Journal of Multidisciplinary Engineering Science and Technology (JMEST)
ISSN: 2458-9403
Vol. 3 Issue 6, June - 2016

Secure Color Image Transmission over WIMAX Communication System

Md. Polas Tai
Dept. of ICE, University of Rajhahi,
Rajshahi-6205, Bangladesh
e-mail:polashice999@gmail.com

Farhana Enam
Assistant Professor
Dept. of ICE, University of Rajshahi
Rajshahi-6205, Bangladesh
e-mail: farhana_ice2008@yahoo.com

Md. Ashraful Islam
Assistant Professor
Dept. of ICE, University of Rajshahi
Rajshahi-6205, Bangladesh
e-mail: ras5615@gmail.com

Md. Arifur Rahman
Lecturer
Dept. of EEE, FCUB
Chuadanga-7200, Bangladesh
e-mail: uzzalruapee@gmail.com

***Abstract*—we live in an information technology age, we generate and process information at a rate never before recorded in the history of mankind. This has led to an ever increasing need to develop wireless access technologies that support high throughput regardless of the transmission environment. WiMAX (Worldwide Interoperability for Microwave Access) is a promising technology which can offer high speed voice, video and data service up to the customer end. Security is crucial to a wide range of Wireless data application and service. This research work presents a simulation based work of a wireless communication system with implementing of the secured asymmetric RSA cryptographic Algorithm for color image transmission. The key contribution of this research work was the implementation of the WiMAX communication to evaluate the system performance under AWGN, Rayleigh fading channel and Rician fading channel under 16-QAM modulation technique for the secure transmission of color image. Developing and understanding of the WiMAX communication system for secure color image transmission can be achieved by the communication model of the WiMAX physical layer using computer simulation using Matlab simulation software version R2009a. This research work presents, when SNR value is 0dB, all channel performance is weird. For SNR value 20dB, it is observed that, the original transmitted image is not received perfectly through AWGN channel, Rayleigh fading channel and Rician fading channel. For SNR value 40dB, it is seen that, the original transmitted image is received perfectly through AWGN channel, but not perfectly received through Rayleigh fading channel and Rician fading channel. For SNR value 45dB, it is seen that, the original transmitted image is retrieved perfectly through Rician fading channel, but not Rayleigh fading channel. This research work for 16QAM modulation technique shows that, the color image is transmitted securely with low SNR value over AWGN communication channel.**

Keywords—WiMAX; RSA; Color Image; Security Algorithm; Fading Channel

I. INTRODUCTION

WiMAX stands for Worldwide Interoperability for Microwave Access. WiMAX technology is a telecommunications technology that offers transmission of wireless data via a number of transmission methods; such as portable or fully mobile internet access via point to multipoint links [1, 2]. WiMAX is a wireless digital communications system, also known as IEEE 802.16 that is intended for wireless "metropolitan area networks". WiMAX can provide broadband wireless access (BWA) up to 30 miles (50 km) for fixed stations, and 3 - 10 miles (5 - 15 km) for mobile stations. In contrast, the Wi-Fi/802.11 wireless local area network standard is limited in most cases to only 100 - 300 feet (30 - 100m). With WiMAX, Wi-Fi like data rates are easily supported, but the issue of interference is lessened [3]. WiMAX operates on both licensed and non-licensed frequencies, providing a regulated environment and viable economic model for wireless carriers. WiMAX can be used for wireless networking in much the same way as the more common Wi-Fi protocol. WiMAX is a second-generation protocol that allows for more efficient bandwidth use, interference avoidance, and is intended to allow higher data rates over longer distances. Orthogonal frequency-division multiplexing (OFDM) [7] is used in most recent WiMAX communications systems due to its high spectrum efficiency and robustness in multi-path propagation. OFDM is a special form of multi-carrier modulation and mitigate inter symbol interference (ISI) by multiplexing the data on orthogonal property [2]. Security is always important in data networks, but it is

particularly critical in wireless networks such as WiMAX. Authentication is the first element in wireless security that, if not well safeguarded, all following security measures will be vulnerable. Denial of Service, Brute Force, Mathematical attack, Timing attack, Chosen cipher text attack are the attacks that could target a WiMAX network to make its operation inefficient[4].

