International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 8 (2018) pp. 6009-6018

Study of WiMAX Based Communication Channel Effects on the Ciphered Image Using MAES Algorithm

Ahmed G. Wadday, Salim M. Wadi, Hayder J. Mohammed Ali A. Abdullah

Communications Techs. Engineering Department, Al-Furat Alwasat Technical University, Iraq.

Technical Institute of Najaf, Al-Furat Alwasat Technical University

Abstract

Protection of multimedia information from different types of attackers and send it over communication channels has become important for people and governments. The form of reconstructed image from an actual transmission channel is an important challenge faces the ciphering algorithms. MAES algorithm is an important modified version of AES algorithm used to cipher an image with high security level and low computation cost. This paper presents an study of Channel effects on MAES ciphering algorithm. An encrypted image by MAES is transmitted and received over WiMAX standard then check its features. Comparison between original and reconstructed versions of secret image was done. Many parameters such as visual scene, histogram analysis, correlation coefficients and entropy were used to achieve this comparison. The results of study achieved in this work proved that the ciphered algorithm is strong against WiMAX channel problems especially when the SNR of the channel increased.

Keywords: WiMAX, image protection, MAES, channel communications

INTRODUCTION

The secure transmissions for digital images have its importance in today's video conferencing and image communications [1]. Owing to the long-term the increasing growth of digital multimedia and telecommunication services, resources of digital are obtainable for public common accesses. However, the important issue is to keep intellectual property of worthy digital masterwork while Guaranteed the public accessibility [2].

Video and Image encryption have enforcements in diverse fields including medical imaging, Tele-medicine, internet, multimedia and military communication [1]. Many of the cryptographic algorithms have been proposed and widely used such as DES, IDEA, Triple-DES, AES, and RSA etc. In spite of the AES algorithm considers quite resistance versus attacks, channel attack has become the new menace against AES [3]. Wide applications for AES algorithm in our daily life were obtained, such as cell phones, smart cards, WWW servers and automated teller machines. AES is recognized block cipher algorithm and have various features, such as implementation ability and high security level [4].

On the other side, very fast spread of smart phones has produced an growing demand for transfer multimedia over wireless networks. Leading two standards, i.e., IEEE 802.16m WiMAX and LTE- Advanced, fit out high transmission data rates for multimedia of the real-time applications (e.g., video conferencing) that require to transmit vast of data[5, 6]. Worldwide Interoperability for Microwave Access (WiMAX, IEEE 802.16), is a modern wireless channel for broadband applications with transmission in much applications and high bandwidth[7]. WiMAX rising network coverage and improving performance of communication. 802.16 provides extensive coverage area of broadband services. The broadband access could fitting the wanting link for the connection in wireless metropolitan area networks [8].

In present study, performance of our previous proposed algorithm MAES algorithm [9] is evaluated under channel condition. A WiMAX network is used as communication medium in this evaluation operation.

This paper is organized as follows: In section II a brief description of AES algorithm is given. Section III describes the details of WIMAX Standards physical layer. Section IV presents simulation and discussion of results. Paper is ended with conclusion.

AES ALGORITHM

Cryptography is the important process, which plays role in data security. Where customers can store important and sensitive information and then transfer it over insecure networks so that unauthorized people cannot read it.

1. Algorithm: AES is a block cipher well--kown round-based symmetric, where sizes of the input and output are equal are to 128 bits and fixed. The length of AES secret key is flexible and allow key lengths of 128,192 or 256 bits. Primitive four functions are executede in a sequence Nr -1 time compose a loop called a round, SubByte, ShiftRow, MixColumn and AddRoundKey. The iteration number of loop (Nr) may be 14, 12, or 10 consisting on the key size. The operation of the SubByte is a byte nonlinear substitution which perform independently on every byte of the situation using a substitution table. ShiftRow is a circular shifting operation on the rows of the state with various numbers of bytes (offsets). Mixes operation of the bytes in each column through the MixColumn by the multiplication of the state with a fixed polynomial ($3x^3+x^2+x+2$, bx^3+dx^2+9x+e for encryption and

decryption respectively) modulo x4+1. In AddRoundKey process XOR operation is performed by adds at each iteration loop round key to the state [10].

