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

Laila Naznin[1], Mohammad Reaz Hossain[2] and Shaikh Enayet Ullah[3]

[1] Rajshahi University

*Received: 16 December 2016 Accepted: 4 January 2017 Published: 15 January 2017*

## 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.

***Index terms***— 4-weighted fractional fourier transform, MIMO, LDPC, SNR.

# 1 I. Introduction

ur 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 multicarrier (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 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.

# 2 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:

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: 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] ) 0,1,2,3ln 2 1 0 0 3 0 2 ln 2 1 0 0 1 0 0 3 k k 3 2 k k 2 1 k k 1 0 k k 0 0 k n , k m ?, 0 (l) X 1 . w (-n) X w (l) X 1 . w (n) X w (n) )X n , m , ( . w (n) )X n , m , ( w (n) )X n , m , ( . w (n) )X n , m , ( w (n)] [X F (n) S= (p ]} ) 4 ( ) 1 4 [( 4 2 exp{ 4 1 3 0 pk n k m j w k k k k p ? + + ± = ? = = ? ? (2)

# 3 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 paritycheck 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 areLc i =-4rx i /N0**(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 ] [LCI]**(4)**

From matrix [LQIJ], ij ? and ij ? are estimated using the following relation:ij ? sign[LQIJ] ij ? |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:Pibetaij(r,l)=ln[(exp( ij ? (r,l)+1)/[(exp( ij ? (r,l)-1)]**(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 PiSum(i,c1)=ln[( exp( (i,c1), PiSum(i,c1) are estimated as:Pibetaij (i,c1)+1)/[( exp(Pibetaij

Similarly, another parameter prodOf(i,c1) values are estimated from the product of all column wise multiplied(i,c1)-1)] (6) ij ?

values with ij ? value at that position. The previously considered [LRJI] matrix is upgraded through inserting the parameter Lrji(i,c1) values as: associated with a row of the parity-check matrix H parity .Lrji(i,c1)=prodOf(i,c1)*PiSum(i,c1)**(7)**

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 1 c 2 c 3 c 4 ??.c 128 ] is given by 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: Lqij(r1,j)=Lc i +sum(Lrji(r1,j))-Lrji(r1,j) (8) where, i=1,2???128, j=1,2???128 Finally, a new parameter value is estimated as:LQi = Lc i + sum(Lrji(r1, j)) (**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.

# 4 c) Signal detection scheme

In n + = Hx y 4 4 3 3 2 2 1 1 x x x x h h h h + + + = (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 byWy x x x x x T = = ] , , , [ ~4 3 2 1 (11)

In Minimum mean square error (MMSE) scheme, the MMSE weight matrix is given byH n H MMSE H I H H W 1 2 ) ( ? + = ?**(12)**

and the detected desired signal from the transmitting antenna is given byy W x MMSE MMSE = ~(13)

In Zero-Forcing (ZF) scheme, the ZF weight matrix is given byH H ZF H H H W 1 ) ( ? = (14)

and the detected desired signal from the transmitting antenna is given byy W x ZF ZF = ~(15)

In MMSE-SIC based signal detection scheme, the received signal, channel matrix and noise are extended asT s 2 n 2 T ex I ? ? H H ? ? ? ? ? ? ? ? ? = ? ? , [ ] T T ex 0 Y Y = and T ? ? ? ? ? ? ? ? ? ? = T s 2 n 2 T ex X ? ? N N (16)

Where, s? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? = = 4 X 3 X 2 X 1 X 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 (4,4) ex R 0 0 0 (3,4)) ex R (3,3) ex R 0 0 (2,4) ex R (2,3) ex R (2,2) ex R 0 (1,4) ex R (1,3) ex R (1,2) ex R (1,1) ex R ex8 Y ex7 Y ex6 Y ex5 Y ex4 Y ex3 Y ex2 Y ex1 Y ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ex Y

From Equation (20), the primarily estimated detected signal X ? from the four transmitting antennas can written as:

( 20)(1,1) ex R ) 4 X (1,4) ex R 3 X (1,3) ex R 2 X (1,2) ex R ex1 Y ( 1 X (2,2) ex R ) 4 X (2,4) ex R 3 X (2,3) ex R ex2 Y ( 2 X (3,3) ex R ) 4 X (3,4) ex R ex3 Y ( 3 X (4,4) ex R ex4 Y 4 X ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? = ? ? = ? = =