The main objective of this paper is to enhance the security of transmitted data over WiMax Communication system. In this work to use the public key encryption algorithm that encrypted the transmitted data at the transmitter section and the receiver section we decrypted the transmitted data then we get the original data. If we are not perform the correctly decryption then we get wrong data which data is not matched to the input data. The WiMAX system simulator is developed by public key encryption algorithm using MATLAB R2009a in order to have better understanding of the standard and evaluate the performance. The performance evaluation is mainly based on the critical examination of the effects of synthetically generated signal transmission through WiMAX system under AWGN and frequency flat fading (Rayleigh/ Rican) channel using QAM modulations. The aim of this paper is to highlight of the security threats that face today's wireless networks such as WiMAX and try to solution of these threats such as Denial of Service (DoS) attack, Brute Force, Mathematical attack, Timing attack, Chosen ciphertext attack.

II. SECUIRITY ALGORITHM

In my research work, I use RSA algorithm as a public key Encryption Algorithm. The RSA is the most popular public key Encryption Algorithm. Description of RSA is given below:

The scheme developed by Rivest, Shamir, and Adleman makes use of an expression with exponentials. Plaintext is encrypted in blocks, with each block having a binary value less than some number n. That is, the block size must be less than or equal to $\log_2(n)$, in practice, the block size is i bits, where $2^i < n \leq 2^{i+1}$. Encryption and decryption are of the following form, for some plaintext block M and ciphertext block C:

$C = M^e \bmod n$
$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$

Both sender and receiver must know the value of n. The sender knows the value of e, and only the receiver knows the value of d. Thus, this is a public-key encryption algorithm with a public key of PU ={e, n} and a private key of PU = {d, n}. For this algorithm to be satisfactory for public-key encryption, the following requirements must be met:

- It is possible to find values of e, d, n such that $M^{ed} \bmod n = M$ for all M <n.
- It is relatively easy to calculate mod $M^e \bmod n$ and C^d for all values of M <n.
- It is infeasible to determine d given e and n.

For now, we focus on the first requirement and consider the other questions later. We need to find a relationship of the form **$M^{ed} \bmod n = M$.** The preceding relationship holds if e and d are multiplicative inverses modulo f(n), where f(n) is the Euler totient function. It is showing that for p, q prime, $\emptyset(pq)$ **= (p- 1) (q -1).** The relationship between e and d can be expressed as

$ed \bmod \emptyset(n) = 1$

This is equivalent to saying
$ed \equiv 1 \bmod \emptyset(n)$
$d \quad e1 \bmod \emptyset(n)$

That is, e and d are multiplicative inverses mod f(n). Note that, according to the rules of modular arithmetic, this is true only if d (and therefore e) is relatively prime to f(n). Equivalently, gcd(f(n),d) = 1.

Table-1 shows the RSA algorithm. From figure-1 the keys were generated as follows:

1. Select two prime numbers, p = 17 and q = 11.
2. Calculate n = pq = 17 x 11 = 187.
3. Calculate f(n) = (p 1)(q 1) = 16 x 10 = 160.
4. Select e such that e is relatively prime to f(n) = 160 and less than f(n) we choose e = 7.
5. Determine *d* such that *de* 1 (mod 160) and *d* < 160. The correct value is *d* = 23, because 23x 7 = 161 = 10 x 160 + 1; *d* can be calculated using the extended Euclid's algorithm. The resulting keys are public key *PU* = {7,187} and private key *PR* = {23,187}. The example shows the use of these keys for a plaintext input of *M* = 88.