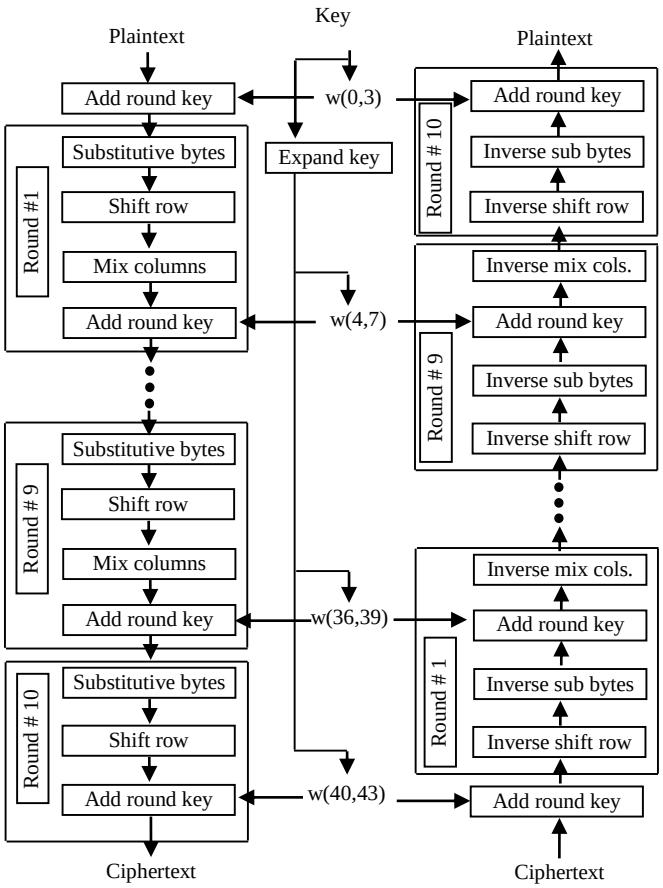


Figure 1: Block diagram for AES encryption and decryption

In the following steps 4×4 array bytes called the State is established. This matrix have four bytes arranged in four rows, each containing Nb bytes, where Nb is the block size divided by 32 (number of words). Whole AES steps (Cipher and Inverse Cipher) are performed on the State matrix, after which its final value is copied to the output (State array set is converted back to the bit sequence). The AES algorithm consist of sequences of 128 bits for each input and output. Sometimes these sequences will be referred to as blocks where the number of bits they include, will be referred to as their length. The AES algorithm cipher key is a sequence of 128, 192 or 256 bits. Ten rounds are on AES algorithm encryption, as can be shown in Fig. (1). Initially, the 128-bit key is expanded into eleven so-called round keys, each of them 128 bits in size. To ensure high security of the encryption each round contain transformation by utilize the corresponding key of cipher. The mentioned sizes state in above is only permit sizes while the other sizes are not allowed. Input block is organized into a (4-by-4) matrix, where every entry represents a byte.

2- A significant problem in images ciphering schemes is the encryption/decryption time because images have large amount of information. Attacks are another challenge of all encryption algorithms. So, ciphering scheme modification should be done carefully such that they do not provide any hiatus to the attackers. One of famous types of attacker is the reduced-round attacker. The AES is a block encryption scheme has set of transformations executed several times (in iterations). Theoretically, the reduced-round adversary can break the AES algorithm in 2^{120} iterations if reduced its rounds to 7. Therefore, reducing the rounds number of the AES algorithm makes it cheap against this attacks. AddRoundKey is one of the AES iteration transforms, where the EX-ORing operation is conducted between subkey derived from the former subkey in the key schedule operation and state. This reason prevents us from reducing the number of AES rounds. The MEAS goal is modifying the AES algorithm through decreasing the computation costs by decreasing the execution time of the MixColumn transformation and replacing the S-box with a new simple S-box to make the algorithm more compatible with our goal. In addition, increasing the security level through enhances the key schedule operation. The detiales of proposed modification in MAES algorithm are exist in (9).

WiMAX STANDARDS (IEE 802.16)

Due to the growing request for Broadband Wireless Access (BWA) in underserved markets has been a major challenge for providers of services, because of, the absence of a really global standard. A standard enables companies to construct systems that will effectively reach residential markets and underserved business in a technique that backup infrastructure build outs comparable to cable, fiber and DSL [11].

The aim of WiMAX is to supply Internet access with high-speed within a several kilometres in radius for the coverage range. Theoretically, WiMAX supplyes for speeds about 70 Mbps within a range of 50 kilometres. The physical layer of WiMAX depends on Orthogonal Frequency Division Multiplexing (OFDM); it transmits information (such as data, video, audio and image) with high-speed, and is utilized by an broadband assortment of commercial systems. The most advantage of the WiMAX standard is of permit wireless connections between a Base Station (BS) and subscribers without needed that they be in a direct line of sight (LOS) with that base station. his technology know by a Non-Line-of-Sight (NLOS) [12]. In this paper performance of cipher image via WiMAX with QPSK modulation and coding is studied on the basis of Bit Error Rate, Signal to Noise Ratio.

Physical layer is used to set up the communication between the devices and is responsible for transporting the data bit sequence. It also determines the type of modulation as well as power of transmission. Two transmission type techniques were used in WiMAX 802.16 PHY-layer OFDM and OFDMA. These techniques operate on band of frequency below 11 GHz that use FDD and TDD as a duplexing technology. Scalable OFDMA was used in physical layer of the IEEE 802.16e, where the size of the FFT is changeable and may be equal to: 128, 512, 1024, and 2048 [13]. 2048 FFT was adopted through this work. The FFT variable size permits to simulate or implement of the system in high band-width channel and radio state conditions; this layer has been accepted by WiMAX for

portable and mobile operations [14]. Figure 2 presents PHY-layer where the PHY-layer includes various functional stages [6, 15]:

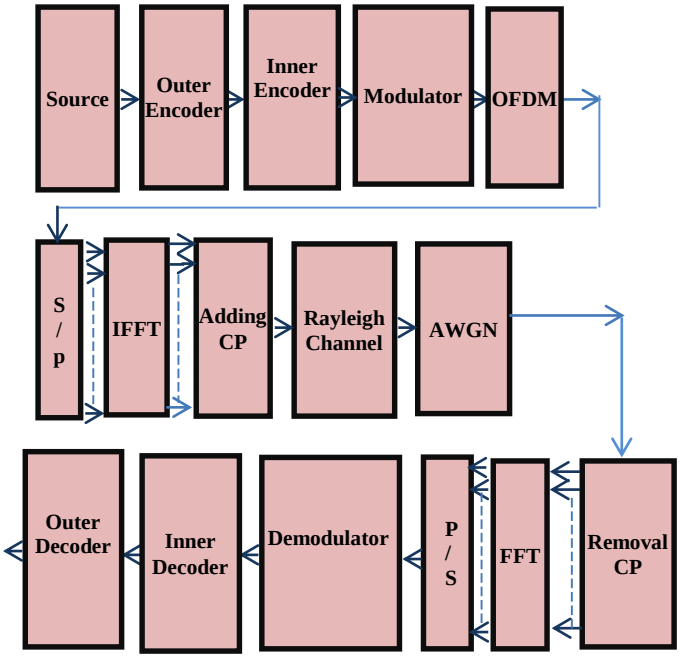


Figure 2: Architecture for the IEEE 802.16 WiMAX Physical Layer

A. Randomizer

To avert long continuous sequence of ones and zeros the randomizer execute input data randomization on each allocation on each burst. This is done by a PseudoRandomBinarySequence (PRBS) generator which employs fifteen stage registers with a polynomial generator with XOR-gates in feedback configuration as shown in Fig. (3).

