AIVP ADVANCES IN IMAGE AND VIDEO PROCESSING
SOCIETY FOR SCIENCE AND EDUCATION UNITED KINGDOM
VOLUME 7, ISSUE 4
ISSN 2054-7412

Encrypted Color Image Transmission in LQ-based GSIC Pre-coded Multiuser Downlink Wireless Communication System

[1]Md. Omor Faruk and [2]Shaikh Enayet Ullah
[1,2]Department of Electrical and Electronic Engineering, Faculty of Electrical and Computer Engineering, University of Rajshahi, Rajshahi-6205, Bangladesh.
omor.apee91@gmail.com, enayet_apee@ru.ac.bd

ABSTRACT

The use of LQ-Based GSIC pre-coding scheme in next generation cellular mobile network can be a robust and effective technique for unique cancellation of multiuser interference. In 5G/beyond 5G a great emphasis is being given on ensuring physical layer security. In this paper, an investigative study has been made on the performance evaluation of encrypted color image transmission in LQ-based GSIC pre-coded multiuser downlink wireless communication system. The 6×2 multi-antenna configured simulated system under investigation incorporates SPC (3, 2) channel coding, low order digital modulations (QAM, QPSK, DQPSK), DNA and sine map based RGB image encryption and Zero Forcing (ZF) signal detection techniques. In the scenario of encrypted multiuser color image transmission over AWGN and Rayleigh fading channels, it is observable that the simulative system is very much effective and robust in retrieving color image for each of the three users under a moderate signal to noise ratio of 10 dB.

Keywords: LQ-Based GSIC pre-coding, DNA and sine map based RGB image encryption, Zero Forcing (ZF), SPC (3, 2), Signal to Noise Ratio (SNR).

1 Introduction

Capacity of communication systems through the use of spatial signal processing with requirement of solving complex task of developing new signal processing algorithms is significantly and effectively increased with the utilization of MIMO technology [1]. Multi-user MIMO (MU-MIMO) has become one of the key technologies of 5th-Generation (5G) networks. Millimeter wave (mmWave) communication which explores shorter propagation distance in frequency band of 20–40 GHz is a key enabler for the fifth generation (5G) mobile communication systems. The mmWave communication also provides significant benefits to a variety of applications such as vehicular communication, wire-able networks and autonomous robots. The MU-MIMO technology can effectively utilize spatial resources to improve the throughput of wireless communication systems without consuming additional spectral bandwidths. The MU-MIMO wireless communication system provides substantial downlink throughput in millimeter wave (mmWave) communication. In the MU-MIMO system, multiple users can use the same frequency simultaneously to receive the data from the BS, and it is necessary to eliminate inter-user interference by precoding [2, 3]. Recently, a New Radio (NR) structure has been

DOI: 10.14738/aivp.74.6644
Publication Date: 21st June, 2019
URL: http://dx.doi.org/10.14738/aivp.74.6644

proposed for fifth generation (5G) mobile radio systems to support higher data rates and low latency scenarios. High bandwidth and low bandwidth transmissions utilizing both cmWave and mmWave radio frequencies (3.4 to 3.6 GHz below 6GHz and then 24.25 to 27.5 GHz, 27.5 to 29.5 GHz, 37 GHz, 39 GHz and 57 to 71 GHz are supported in designing 5G NR (new radio). The performance of 5G New Radio (5GNR) using precoding are being studied extensively for Interference Alignment (IA) [4, 5]. As no specific 5G compatible Radio interface technology has been defined, the present study is confined with the performance evaluative study of MU-MIMO system with implementation of LQ-Based Cascade GSIC precoding Algorithm for suppressing MU interference and obtaining the low-triangular MU-MIMO channel effect for each of three receiving users [6].

2 Signal Processing Techniques

In our present study, 2.1 (3, 2) SPC Channel Coding for FEC correction and LQ-based Generalized Side-information Cancellation (GSIC) Precoding for inter user interference reduction schemes have been used. A brief description is given below.