For encryption, we need to calculate $C = 88^7 \bmod 187$ [8]. Exploiting the properties of modular arithmetic, we can do this as follows:

$88^7 \bmod 187 = [(88^4 \bmod 187) \times (88^2 \bmod 187) \times (88^1 \bmod 187)] \bmod 187$

88^1 mod 187 = 88
88^2 mod 187 = 7744 mod 187 = 77
88^4 mod 187 = 59,969,536 mod 187 = 132
88^7 mod 187 = (88 x 77 x 132) mod 187 = 894,432 mod 187 = 11
For decryption, we calculate *M* = 11^{23} mod 187:
11^{23} mod 187 = [(11^1 mod 187) x (11^2 mod 187) x (11^4 mod 187) x (11^8 mod 187) x (11^8 mod 187)] mod 187
11^1 mod 187 = 11
11^2 mod 187 = 121
11^4 mod 187 = 14,641 mod 187 = 55
11^8 mod 187 = 214,358,881 mod 187 = 33
11^{23} mod 187 = (11 x 121 x 55 x 33 x 33) mod 187 = 79,720,245 mod 187 = 88

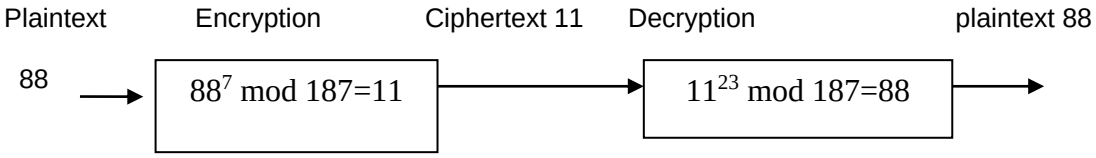


Figure-1: Example of RSA Algorithm

Table-1: The RSA Algorithm [6]

Key Generation	
Select p, q	p, q both prime, $p \neq q$
Calculate $n=p \times q$	
Calculate $\emptyset(n) = (p-1) \times (q-1)$	
Select integer e	gcd $(\emptyset(n), n) = 1$; $1<e<\emptyset(n)$
Calculate d	$d=e^{-1} \pmod{\emptyset(n)}$
Public key	PU = {e, n}
Private key	PR = {d, n}
Encryption	
Plain text	M < n
Cipher text	$C = M^e \bmod n$
Decryption	
Ciphertext	C
Plain text	$M = C^d \bmod n$

III. SIMUATION MODEL

Figure-2 shows the simulation model of a OFDM based WiMAX communication system with the implementation of asymmetric RSA encryption/decryption algorithm for secure color image transmission.In such a communication system, the color image is converted into integer and then encrypted using RSA encryption algorithm. The encrypted data is converted into binary bits and channel encoded using 1/2 rated Convolutional Coder (CC). The encoded bits are subsequently digitally modulated using 16QAM. The modulated data then transmitted over the communication channel. For my research work, I used AWGN and Fadding (Rayleigh & Rician) channel as communication channel [5].The used parameters are listed in Table2 as follows:

The proposed model for WiMAX communication system containing encryption, decryption, transmitter, receiver, and channels in shown in figure-2 is considering the following simulation parameter shown below in table-2.