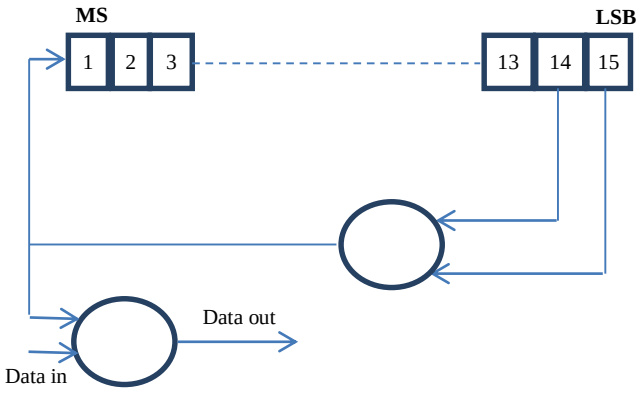


Figure 3: PRBS generator for randomization

B. Reed-Solomon encoder

The feature of Reed-Solomon (RS) code make them appropriate to applications where errors place in bursts. RS correction of error is a scheme of coding which doings through building a polynomial from transmitted data symbols before transmission polynomial with respect to the original symbols. RS code is kmown as RS(n, k ,t) with l-bit symbols. That mean, the encoder occupies k data symbols for each l bit then adds t symbols as parity to build an n-symbol codeword. Where, n is encoding bytes number (output); k is data bytes number (input) before encoding, and t is data bytes number that able to be corrected. An error corrections of any RScode are determined by (n − k), which is redundancy measurement in the block. Actually, RScode can corrected up to t symbols if the wrong location symbols is not known, where t = (n − k)/2. The RS coder found from a organize RS(n, k, t = 255, 239 and 8 respectively) code employ a GaloisField specified as GF(2^8). Primal and generator polynomials which used for the systematic code can be expressed in the next two equations [16]:

Primitive Polynomial:

$$p(x) = x^8 + x^4 + x^3 + x^2 + 1 \quad (1)$$

Generator Polynomial

$$g(x) = (x + \lambda^0)(x + \lambda^1) \dots \dots (x + \lambda^{2t-1}) \quad (2)$$

C. Convolution Encoder

The inner binary convolutional encoder is fed from the outer RS block coded. The generator polynomials is used to derive two output code bits. Figure (4) present convolutional encoder was adopted in this work.

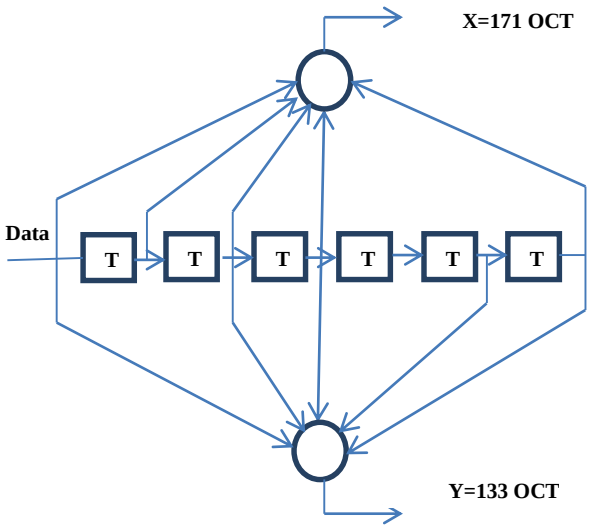


Figure 4: Convolution encoder of binary rate (1/2)

D. Puncturing, Interleaving and Modulation

In order to minimize the amount of transmitted data, puncturing is used to delete bits from the a low-rate output blocks of encoder consistently. Puncturing can be generate

the coding in different rates that important to achieve different levels of system error prediction, these rates are 1/2, 2/3 , 3/4 and 5/6.

Block interleaver is used to interleave the encoded data. The bit encoded number per sub channel is determine interleaving block size, Ncbps. Two step permutation were used in the IEEE 802.16 interleaver.

Depending the size and on the basis of different the data were modulated. Schemes like BPSK, QPSK, 16 QAM and 64 QAM may be used to modulate data coming from interleaver. The modulation was adopted in this work is QPSK.

E. OFDM and Cyclic Prefix

A multi-carrier modulation technique OFDM, that achieve high efficiency of bandwidth that results from orthogonality between carriers and multiple carriers share data among themselves. The robustness to channel fading (Selective and flat fading) is the main advantage of this technique [19].

To preserve orthogonally of the frequency and minimize the delay due to propagation in multipath channel, cyclic prefix is joined in OFDM signals. To make so, before sending the signal, it is joined at the beginning of the signal. In the WiMAX standard four duration of cyclic prefix are available. The ratio of CP to OFDM symbol time, this ratio can be equal to 1/4, 1/8, 1/6 and 1/32.

On the other hand, the channel adds a white no A white noise is added by the channel of a certain variance to the useful signal. Frequency selective and Flat Rayleigh fading is envisioned for further simulator versions. The receiver performs basically the inverse of the transmitter operation blocks.

SYSTEM MODEL

In this paper, a simulation model based on MATLAB (version 2010d) is introduced which consist of a generation of a baseband data from the treated image, encoding unit outer and inner coding is used, digital modulator of QPSK is adopted, OFDM (IFFT) with cyclic prefix insertion blocks in the transmitter and cyclic prefix remover in receiving, OFDM receiver (FFT) followed by demodulator and decoder in the receiver. Figure 4 described all the mentioned stages and Table I listed the parameters of the model. Here, the coding part composed of three steps of Forward Error Correction (FEC), randomization and interleaving [6]. FEC is achieved in two stages through the outer and inner coding (Reed Solomon (RS) and Convolutional Code (CC), respectively). The complementary processes are applied in the reverse order in the receiver end. Rayleigh fading channel with three tap points are implemented. Additive white Gaussian Noise (AWGN) with different variance using to achieve different Signal to Noise Ratio (SNR) values.

SIMULATION RESULTS

In this work the performance of proposed system will be evaluated through studying the effect of transmission system on the decrypted image. The evaluation parameters used are visual scene, histogram evaluation, correlation coefficients, entropy, and BER. Four tests image in different applications are used in this evaluation in different values of SNR.

F. Visual scene

The visual scene of original secret, ciphered transmitted, ciphered received and reconstructed images are viewed and compared to check the effect of channel on the image for two values of SNR only, where the tests of other SNR values shown in appendices. Figures (7-14) show the images visual scene for four tests. As clearly shown the difference between transmitted and received ciphered images is so little such that the human eyes cannot sense this difference for all tests and for all values of SNR as shown in figures (b & c) of all figures. on the other hand, reconstructed image is losses with little values of SNR while this loss is decreased with increase the SNR values (see figures a & d of Figs. 5-12).