2.1 (3, 2) SPC Channel Coding

In SPC channel coding, the transmitted binary bits are rearranged into very small code words consisting of merely two consecutive bits. In such coding, (3, 2) SPC code is used with addition of a single parity bit to the message u = [u0, u1] so that the elements of the resulting code word x = [x0, x1, x2] are given by x0 = u0, x1 = u1 and x2 = u0 ⊞ u1

Where, ⊞ denotes the sum over GF (2) [7]

2.2 LQ-based Generalized Side-information Cancellation (GSIC) Precoding

LQ-based GSIC precoder exhibits superior performance in cancelling MU interference. In our presently considered downlink transmission scenario, three users each of which is equipped with two receiving antennas are receiving signals from BS with six transmitting antennas. The channel assigned for three users are designated by H1, H2 and H3. The channel matrix H can be undergone LQ decomposition as follows:

$$H = [H_1^T \;\; H_2^T \;\; H_3^T \;]^T = LQ \tag{1}$$

Where, L is a lower triangular matrix and Q is a unitary matrix. The channel matrix H can be rewritten as

$$H = \begin{bmatrix} H_1 \\ H_2 \\ H_3 \end{bmatrix} = \begin{bmatrix} L_{11} & 0 & 0 \\ L_{21} & L_{22} & 0 \\ L_{31} & L_{32} & L_{33} \end{bmatrix} \begin{bmatrix} Q_1 \\ Q_2 \\ Q_3 \end{bmatrix} = \begin{bmatrix} L_{11}Q_1 \\ L_{21}Q_1 + L_{21}Q_2 \\ L_{31}Q_1 + L_{32}Q_2 + L_{33}Q_3 \end{bmatrix} \tag{2}$$

The unitary matrix **Q** has three orthogonal unitary matrices as

$$Q = \begin{bmatrix} Q_1 \\ Q_2 \\ Q_3 \end{bmatrix} \tag{3}$$

Where, L_{11}, L_{22} and L_{33} are triangular matrices; L_{21}, L_{31} and L_{32} are full-rank matrices; Q_1, Q_2, and Q_3 are orthogonal unitary matrices. The received data matrix can be represented by

$$y=\begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix}=\begin{bmatrix} L_{11}Q_1 \\ L_{21_1}Q_1+L_{22}Q_2 \\ L_{31}Q_1+L_{32}Q_2+L_{32}Q3 \end{bmatrix}\begin{bmatrix} P_1 & P_2 & P_3 \end{bmatrix}\begin{bmatrix} s_1 \\ s_2 \\ s_3 \end{bmatrix}+\begin{bmatrix} w_1 \\ w_2 \\ w_3 \end{bmatrix} \quad (4)$$

Where,

$$y_1 = L_{11}Q_1P_1s_1 + L_{11}Q_1P_2s_2 + L_{11}Q_1P_3s_3 + w_1 \quad (5a)$$

$$y_2 = L_{21}Q_1P_1s_1 + L_{22}Q_2P_1s_1 + L_{21}Q_1P_2s_2 + L_{22}Q_2P_2s_2 + L_{21}Q_1P_3s_3 + L_{22}Q_2P_3s_3 + w_2 \quad (5b)$$

$$y_3 = L_{21}Q_1P_1s_1 + L_{32}Q_2P_1s_1 + L_{33}Q_3P_1s_1 + L_{31}Q_1P_2s_2 + L_{32}Q_2P_2s_2 + L_{33}Q_3P_2s_2 + L_{31}Q_1P_3s_3 + L_{32}Q_2P_3s_3 + L_{33}Q_3P_3s_3 + w_3 \quad (5c)$$

And w_1, w_2 and w_3 are AWGN noises. The optimal cancellation matrix Z_1 can beobtained from the following equation:

$$Z_1 = \left(L_{22}^H L_{22} + \frac{(N_1+N_2+N_3)\sigma_w^2}{P_{Total}} I\right)^{-1}\left(L_{22}^H L_{21}\right)$$

Where,$T_r(Q_K^H Q_K) = N_K$, k=1,2,3, PTotal is the total transmitted power and $\sigma^2 w$ is the noise variance estimated from a typically assumed noise floor power(-92dBm/6.31×10^{-13} watt).