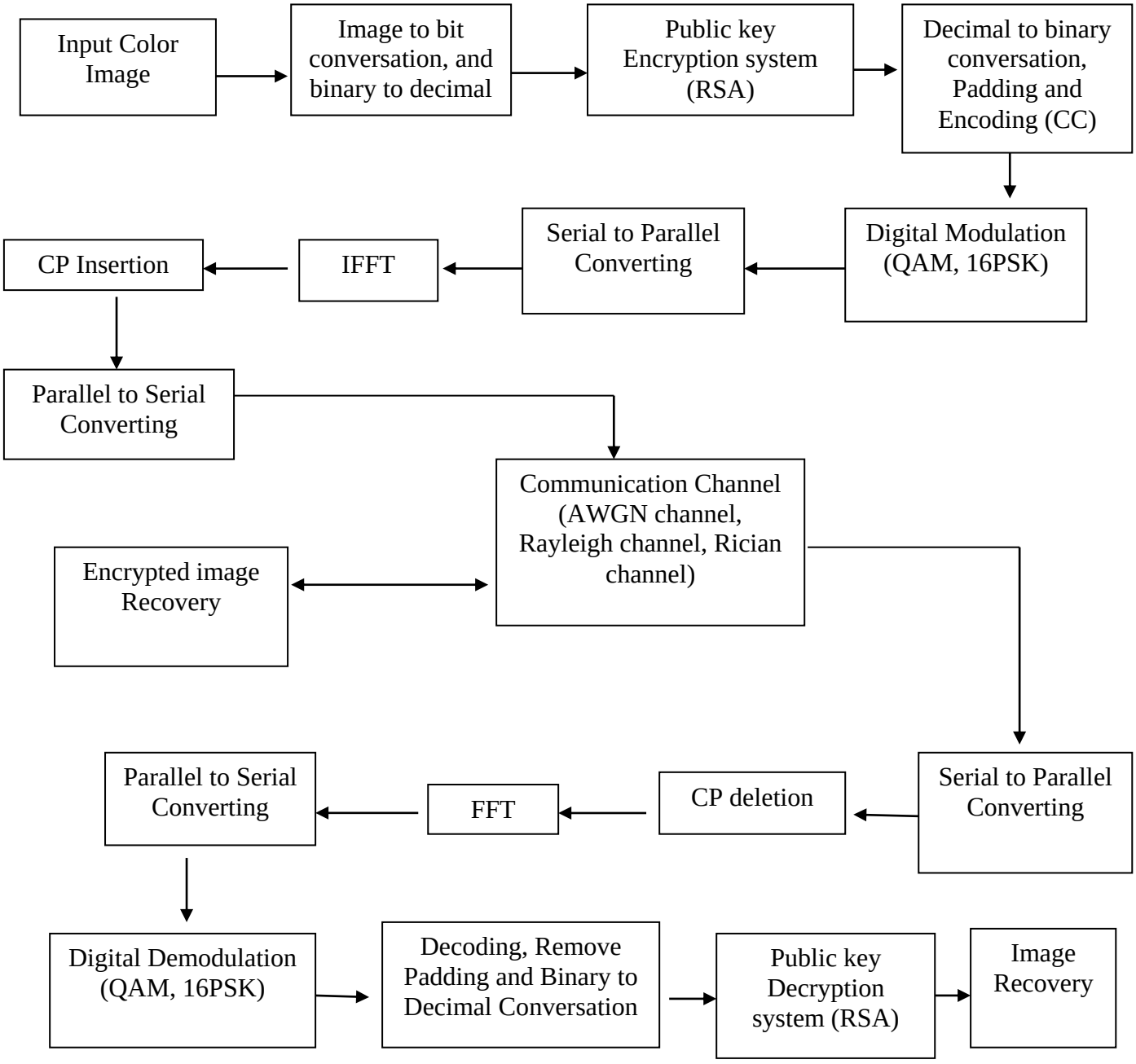


Figure-2: A Block Diagram for the simulation model of WiMAX communication system over transmitting secure color image.

Table -2: Simulation model parameters

Parameter	Values
Input	Color Image
Encryption Algorithm	RSA
FFT Size	1024
CP	1/4
Coding	Convolution Coding (CC)
CC	1/2
Decryption Algorithm	RSA
Modulation	16QAM, 16PSK
SNR	0-60 dB
Noise Channels	AWGN, Rayleigh and Rician
K-factor	3

The procedures that we have followed to develop the WiMAX communication system simulation is briefly stated as follows:
At the transmission section:

1. At first we take color image and converting binary to decimal number which is used for encryption. We using public key encryption algorithm (RSA). Then the encrypted number is converted into bit. This bit is arranged randomization process has been carried out to scramble of 0's or 1's in a random sequence to improve the coding performance.
2. Secondly we have performed ½ rate convolution coding that encoded the data and improve the channel performance.The encoding section was completed by interleaving the encoded data.
3. Then 16QAM digital modulation technique is used to modulate the encoded data.
4. Then we perform the serial to parallel converting where every modulated data is arranged in parallel manner.
5. The modulated data in the frequency domain is then converted into time domaindata by performing IFFT (using Mat lab built in function 'ifft') on it.
6. For reducing inter-symbol interference (ISI) cyclic prefix has been added with the time domain data.
7. Finally the modulated parallel data were converted into serial data stream and transmitted through different communication channels.
8. From the channel we get the data and recovery the image then we get encrypted image .This image not match the input and output image.

At the receiving section, the received complex digitally modulated symbols are first demodulated and then fed to the CC channel decoder. The decoded binary data are converted into integer and decrypted with RSA decryption algorithm. The decrypted data are finally converted into color image.

IV. Simulation Result

This section of the chapter presents and discusses all of the result obtained by the computer simulation program written in MATLAB R2009a, following the analytical approach of a wireless communication system considering AWGN, Rayleigh fading channel and Rician fading channel. The results are represented in terms of BER vs. SNR for practical value of system parameter.

The following figure shows the BER performance of ½ rate convolutional encoded and 16QAM modulated WIMAX communication system for AWGN, Rayleigh fading channel and Rician fading communication channel.

It is viewed from figure-3 that, when transmitted signal is very week, that means when SNR value is 0dB, all channel performance is weird. For SNR value 20dB, it is seen that, the original transmitted image is not received perfectly through AWGN channel, Rayleigh fading channel and Rician fading channel. For SNR value 40dB, it is found that, the original transmitted image is received perfectly through AWGN channel, but not perfectly received through Rayleigh fading channel and Rician fading channel. For SNR value 45dB, it is shownthat, the original transmitted image is retrieved perfectly through Rician fading channel, but

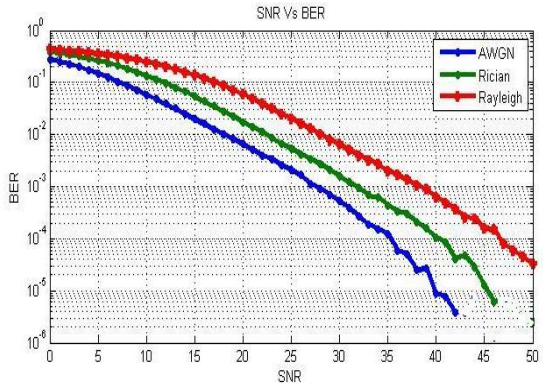
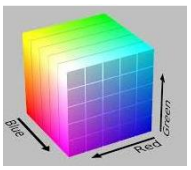
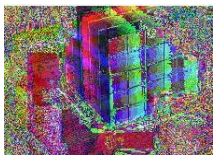
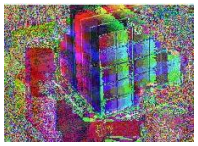
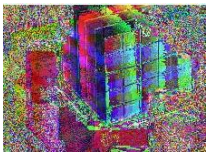


Figure 3: Bit error rate (BER) performance of WiMAX Communication System.

not Rayleigh fading channel. So it can be said that, Rayleigh fading channel has the worst performance of all the three channels for SNR values (0 – 50dB). AWGN and Rician fading channels perform better. We can also say that, better performance of OFDM based WiMAX communication system can be gained for higher value of SNR, while using 16QAM modulation technique.

Table-3 shows the input image and corresponding Encrypted image over different communication channels (AWGN, Rayleigh, Rician) for 16QAM modulation technique.