With ML decoding, the digitally modulated detected signals can be written using the following relation,:x x x x x k m k m ? ? ? ? ? ? = ) ( 2 ) ( min arg (22)

where, x ? is the digitally modulated complex symbols.? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? = = 4 , 3 4 , 3 3 , 3 4 , 2 3 , 2 2 , 2 4 , 1 3 , 1 2 , 1 1 , 1 0 0 0 0 0 0 R R R R R R R R R R Q QR H n Q Rx y Q y H H + = = (24)

where, N Q H is a zero-mean complex Gaussian random vector. Since n Q H and n have the same statistical properties, n Q H can be used to denote n. We get Equation ( **??**4 With ML decoding, the digitally modulated detected signals can be written using the following relation,:x x x x x x k m k m ? ? ? = ) ( 2 ) ( ?min arg ~(27)

where, x ? is the digitally modulated complex symbols [10,11] .

# 5 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]. In ZF-SIC channel equalization scheme, the channel matrix H undergoes QR factorization as where, Q and R are the unitary and upper triangular matrix respectively. Equation ( **??**0) can be rewritten on multiplying by Q H as

# 6 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.

# 7 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 **??**. In Figure **??**, 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. 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. [1] [2] [3] [4]

**1**

Figure 1: 1 A

Figure 2: A

**1**

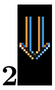
Figure 3: Figure 1 :

[1] Year 2017 ( ) © 2017 Global Journals Inc. (US)

[2] © 2017 Global Journals Inc. (US)

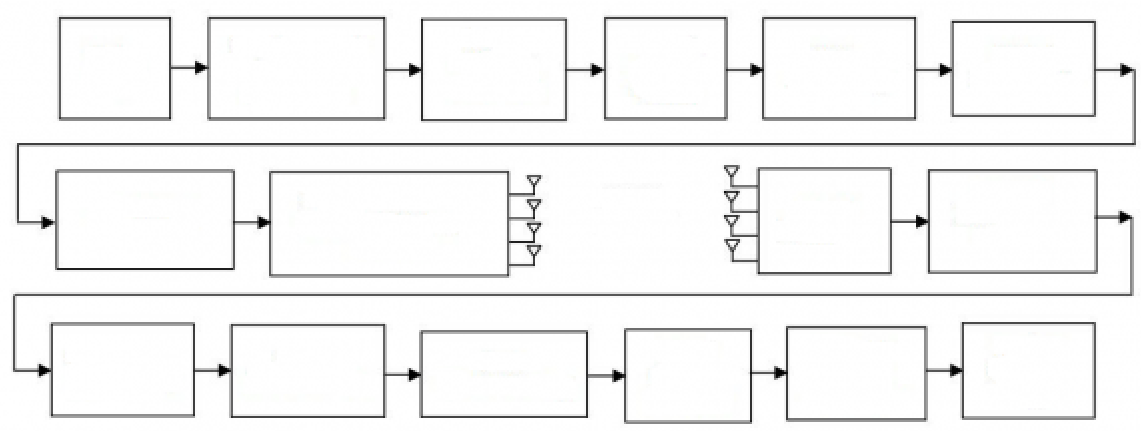
[3] Year 2017 ( ) © 2017 Global Journals Inc. (US) 1