Using estimated value of optimal cancellation matrix Z_1, $\tilde{L}_{31}$ is estimated from the relation

$$\tilde{L}_{31} = L_{31} - L_{32}Z_1 \quad (7)$$

The optimal cancellation matrices Z_2 and Z_3 are calculated from the relation

$$Z_2 = (L_{33}^H L_{33} + \frac{N_2\sigma_w^2}{P_{Total}} I)^{-1}(L_{33}^H \tilde{L}_{31}) \quad (8)$$

$$Z_3 = (L_{33}^H L_{33} + \frac{N_3\sigma_w^2}{P_{Total}} I)^{-1}(L_{33}^H L_{32}) \quad (9)$$

The scaling factor β for constraining the total transmit power can be written as:

$$\beta = \sqrt{P_{total}}\{N_1+N_2+N_3+\mathrm{tr}(Z_1Z_1^H)+\mathrm{tr}(Z_2Z_2^H)+\mathrm{tr}(Z_3Z_3^H)\}^{-\frac{1}{2}} \quad (10)$$

The three-user precoding matrices with the transmit power constraint can be expressed as [6]:

$$P_1 = \beta(Q_1^H - Q_2^H Z_1 - Q_3^H Z_2) \quad (11a)$$

$$P_2 = \beta(Q_2^H - Q_3^H Z_3) \quad (11b)$$

$$P_3 = \beta(Q_3^H) \quad (11c)$$

2.3 DNA and Sine Map based RGB image encryption

DNA cryptogram utilizes DNA as information carrierand takes advantage of biological technology to achieve encryption. A DNA sequence contains four nucleic acid bases A .adenine/, C .cytosine/, G .guanine/, T .thymine/, where A and T are complementary, and G and C are complementary. In the binary, 0 and 1 are complementary, so 00 and 11 are complementary, 01 and 10 are also

complementary. C, A, T, G are used to denote 00, 01, 10, 11, respectively.With the development of computer network technology, digital image is widely used in various sectors of our society. As the security of image is threatened seriously due to openness of the network, a great emphasis is being given on image encryption to ensure security of images. However,

DNA computing has permeated the domain of cryptography. As each pixel of R,G,B components of color image consists of 8 bits, it can be expressed as a DNA sequence whose length is 4.In RGB image encryption algorithm based on DNA encoding without using any keys, the RGB image may be spilt up into R, G, B components and each pixel of the decomposed matrixes of R, G, B are transformed into to binary matrices R(m, n×8), G(m, n×8) and B(m, n× 8) and subsequently three DNA sequence matrixes Ar(m, n× 4), Ag(m, n× 4)and Ab(m, n× 4) are formed for R, G and B components. In DNA addition operation (module 2 XOR operation), the modified form of sequences for the whole R, G and B components are:

$$Ar^1(i,j)=Ar(i,j)\oplus Ag(i,j)$$
$$Ag^1(i,j)=Ag(i,j)\oplus Ab(i,j) \quad (12)$$
$$Ab^1(i,j)=Ag^1(i,j)\oplus Ab(i,j)$$

where, i=1,2,3…….nrow and j= =1,2,3…….ncol ; nrow and ncol are the number of rows and number of columns of the color image respectively [8].

In sine map based image cryptosystem, standard sine map (SSM) has drawbacks of small key space, weak security, poor efficiency and low complexity.

Its modified form through adding a parameter to the map equation can be written as:

$$x_{n+1} = \lambda \sin(\pi x_n) + p \quad (13)$$

Where, x_n values are restricted to the interval of $[1/\alpha, 1-(1/\alpha)]$ with $2 < \alpha < \infty$. In Equation (13), the maximum point occurs at x_n=0.5 and its value is $\lambda + p$, while the minimum occurs at $x_n = 1/\alpha$ and its value is $\lambda \sin(\pi/\alpha) + p$

$$\lambda = \frac{\alpha - 2}{\alpha\left[1 - \sin\frac{\pi}{\alpha}\right]} \text{ and } p = \frac{\alpha - 1}{\alpha} + \frac{2 - \alpha}{\alpha\left[1 - \sin\frac{\pi}{\alpha}\right]}$$

Equation (13) can be written as:

$$x_{n+1} = \frac{\alpha - 2}{\alpha\left[1 - \sin\frac{\pi}{\alpha}\right]}.[\sin((\pi x_n) - 1] + \frac{\alpha - 1}{\alpha} \quad (14)$$

Equation (14) is used to get secret key value for each pixel. Considering α=300, $x_0 = 0.123456789$, a nrow×ncol number of secret key values (x_n) are generated for each of R, G, B components.

