of 1.48dB and 3.98dB are achieved in QAM as compared to QPSK and DQPSK.

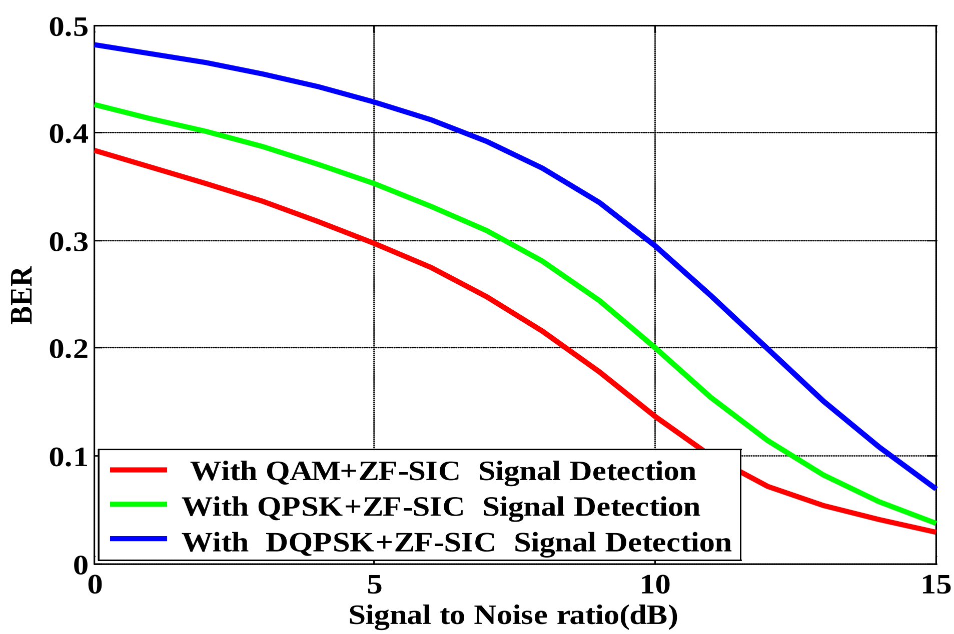

Figure 4: BER performance of LDPC channel encoded MP-WFRFT based Physical Layer Security Scheme implemented MIMO wireless communication under utilization of QAM and ZF-SIC signal detection technique

In Figure 4, the estimated BER values are found to have values 0.2978 and 0.4284 in case of QAM and DQPSK for a typically assumed SNR value of 5dB which implies a system performance improvement of 1.58 dB in QAM as compared to DQPSK. At 15% BER, SNR gain of 1.56dB and 1.95dB are achieved in QAM as compared to QPSK and DQPSK.

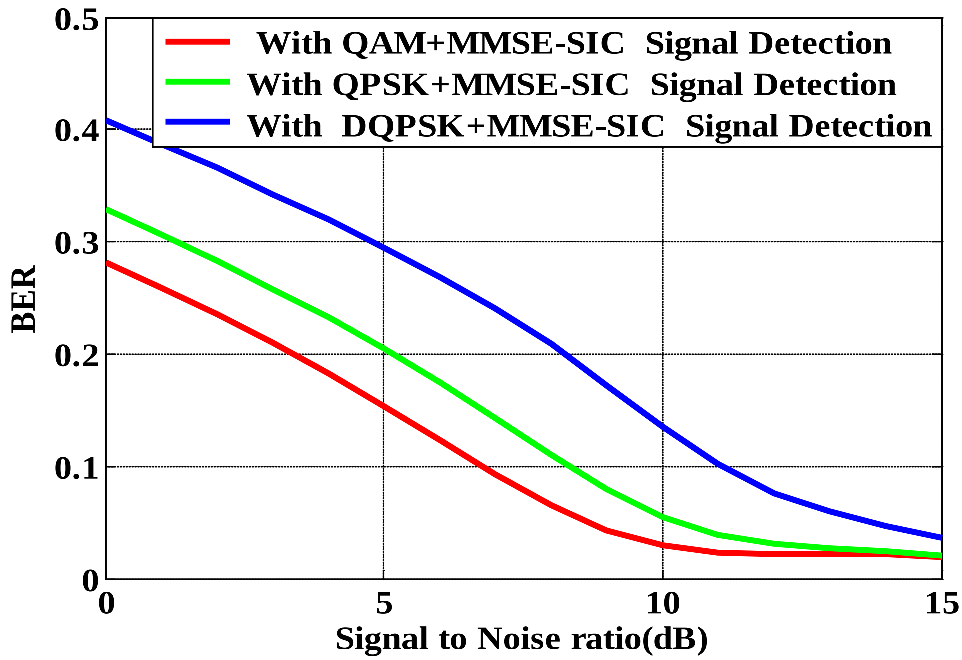

Figure 5: BER performance of LDPC channel encoded MP-WFRFT and CS based Physical Layer Security Scheme implemented MIMO wireless communication under utilization of QAM and MMSE-SIC signal detection technique

It is quite observable from Figure 5 that at a SNR value of 5dB, the estimated BER values are 0.1541 and 0.2947 in case of QAM and DQPSK which ratifies a system performance improvement of 2.82 dB in QAM as compared to DQPSK. It is also quite obvious from Figure 5 that at 15% BER, SNR gain of 1.60dB and 4.53dB are achieved in QAM as compared to QPSK and DQPSK.