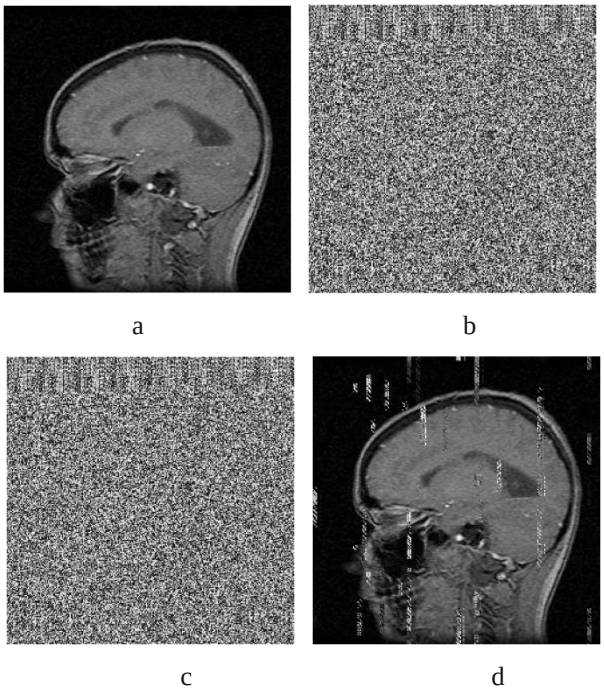
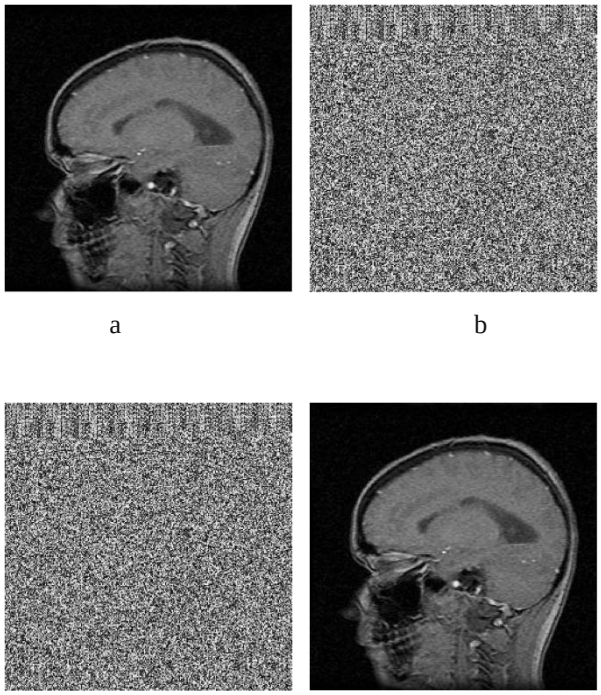


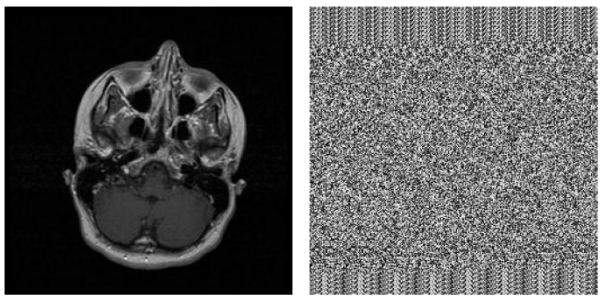
Figure 5: Visual scene Test1 SNR 10 dB; a- Original Secret Image; b- Transmitted Ciphered Image; c- Received ciphered image; d- reconstructed secret image.



a b

c d

Figure 6: Visual scene Test1 SNR 20 dB; a- Original Secret Image; b- Transmitted Ciphered Image; c- Received ciphered image; reconstructed secret image.

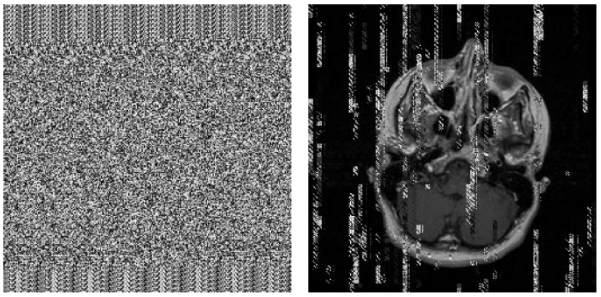


a b

TABLE I: SYSTEM MODEL PARAMETER

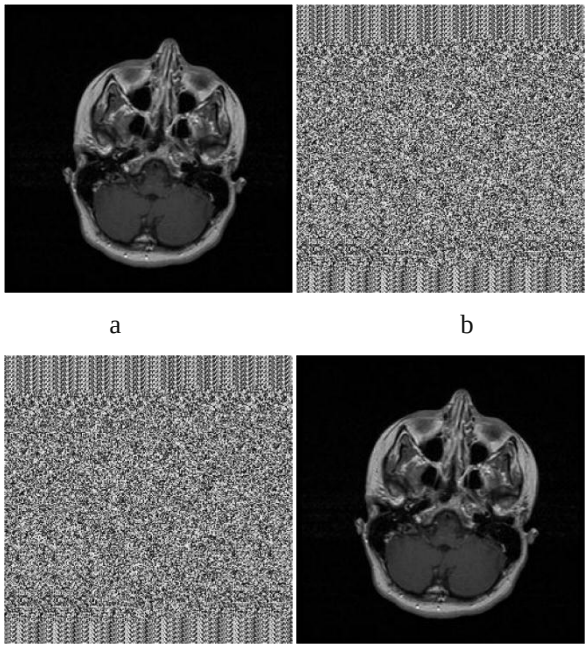
Specification	Puncture vector
Coding	RS outer Convolution
NFFT	2048
Modulation	QPSK
OFDM symbol duration	0. 446e-7 sec
Cyclic Prefix guard interval	1/4