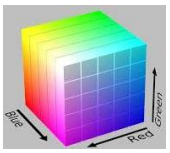
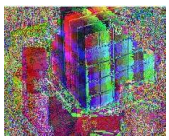
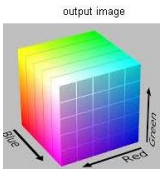
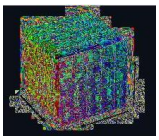
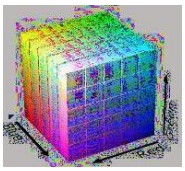
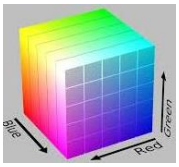
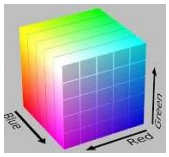
Table 3: Input image and corresponding encrypted for 16QAM modulation.

Input Image	Encrypted image for AWGN channel
	
Encrypted image for Rayleigh channel	Encrypted image for Rician channel
	

From table-3, it is observed that, the resulted encrypted image is same for all communication channels such as AWGN channel, Rayleigh fading channel and Rician fading channel. So we say that encrypted image is independent of communication Channel, it depends on the Encryption Algorithm.

Table-4 shows the input image, corresponding Encrypted image, and retrieved image over AWGN communication channels for different SNR values (0 – 50dB).

Table-4 Input image, corresponding Encrypted image and effect of SNR on the retrieved image over AWGN communication channel.

Input Image	Encrypted Image	Output Image
		
SNR=0 dB	SNR=20 dB	SNR=30 dB
		
SNR=35 dB	SNR=40 dB	SNR=45 dB
		

From table-4, it is observed that the transmitted image is retrieved perfectly for SNR value 40dBover AWGN channel.

Table-5 shows the input image, corresponding Encrypted image, and retrieved image over Rician communication channels for different SNR values (0 – 50dB).

From table-5,it is shown that the transmitted image is retrieved perfectly for SNR value 45dBwhich has the worst performance than AWGN channel..

Table-5 Input image, corresponding Encrypted image and effect of SNR on the retrieved image over Rician communication channel

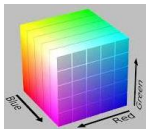
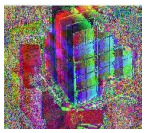
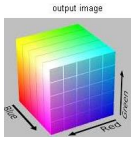
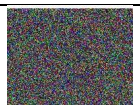
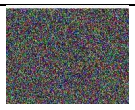
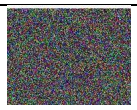
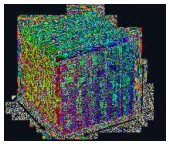
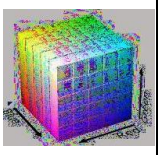
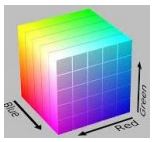
Input Image	Encrypted Image	Output Image
		
SNR=0 dB	SNR=20 dB	SNR=30 dB
		
SNR=35 dB	SNR=40 dB	SNR=45 dB
		

Table-6 Input image, corresponding Encrypted image and effect of SNR on the retrieved image over Rayleigh communication.

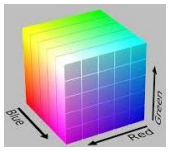
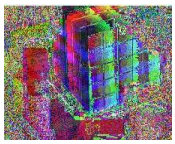
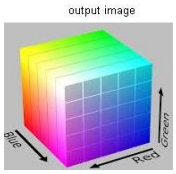
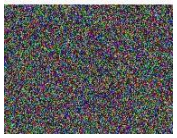
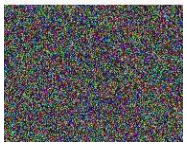
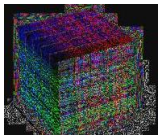
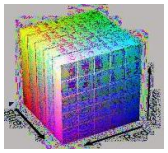
Input Image	Encrypted Image	Output Image
		
SNR=0 dB	SNR=20 dB	SNR=30 dB
		
SNR=35 dB	SNR=40 dB	SNR=45 dB
		

Table-6 shows the input image, corresponding Encrypted image, and retrieved image over Rayleigh communication channels for different SNR values (0 – 50dB).