Our critical observation at various images presented in Figure 6, it is justified that the encrypted image is not understandable. The quality of the retrieved images improves with the increase in SNR values. The impact of 2-D filtering technique on improvement of retrieved image is reasonably acceptable.

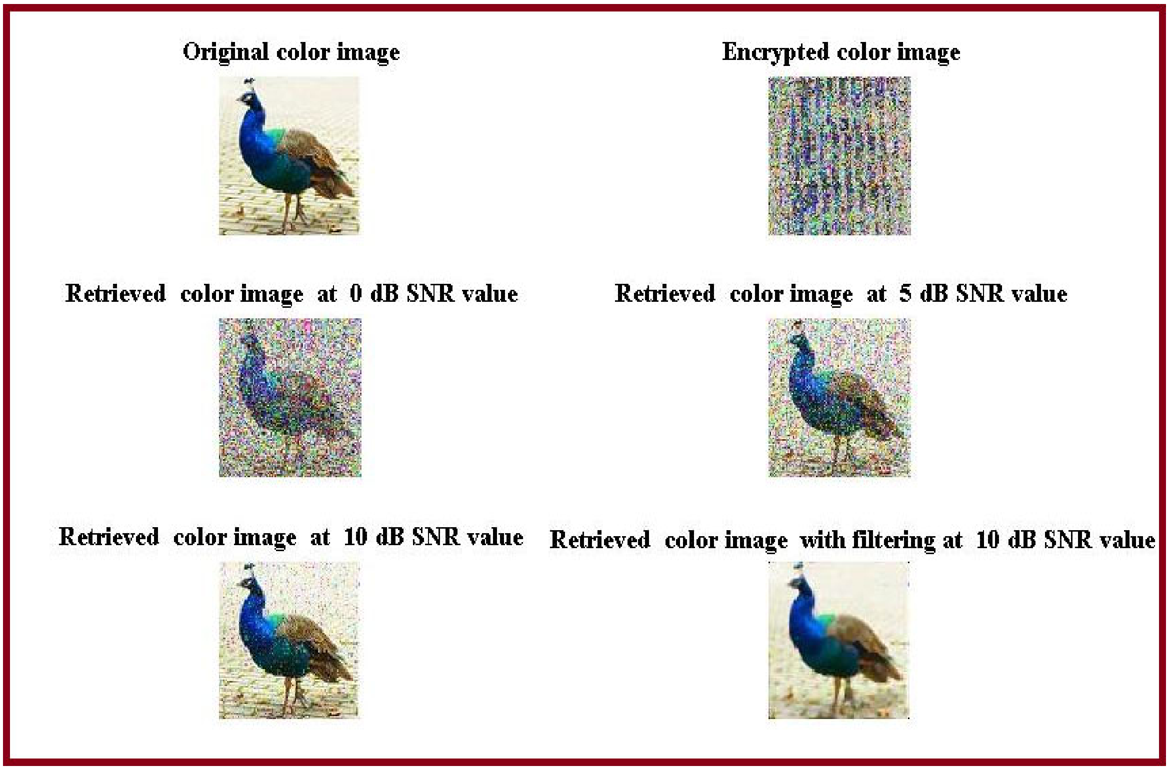

Figure 6: Transmitted, Encrypted and Retrieved color images in LDPC channel encoded MP-WFRFT and CS based physical layer security scheme implemented MIMO wireless communication

In Figure 7, it is quite obvious that the pixel values of the original color image have comparatively higher values at the lower and upper regions. Over significant part of the histogram, the original color image contains low pixel values. In case of 0dB SNR and encrypted image, distribution of pixel values are totally changed. In case of higher SNR value preferably 10dB and filtered image, the presented histograms get resemblance as to original image.