Column 1	Column 2	Column 3 [a]
xx1	yyy1	zzz1
xxx2	yy2	zzz2
xxx3	yyy3	zz3
xxx4	yy4	zzzzz4
xxx5	yyyyy5	zz5



c d

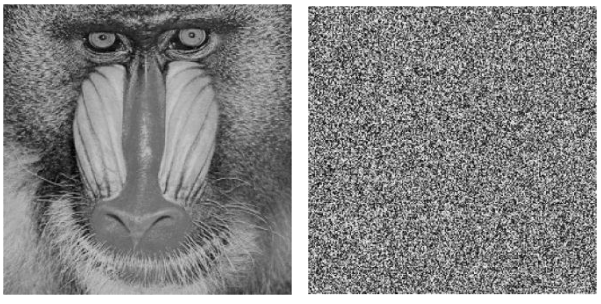
Figure 7: Visual scene Test2 SNR 10 dB; a- Original Secret Image; b- Transmitted Ciphered Image; c- Received ciphered image; reconstructed secret image.



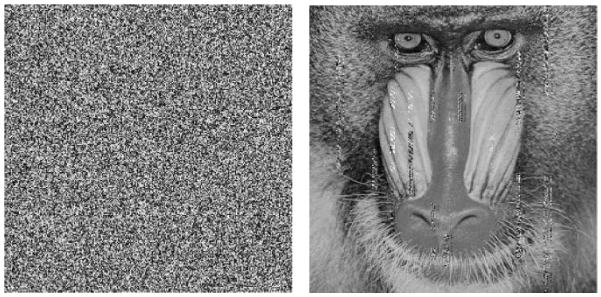
a b

c d

Figure 8: Visual scene Test2 SNR 20 dB; a- Original Secret Image; b- Transmitted Ciphered Image; c- Received ciphered image; reconstructed secret image.

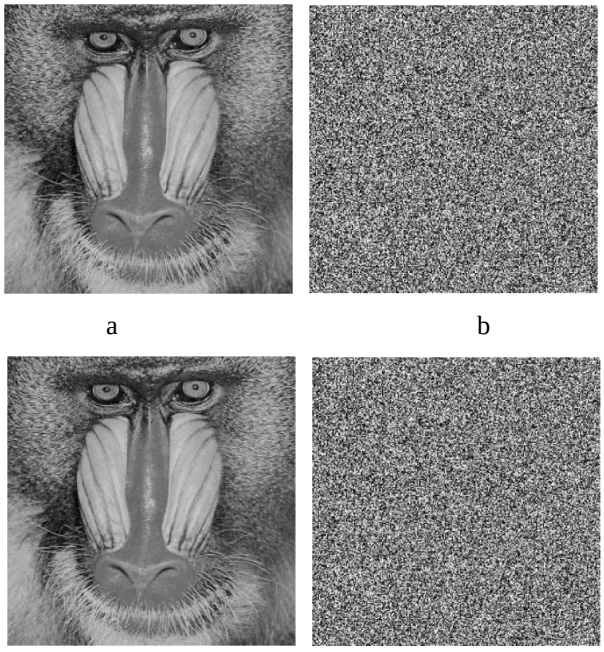


a b



c d

Figure 9: Visual scene Test3 SNR 10 dB; a- Original Secret Image; b- Transmitted Ciphered Image; c- Received ciphered image; reconstructed secret image.

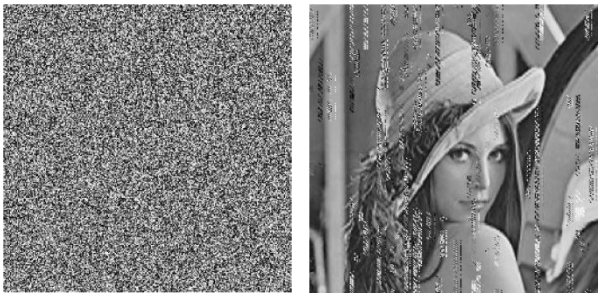


a b

c d

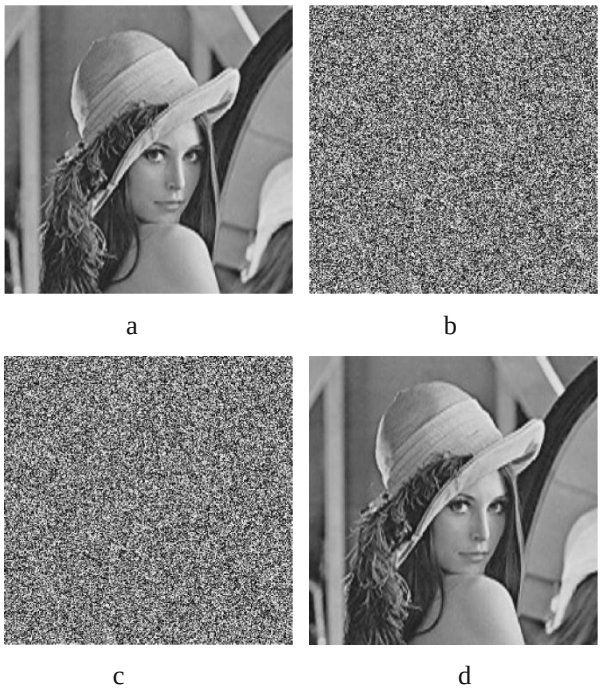
Figure 10: Visual scene Test3 SNR 20 dB; a- Original Secret Image; b- Transmitted Ciphered Image; c- Received ciphered image; reconstructed secret image.

a b



c d

Figure 11: Visual scene Test4 SNR 10 dB; a- Original Secret Image; b- Transmitted Ciphered Image; c- Received ciphered image; reconstructed secret image.



a b

c d

Figure 12: Visual scene Test4 SNR 20 dB; a- Original Secret Image; b- Transmitted Ciphered Image; c- Received ciphered image; reconstructed secret image.