The encrypted keys for R, G, B components are [9]

$$K_R=\text{mod}(\text{round}(x_n\times\lambda_1),256)$$
$$K_G=\text{mod}(\text{round}(x_n\times\lambda_2),256) \quad (15)$$
$$K_B=\text{mod}(\text{round}(x_n\times\lambda_3),256)$$

Where, $\lambda_1 == 2.5\times10^9$, $\lambda_2 = 1.5\times10^9$ and $\lambda_3 = 1.0\times10^9$

Using pixel wise XOR operation, DNA and sine map based encrypted pixel take the following form:

$$K_{RR}=Ar^1 \oplus K_R$$
$$K_{GG}= Ag^1 \oplus K_G \quad (16)$$
$$K_{BB}=Ab^1 \oplus K_B$$

3 System Description

The key concept underlying the transmission mechanism of our proposed LQ-based GSIC pre-coded multiuser downlink wireless communication system is briefly illustrated in Figure 1. Each user is sending identical 200 pixels (width) ×133 pixels (height) in size RGB color image. Each color image is encrypted, channel encoded, interleaved and subsequently processed for generating complex digitally modulated symbols [10]. The signal vector is reshaped and precoded with implementation of LQ-Based GSIC algorithm. The precoded signals for all the users are summed up and D/A converted and sent up from the transmitting antennas. In receiving section, all the transmitted signals are detected with linear signal detection schemes and the detected signals are subsequently sent up to the Analog to Digital (A/D) converter and subsequently restructured for processing to eliminate the effect of precoding. The processed signal digitally demodulated, deinterleaved, channel decoded, image decrypted and eventually color image is retrieved

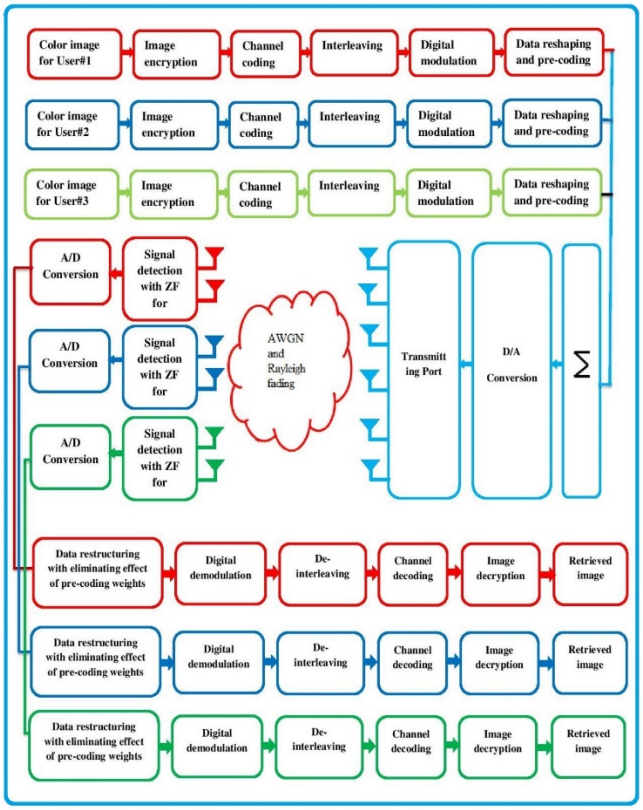

Figure 1: Block diagram of Encrypted Color image transmission in LQ-based GSIC pre-coded multiuser downlink wireless communication system.

4 Result and Discussion

In this part of this paper, the system performance in terms of simulated BER results using MATLAB R2018a have been presented to assess critically the performance analysis of LQ-based GSIC Pre-coded multiuser downlink wireless communication system. . The present study is based on the assumption that the Channel state information (CSI) of the Non geometrical MIMO Rayleigh fading channel is available at the receiver and the fading channel coefficients are constant during simulation. The proposed model is simulated to evaluate the system performance under consideration of the parameters presented in Table 1.

Table 1. Summary of the Simulated Model Parameters

Data type	Color image (200×133)
Antenna configuration for each user	6-by-2
Channel Coding	SPC (3, 2) channel coding
Data Modulation	QAM, QPSK and DQPSK
Pulse shaping filter	Raised cosine with rolloff 0.25 and filter order 22
Image Encryption	DNA and Sine Map based RGB image encryption
Precoding scheme	LQ-based Generalized Side-information Cancellation (GSIC) Precoding
Signal detection Scheme	Zero Forcin (ZF)
Channel	AWGN and Rayleigh fading
Signal to noise ratio (SNR)	0 to 10dB

The estimated total transmitted and total received powers at different users are presented in Table 2. It is ratified that the LQ-Based GSIC pre-coding scheme is very much effective in cancelling out user interference.