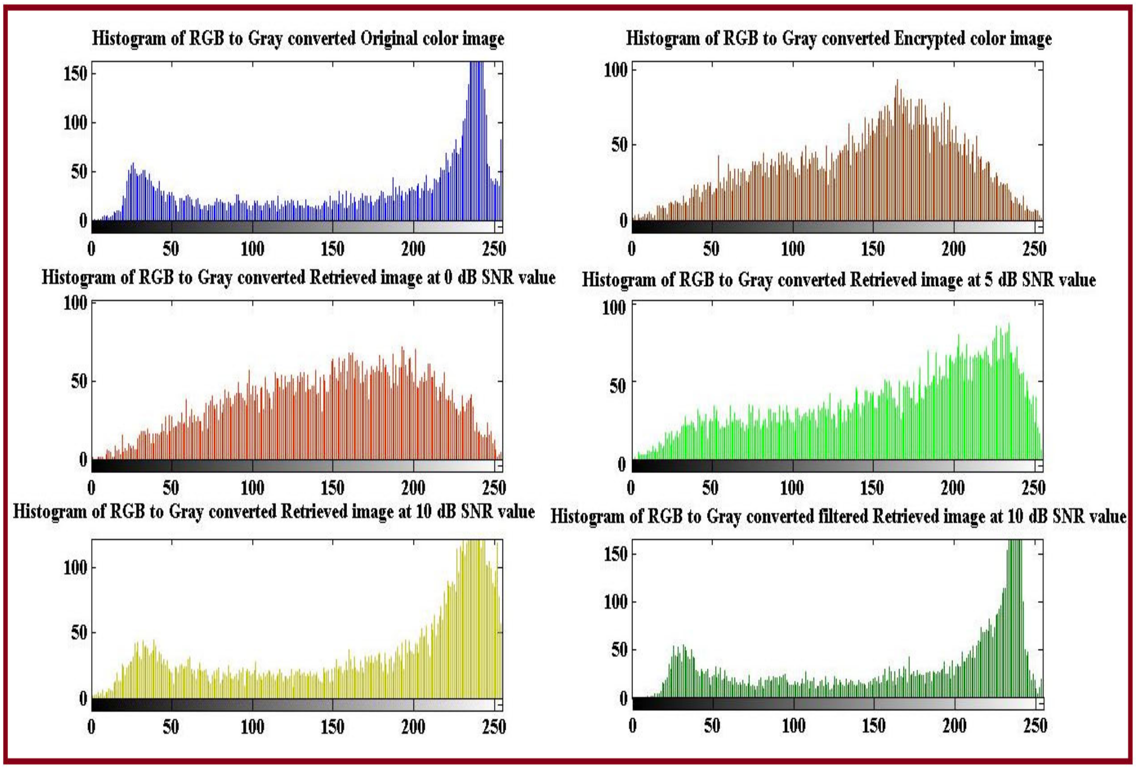

Figure 7: Histogram of RGB to Gray converted Transmitted, Encrypted and Retrieved color images in LDPC channel encoded MP-WFRFT based physical layer security Scheme implemented MIMO wireless communication

In Figure 8, 3 dimensional graphical illustration showing transmitted, encrypted and retrieved color images with and without filtering have been presented to justify the suitability of our proposed physical layer security scheme implemented wireless communication system.