G. Histogram Analysis

An image histogram is representing distribution of image pixels on intensity levels. Encrypted image histogram should be uniformly distributed to cope the statistic attacks[5]. This factor used to evaluate in two direction, one by comparing between the histogram of transmitted and received ciphered images, while the other by comparing between histogram of original and extracted versions of secret image. As shown in Figure 13, the histogram of two versions of secret images are much compatible especially with 20 dB as in 13-c, which mean the encryption algorithm was more stronger against channels problems. Figure 14 is also confirm this analysis.

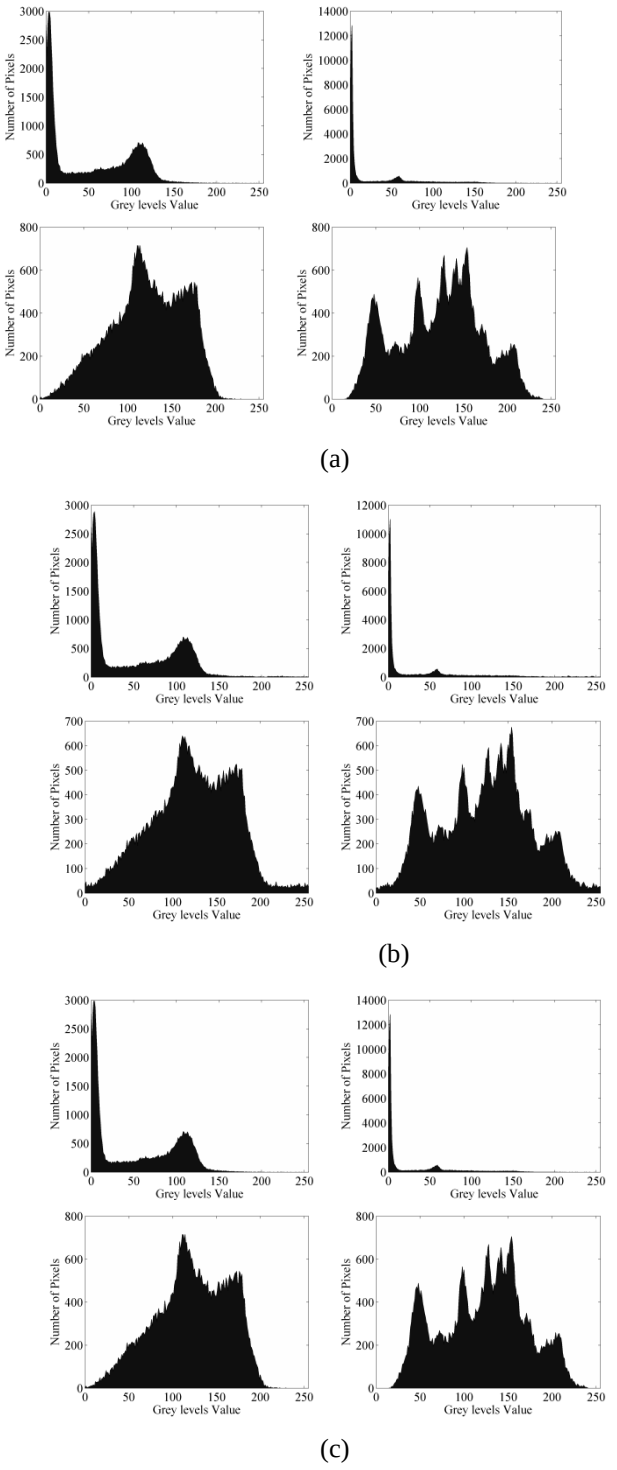


Figure 13: Histogram analysis of original and extracted versions of secret image; a- Original Secret Image; b- Extracted secret image with 10 dB; c- Extracted secret image with 20 dB. 1st , 2nd, 3rd and 4th tests in 1st, 2nd, 3rd and 4th columns respectively.

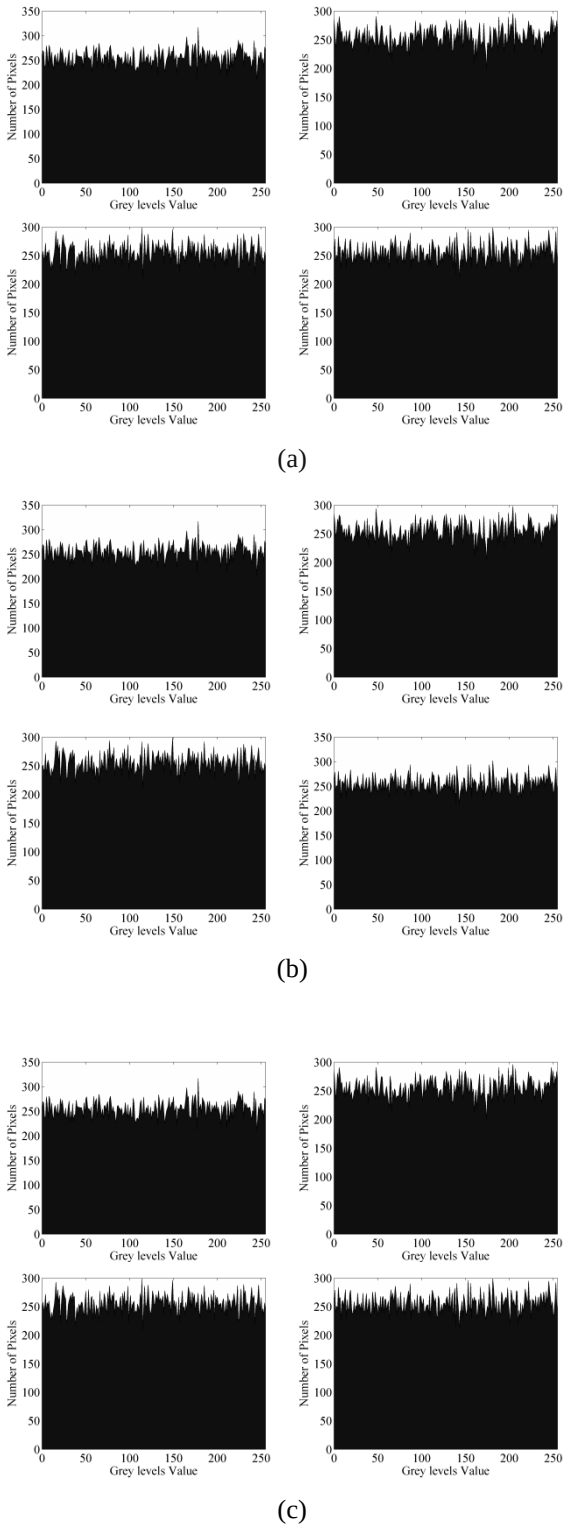
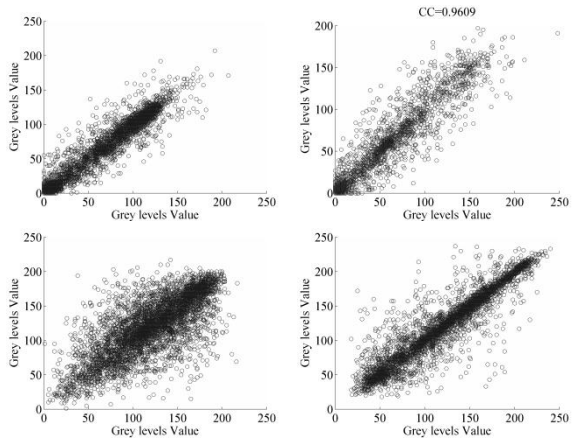