Table-6 shows thatthe transmitted image is not retrieved perfectly for SNR value 45db in the modulation technique. Rayleigh fading channel has the worst performance as it has highest BER in this modulation technique. This technique required more SNR value. If the transmitted image is retrieved perfectly, we required SNR value at least 55dB for 16QAM modulation technique over Rayleigh fading channel.

V. CONCLUSION

The key contribution of this research work was the implementation of WiMAX communication system using MATLAB in order to evaluate the WiMAX communication performance under AWGN, Rayleigh fading channel and Rician fading channel and under 16QAM modulation technique. In this work, we shown the input image, Encrypted image and output image with the variation of SNR values.

This paper focuses on the performance investigation by bit error rate (BER) against SNR (signal to noise ratio) plots for all the essential modulation techniques under AWGN, Rayleigh fading channel and Rician fading channel. Figure-3 shows the performance of WiMAX communication system using 16QAM modulation technique. From these figure-3 and four tables-3, table-4, table-5, and table-6, conclusions can be drawn about the BER performance evaluation of WiMAX communication system over AWGN, Rayleigh fading channel and Rician fading channel as below:

1. Among the three communication channels, AWGN channel has the best performance as it has lowest BER in the modulation technique (16QAM) as the transmitted image is retrieved perfectly for SNR value 40dB in the modulation technique.

2. Performance of Rician fading channel is worse than that of the AWGN channel and better than that of Rayleigh fading channel for 16QAM modulation technique. The transmitted image is retrieved perfectly for SNR value 45dB in the modulation technique.

3. Among the three communication channels, Rayleigh fading channel has the worst performance as it has highest BER in this modulation technique. The transmitted image is not retrieved perfectly for SNR value 45dB in the modulation technique. This technique required more SNR value. If the transmitted

image is retrieved perfectly, we required SNR value at least 55dB for 16QAM modulation technique.

From table-3, we get that the resulted encrypted image is same for all the communication channel such as AWGN channel, Rayleigh fading channel and Rician fading channel. So we say that encrypted image is independent of modulation technique and communication Channel, it depends on the Encryption Algorithm.

From these discussions we get a result that AWGN channel has lower BER than fading channel such as Rayleigh fading channel and Rician fading channel.

REFERENCES

[1] Yan Zhang and Hsiao-Hwa Chen, "MOBILE WiMAX Toward Broadband Wireless Metropolitan Area Networks", Auerbach Publications Taylor & Francis Group, 2008.

[2] Hung-Yu Wei, Samrat Ganguly, Rauf Izmailov,Zygmunt J. Haas,"Interference-Aware IEEE 802.16 WiMax Mesh Networks", 61st IEEE Vehicular Technology Conference (VTC 2005 Spring), Stockholm, Sweden, May 29-June 1, 2005.

[3] Syed Ahson and Mohammad Ilyas, "WiMAX Standards and Security", CRC Press Taylor & Francis Group, 2008.

[4] Mohhammod Azizul Hasan, "Performance Evaluation of WiMAX/IEEE 802.16 OFDM Physical Layer", Espoo, June, 2007.

[5] Md. Ashraful Islam and A.Z.M. Touhidul Islam "Performance of WiMAX Physical Layer with Variations in Channel Coding and Digital Modulation Under Realistic Channel Conditions", International Journal of Information Sciences and Techniques, IJIST, Vol. 2, pp. 39-47, No. 4, July 2012.

[6] Md. Ashraful Islam and A. Z. M. Touhidul Islam, "Secure Wireless Text Message Transmission with the Implementation of RSA Cryptographic Algorithm", International Journal of Computer Networks and Communications Security, VOL. 2, NO. 5, MAY 2014, 146–151, Available online at: www.ijcncs.org, ISSN 2308-9830.

[7 Sweeney, Daniel, "WiMAX Operator's Manual: Building 802.16 WirelessNetworks", Apress Publishing, May 2004.

[8] William Stalling "Cryptography and Network Security ",4th Edition