[4] Year 2017 ( ) © 2017 Global Journals Inc. (US) 1



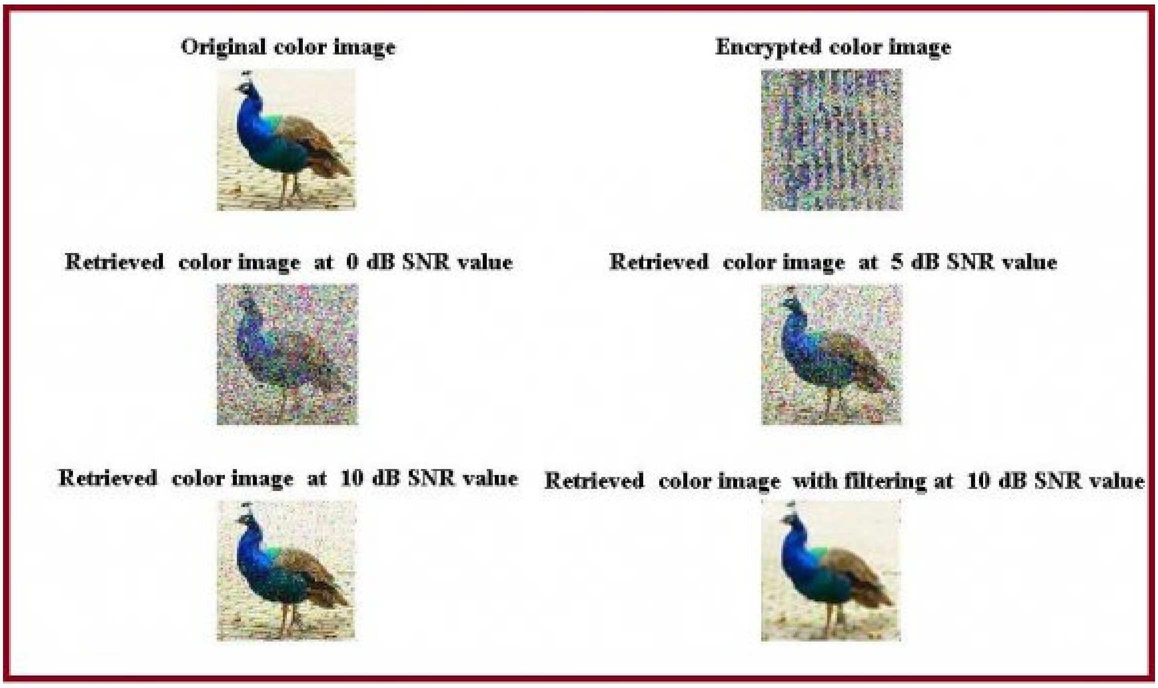
12

Figure 4: Table 1 :Figure 2 :