Table 2: Estimated total transmitted and received powers

Total transmitted power(watt)	0.333
Total received power at user#1 (watt)	0.2770
Total received power at user#2 (watt)	0.0445
Total received power at user#3 (watt)	0.1048
Total user 1 received interference signal power (watt)	8.0053×10^{-33}
Total user 2 received interference signal power (watt)	4.3226×10^{-24}
Total user 3 received interference signal power (watt)	1.8173×10^{-25}

It is keenly observed that the result of the system provides comparatively better performance under the implementation of QAM modulation technique from the graphical illustration presented in Figure 2 to Figure 4.

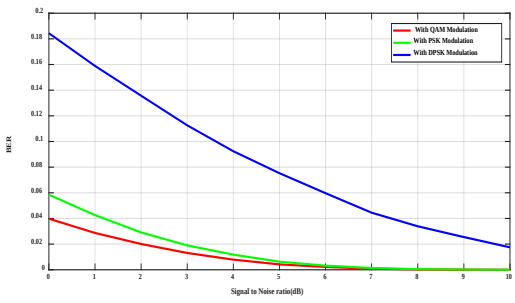

Figure 2: BER performance of Encrypted Color image transmission in LQ-based GSIC pre-coded multiuser downlink wireless communication system for user#1 under implementation of different low order digital modulation.

It is seen from Figure 2 that for a typically assumed SNR value of 1dB, the estimated BER values are 0.0287, 0.0426 and 0.1589 In case of QAM,QPSK and DQPSK digital modulations which is indicative of system performance of 7.43 dB and 5.72 dB in case of DQPSK relative to QAM and DQPSK relative to QPSK.

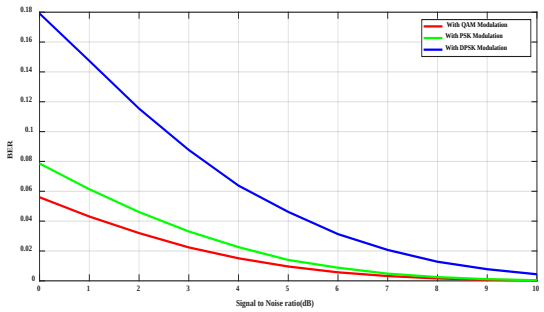

Figure 3: BER performance of Encrypted Color image transmission in LQ-based GSIC pre-coded multiuser downlink wireless communication system for user#2 under implementation of different low order digital modulation.

It is observable from Figure 3 with identical consideration of SNR value (1dB), the estimated BER values are 0.0431, 0.0614 and 0.1474 In case of QAM, QPSK and DQPSK digital modulations which is indicative of system performance of 5.34 dB and 3.80 dB in case of DQPSK relative to QAM and DQPSK relative to QPSK.

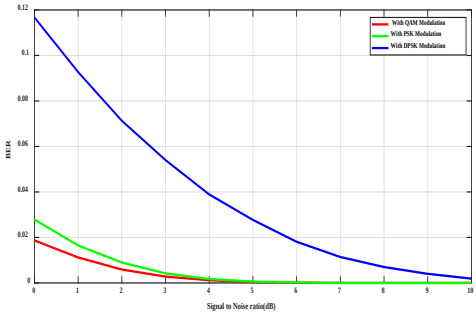

Figure 4: BER performance of Encrypted Color image transmission in LQ-based GSIC pre-coded multiuser downlink wireless communication system for user#3 under implementation of different low order digital modulation.

It is quite obvious from Figure 4 with consideration of SNR value 1dB, the estimated BER values are 0.0112, 0.0165 and 0.0927 In case of QAM, QPSK and DQPSK digital modulations which is indicative of system performance of 9.18 dB and 7.50 dB in case of DQPSK relative to QAM and DQPSK relative to QPSK. It is observable from Figure 5 that the transmitted color images are uniquckly encrypted. It is very much clear from Figure 6 through Figure 8 that the quality of the retrieved images improves with increase in SNR values.