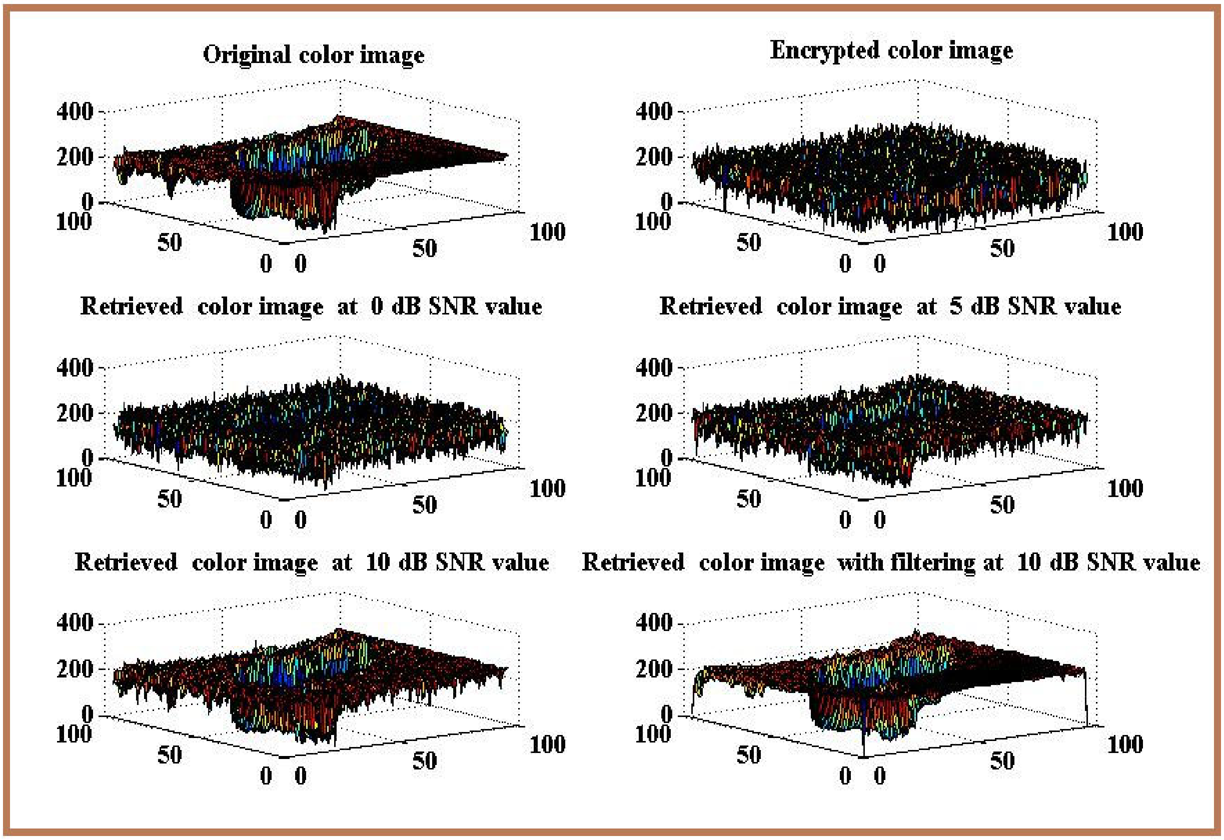

Figure 8: 3-Dimensional Graphical illustration showing transmitted, Encrypted and retrieved color images with and without filtering in LDPC channel encoded MP-WFRFT based physical layer security scheme implemented MIMO wireless communication

V. Conclusions

In this paper, the performance of MP-WFRFT based physical layer security scheme implemented LDPC encoded MIMO wireless communication system has been investigated on secured color image transmission with .utilization of various channel equalization/signal detection techniques. In all cases, the system out performs in 4-QAM and shows worst performance in DQPSK digital modulations. The simulation results show that the implementation of MMSE-SIC signal detection scheme with utilization of 4-QAM digital modulation schemes ratifies the robustness of LDPC encoded and MP-WFRFT based physical layer security scheme implemented MIMO wireless communication system in retrieving color image transmitted over noisy and Rayleigh fading channels.

References Références Referencias

1. Xiangyun Zhou, Lingyang Song and Yan Zhang, “Physical Layer Security in Wireless Communications”, CRC Press, Taylor and Francis Group, Florida, USA, 2014.
2. Xiang, Kan Zheng, Xuemin (Sherman) Shen, “5G Mobile Communications”, Springer International Publishing company, Switzerland, 2017.
3. Elias Yaacoub and Mohammed Al-Husseini, “Achieving Physical Layer Security with Massive MIMO Beamforming”, European Conference on Antennas and Propagation (EUCAP), pp.1753-1757, 2017.
4. Lin Mei, Xue-junSha, and Nai-tong Zhang, “The Approach to Carrier Scheme Convergence Based on 4-Weighted Fractional Fourier Transform”, IEEE COMMUNICATIONS LETTERS, vol. 14, no. 6, pp.503-505, 2010.
5. FANG Xiaojie, SHA Xuejun, LI Yue, “MP-WFRFT and Constellation Scrambling Based Physical Layer Security System”, China communications, pp.138-145, 2016.
6. Dajiang Chen, Xuejun Sha, and Xuemin (Sherman) Shen, Xiaojie Fang, Ning Zhang, Shan Zhang, “On Physical Layer Security: Weighted Fractional Fourier Transform based User Cooperation”, 2017.
7. Lin Mei, Xue-jun Sha, and Nai-tong Zhang, “The Approach to Carrier Scheme Convergence Based on4-Weighted Fractional Fourier Transform”, IEEE Communications Letters, vol. 14, no.6, pp. 503-505, 2010.
8. Yuan Jiang, “A Practical Guide to Error-ControlCoding Using MATLAB”, Artech House, Norwood, MA, USA, 2010.

9. Bagawan Sewu Nugroho, https://sites.google.com/site/bsnugroho/ldpc.
10. Yong Soo Cho, Jackson Kim, Won Young Yang, Chung G. Kang, "MIMO-OFDM Wireless Communications with MATLAB", John Wiley and Sons (Asia) PTE Limited, Singapore, 2010.
11. Lin Baiand Jinho Choi, "Low Complexity MIMO Detection", Springer Science and Business Media, LLC, New York, USA, 2012.
12. Oge Marques, "Practical Image and Video Processing Using MATLAB", John Wiley and Sons, New Jersey, USA, 2011.
13. T. S. Rappaport, "Wireless communications", Upper Saddle River, New Jersey, USA: Prentice Hall, 1st ed.1996.