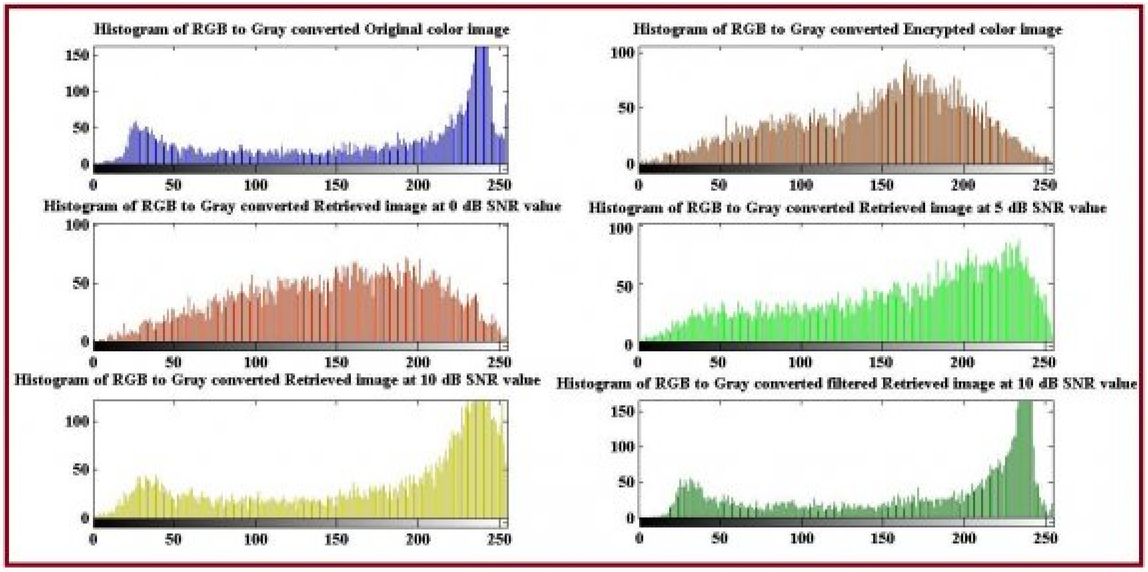
341

Figure 5: Figure 3 :Figure 4 : 1 A



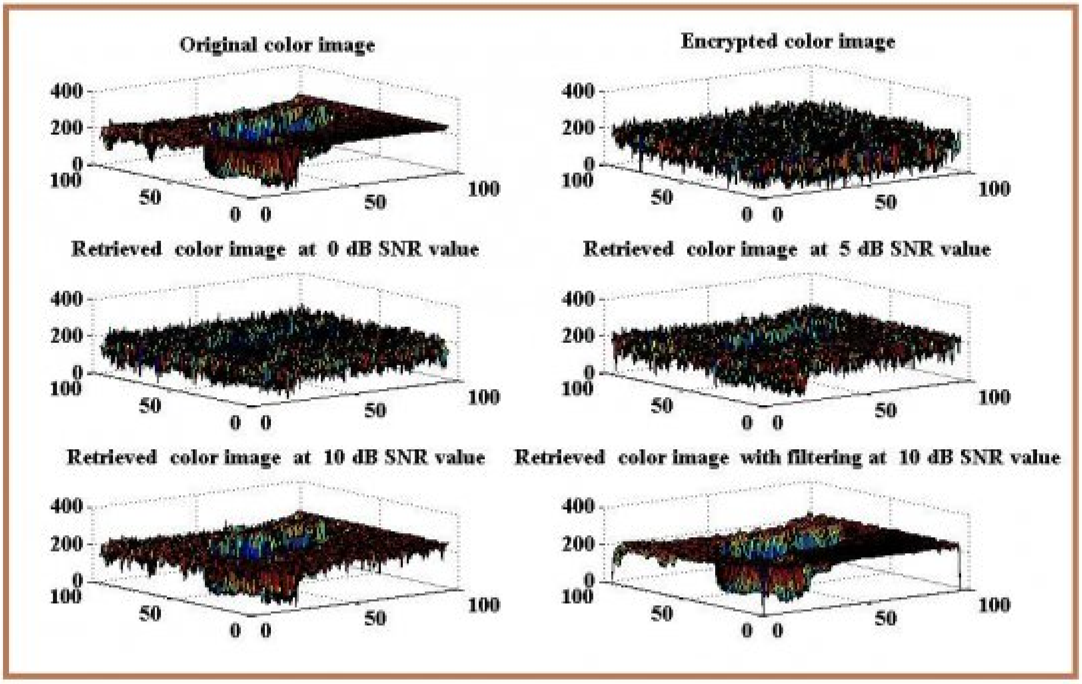

5

Figure 6: Figure 5 :




6

Figure 7: Figure 6 :




7

Figure 8: Figure 7 :

Figure 9:

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

[Jiang ()] *A Practical Guide to Error-ControlCoding Using MATLAB*, Yuan Jiang . 2010. Norwood, MA, USA: Artech House.

[Yaacoub and Al-Husseini ()] 'Achieving Physical Layer Security with Massive MIMO Beamforming'. Elias Yaacoub , Mohammed Al-Husseini . *European Conference on Antennas and Propagation (EUCAP)*, 2017. p. .

[Cho et al. ()] Yong Soo Cho , Jackson Kim , Won Young Yang , Chung G Kang . *MIMO-OFDM Wireless Communications with MATLAB*, (Singapore) 2010. John Wiley and Sons.

[Baiand and Choi ()] 'Low Complexity MIMO Detection'. Lin Baiand , Jinho Choi . *LLC* 2012. Springer Science and Business Media.

[Fang Xiaojie et al. ()] *MP-WFRFT and Constellation Scrambling Based Physical Layer Security System*, Fang Xiaojie , L I Sha Xuejun , Yue . 2016. p. .

[Chen et al. ()] *On Physical Layer Security: Weighted Fractional Fourier Transform based User Cooperation*, Dajiang Chen , Xuejun Sha , Xuemin ( Sherman) Shen , Xiaojie Fang , Ning Zhang , Shan Zhang . 2017.

[Zhou et al. ()] *Physical Layer Security in Wireless Communications*, Xiangyun Zhou , Lingyang Song , Yan Zhang . 2014. Florida, USA: CRC Press. Taylor and Francis Group

[Marques ()] *Practical Image and Video Processing Using MATLAB*, Oge Marques . 2011. New Jersey, USA: John Wiley and Sons.

[Mei et al. ()] 'The Approach to Carrier Scheme Convergence Based on 4-Weighted Fractional Fourier Transform'. Lin Mei , Nai-Tong Xue-Junsha , Zhang . *IEEE COMMUNICATIONS LETTERS* 2010. 14 (6) p. .

[Mei et al. ()] 'The Approach to Carrier Scheme Convergence Based on4-Weighted Fractional Fourier Transform'. Lin Mei , Sha Xue-Jun , Nai-Tong Zhang . *IEEE Communications Letters* 2010. 14 (6) p. .

[Rappaport ()] *Wireless communications*, T S Rappaport . 1996. Upper Saddle River, New Jersey, USA: Prentice Hall. 1. (st ed.)

[Xiang and Zheng ()] 'Xuemin (Sherman) Shen'. Kan Xiang , Zheng . *5G Mobile Communications*, (Switzerland) 2017. Springer International Publishing company.