Figure 14: Histogram analysis of transmitted and received ciphered image; a- Transmitted image; b- Received ciphered image with 10 dB; c- received ciphered image with 20 dB. 1st , 2nd, 3rd and 4th columns are represent 1st, 2nd, 3rd and 4th tests respectively

H. Correlation coefficients

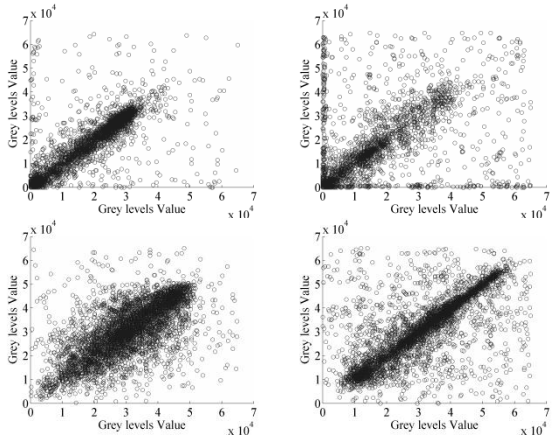
Generally, adjusted pixels in all types of images highly correlated with itself. The best encryption algorithm that introducing protected image with very low engagement between the neighboring pixels [19]. Firstly, 5000 pair of adjacent pixels was randomly selected from tests images. Figure 15 shows the correlation coefficients of original and reconstructed version of secret images for four tests used. as clearly shown in Figure the correlation coefficient of original and extracted images was so convergence especially with SNR equal to 20 dB (15.c), where with 10 dB there are more random pixel values (15.b). Table II shows the value of correlation coefficients.



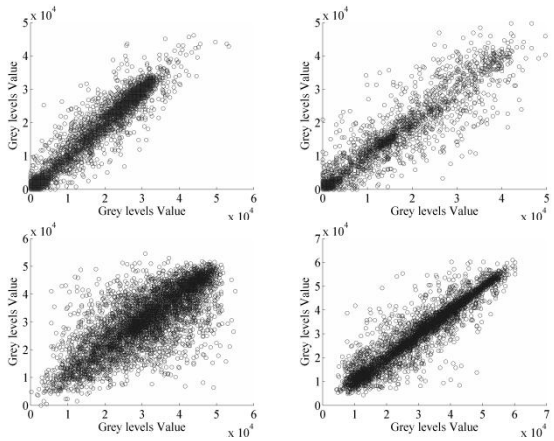
(a)

TABLE II: CORRELATION COEFFICIENTS VALUES

images		SNR					
		10 dB	12 dB	14 dB	16 dB	18 dB	20 dB
Test1	OI	0.9730	0.9730	0.9730	0.9730	0.9730	0.9730
	TCI	0.0222	0.0222	0.0222	0.0222	0.0222	0.0222
	RCI	0.0064	0.0057	-0.0034	0.0093	0.0013	0.0099
	EI	0.8622	0.8928	0.9032	0.9246	0.9408	0.9747
Test2	OI	0.9674	0.9674	0.9674	0.9674	0.9674	0.9674
	TCI	0.0223	0.0223	0.0223	0.0223	0.0223	0.0223
	RCI	0.0246	0.0103	0.0056	0.0654	0.0218	0.0069
	EI	0.7344	0.7705	0.8615	0.8657	0.9319	0.9568
Test3	OI	0.7751	0.7751	0.7751	0.7751	0.7751	0.7751
	TCI	0.0020	0.0020	0.0020	0.0020	0.0020	0.0020
	RCI	0.0193	0.0059	0.0099	0.0108	0.0104	0.0274
	EI	0.5022	0.6676	0.7455	0.7541	0.7623	0.7707
Test4	OI	0.9784	0.9784	0.9784	0.9784	0.9784	0.9784
	TCI	0.0001	0.0001	0.0001	0.0001	0.0001	0.0001
	RCI	0.0062	0.0239	0.0088	0.0052	0.0161	0 .0044
	EI	0.7036	0.8327	0.8933	0.8964	0.9323	0.9436



(b)



(c)

Figure 15: Correlation coefficients of original and extracted versions of secret image; a- Original Secret Image; b- Extracted secret image with 10 dB; c- Extracted secret image with 20 dB. 1st , 2nd, 3rd and 4th columns represent 1st, 2nd, 3rd and 4th columns respectively.

I. Entropy

The concept of entropy comes from information theory and Ergodic theory. Shannon entropy is defined as a metric associated with information content of input signal. In image processing fields, the entropy known as the randomness size which can be explain as the doubt range of the information source [20]. Entropy values for 4 image tests in different values of SNR are shown in Table IV below

From results of histogram analysis, correlation coefficients and entropy, we can find that the protected image by encryption algorithm is not much affected by channels effects. Also, the effects of channels on the protected image is decreased when the SNR increased.