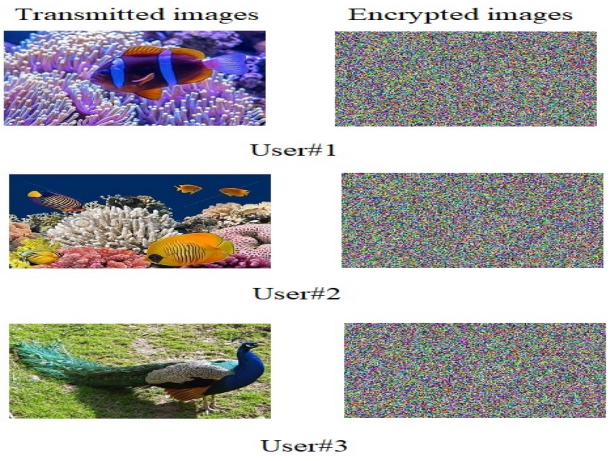

Figure 5: Transmitted and Encrypted images for different users

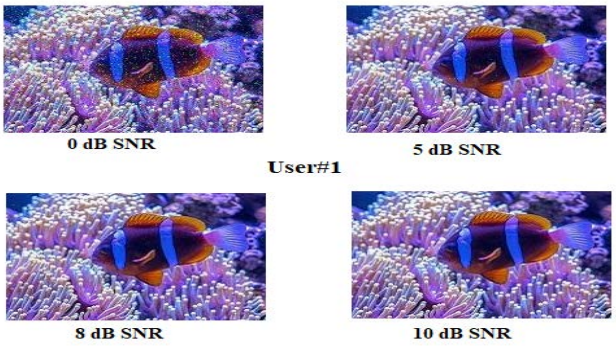

Figure 6: Retrieved Color images of user#1 at different SNR values.

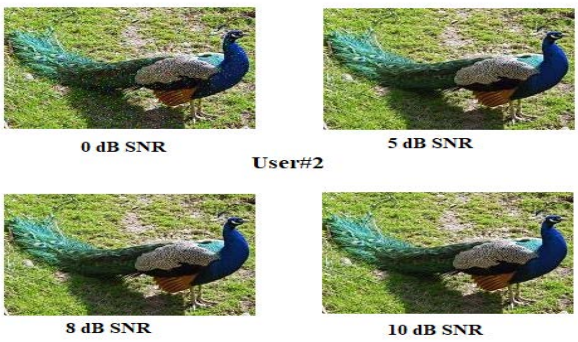

Figure 7: Retrieved Color images of user#2 at different SNR values.

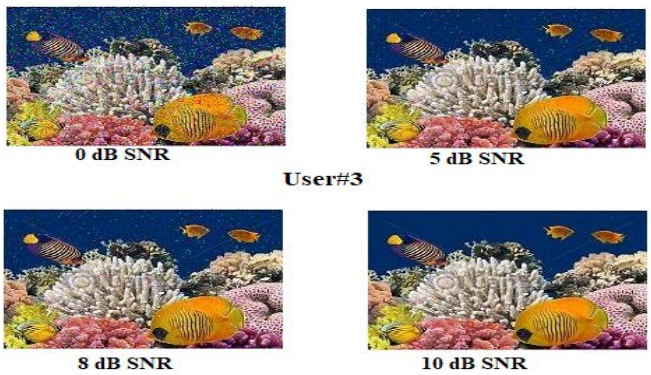

Figure 8: Retrieved Color images of user#2 at different SNR values.

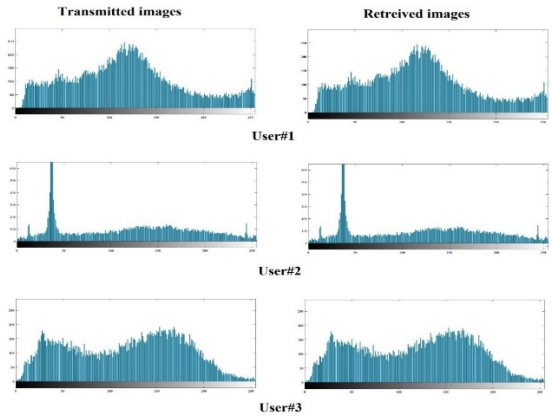

Figure 9: Histogram of RGB to Gray converted Transmitted and Retrieved color image at SNR value of 10 dB for user#1, user#2 and user #3.

The histograms presented in Figure 9 clearly show the distribution of pixel values of RGB to Gray converted retrieved color images.

5 Conclusion

In this paper, an investigative study has been made on the performance evaluation of encrypted color image transmission in LQ-based GSIC pre-coded multiuser downlink wireless communication system. The 6×2 multi-antenna configured simulated system under investigation incorporates SPC (3, 2) channel coding, low order digital modulations (QAM, QPSK, DQPSK), DNA and sine map based RGB image encryption and Zero Forcing (ZF) signal detection techniques. In the scenario of encrypted multiuser color image transmission over AWGN and Rayleigh fading channels, it is observable that the simulative system is very much effective and robust in retrieving color image for each of the three users with QAM modulation technique under a moderate signal to noise ratio of 10 dB.

From critical analysis of the simulated results, it can be concluded that such LQ-based GSIC pre-coded multiuser downlink wireless communication can be effectively used in future generation wireless communication networks.

REFERENCES

[1]. V.B. Kreyndelin; Taoufik Ben Rejeb; M. G. Bakulin, *Novel Efficient Precoding Technique with Reduced Feedback for Multiuser MIMO Systems with Multiple Antenna User Equipment*, In Proceeding of IEEE Conference on Systems of Signals Generating and Processing in the Field of on Board Communications, Moscow, Russia, 2019. p. 1-5. https://ieeexplore.ieee.org/abstract/document/8706795/

[2]. Su Pan ,Yan Yan ,Kusi Ankrah Bonsu and Weiwei Zhou, *Resource Allocation Algorithm for MU-MIMO Systems Wth Double-Objective Optimization Under the Existence of the Rank Deficient Channel Matrix*, IEEE Access, 2019 vol. 7, pp. 61307 – 61319. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8710242

[3]. Adam Mohamed Ahmed Abdo, Xiongwen Zhao, Rui Zhang, Zhenyu Zhou, Jianhua Zhang, , Yu Zhang, and Imran Memon, *MU-MIMO Downlink Capacity Analysis and Optimum Code Weight Vector Design for 5G Big Data Massive Antenna Millimeter Wave Communication*, Wireless

Communications and Mobile Computing, 2018. p. 1-12. https://www.hindawi.com/journals/wcmc/2018/7138232/

[4]. Khawla A. Alnajjar, Mohamed El-Tarhuni, *Performance of 5G NR with Interference Aligment,* In proceeding of IEEE International Conference on Communication, Signal Processing, and their Applications (ICCSPA), Sharjah, United Arab Emirates, 2019. p. 1-4. https://ieeexplore.ieee.org/document/8713752

[5]. https://www.electronics-notes.com/articles/connectivity/5g-mobile-wireless-cellular/5g-nr-new-radio.php

[6]. Juinn-horngdeng, Kuang-min lin,and Meng-lin ku, *Precoding Design for Multiuser MIMO Downlink Communication Systems Using an LQ-Based Cascade GSIC Algorithm*, IEEE Access, 2017. vol. 5. p. 20578- 20589. https://ieeexplore.ieee.org/document/8051043

[7]. Giorgio M. Vitetta, Desmond P. Taylor, Giulio Colavolpe, Fabrizio Pancaldi and Philippa A. Martin, *Wireless Communication; Algorithmic Techniques*, John Wiley and Sons Ltd, United Kingdom, 2013.p. 744. https://onlinelibrary.wiley.com/doi/book/10.1002/9781118576618

[8]. Lili Liu, Qiang Zhang and Xiaopeng Wei, *A RGB image encryption algorithm based on DNA encoding and chaos map*, Computers and Electrical Engineering, 2012. vol.38. p. 1240–1248. https://www.sciencedirect.com/science/article/pii/S0045790612000201

[9]. Hidayet Oğraş and Mustafa Türk, *A Secure Chaos-based Image Cryptosystem with an Improved Sine Key Generator*, American Journal of Signal Processing, 2016. vol.6(3). p.67-76. http://article.sapub.org/10.5923.j.ajsp.20160603.01.html

[10]. Theodore S Rappaport, Second Edition, 2002: *Wireless Communications Principles and Practice* (New York, USA) pp. 736. https://www.academia.edu/9079804/Wireless_Communications-_Principles_And_Practice_by_Theodore_S_Rappaport