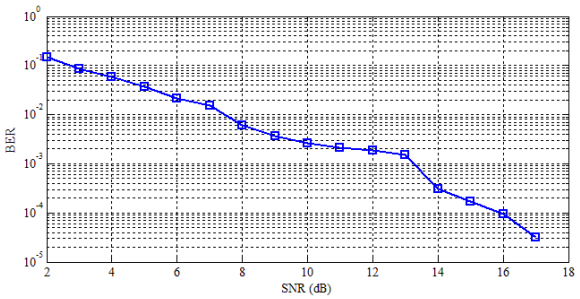


Figure 16: BER v. SNR

CONCLUSIONS

An studying of transmission channel effect on the ciphering algorithm was introduced in this paper. An image encrypted by new modified version of AES algorithm and transmitted over channel in WiMAX standard then received it and check its features. This study is achieved through comparison between transmitted ciphered image and received ciphered image and through comparison between original and reconstructed versions of secret image. Several parameters used to achieve this comparison such as visual scene, histogram analysis, correlation coefficients and entropy. The results of evaluation proved that the effects of transmission channel problems is very low on the image ciphered by MAES algorithm which mean this ciphered algorithm is strong against channel problems especially if the SNR of the channel increased.

TABLE III: ENTROPY

images		SNR					
		10 dB	12 dB	14 dB	16 dB	18 dB	20 dB
Test1	OI	6.5181	6.5181	6.5181	6.5181	6.5181	6.5181
	TCI	7.9970	7.9970	7.9970	7.9970	7.9970	7.9970
	RCI	7.9956	7.9960	7.9963	7.9965	7.9967	7.9969
	EI	6.6421	6.6387	6.6289	6.5744	6.5594	6.5281
Test2	OI	5.1560	5.1560	5.1560	5.1560	5.1560	5.1560
	TCI	7.9970	7.9970	7.9970	7.9970	7.9970	7.9970
	RCI	7.9956	7.9960	7.9963	7.9965	7.9967	7.9969
	EI	5.7334	5.4604	5.2508	5.2377	5.2002	5.1570
Test3	OI	7.3481	7.3481	7.3481	7.3481	7.3481	7.3481
	TCI	7.9970	7.9970	7.9970	7.9970	7.9970	7.9970
	RCI	7.9956	7.9960	7.9963	7.9965	7.9967	7.9969
	EI	7.5273	7.4244	7.3787	7.3568	7.3533	7.3481
Test4	OI	7.4959	7.4959	7.4959	7.4959	7.4959	7.4959
	TCI	7.9970	7.9970	7.9970	7.9970	7.9970	7.9970
	RCI	7.9956	7.9960	7.9963	7.9965	7.9967	7.9969
	EI	7.6350	7.5706	7.5256	7.5245	7.4978	7.4959

REFERENCES

[1] S. H. Kamali & R. Shakerian, " A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption" *International Conference on Electronics and Information Engineering (ICEIE 2010)*, Vol. 1 , pp. 141-145.

[2] T. M. Triet & D. A. Duc, "Applying the AES and Its Extended Versions in a General Framework for Hiding Information in Digital Images", CIS, Part II, LNAI 3802, 2005, pp. 605 – 610.

[3] C. Yi-cheng, Z. Xue-cheng, L. Zheng-lin, C. Xiao-fei, H. Yu, " Dynamic Inhomogeneous S-Boxes design for efficient AES masking mechanisms," *The Journal of China Universities of Posts and Telecommunications*, Vol. 15, No. 2, 2008, pp. 72-76.

[4] C.W. Huang, C.L. Yen, C.H. Chiang, K.H. Chang and C.J. Chang, "The Five Modes AES Applications in Sounds and Images," *Sixth International Conference on Information Assurance and Security*, 2010, pp. 28-31.

[5] S.M. Wadi & N. Zainal, "Decomposition by Binary Codes-Based Speedy Image Encryption Algorithm for Multiple Applications," *IET Image Processing* Vol. 9, No. (5), 2015, p.p. 413-423.

[6] C.H. Lin, R.H. Hwang, J.J. Wu, J.F. Lee, and Y.D. Lin, "Integration of Spatial Reuse and Allocation for Downlink Broadcast in LTE-Advanced and WiMAX Relay Networks," *IEEE Transactions on Vehicular Technology*, VOL. 64, NO. 11, NOVEMBER 2015, pp. 5246- 5256.

[7] J. Rakesh, W. Vishal, U. Dalal, "A Survey of Mobile WiMAX IEEE 802.16m Standard," *International Journal of Computer Science and Information Security (IJCSIS)*, Vol. 8, No. 1, April 2010. pp.125-131.

[8] A. Bouacha & F. T. Bendimerad, "Performance Study Of The MCCDMA As Physical Layer For Mobile Wimax Technology," *International Journal of Computer Networking, Wireless and Mobile Communications (IJCNWMC)*,Vol. 3, No. 2, Jun 2013, pp. 47-52.

[9] S. M. Wadi, & N. Zainal, "High definition image encryption algorithm based on AES modification," *Wireless Personal Communications*, Vol. 79, No.2, 2014, pp.811-829.

[10] Department of Commerce, N. I. O. S. a. T., Information Technology Laboratory (Itl). (2001). Advanced Encryption Standard (AES) (Fips Pub 197). Computer Security Standard, Cryptography. 5285 Port Royal Road, Springfield, VA 22161, National Technical Information Service (NTIS): 51.

[11] V. Grewal, A.K. Sharma, "On Performance Enhancements of WiMax PHY Layer with Turbo Coding for Mobile Environments," *International Journal of Advanced Science and Technology*, Vol. 31, June, 2011.

[12] M. Rooyen, J.W. Odendaal, and J. Joubert, "High Gain Directional Antenna for WLAN and WiMAX

Applications," *IEEE Antennas and Wireless Propagation Letters*,DOI 10.1109/LAWP.2016.2573594, 2016.

[13] M.M. Matalgah, O.M. Hammouri, B. Paudel, "Cross-layer Capacity Optimization in WiMAX Orthogonal Frequency Division Multiple Access Systems with Multi-class Quality of Services and Users Queue Status," *IET Commun.*, Vol. 8, No. 14, 2014, pp. 2500–2508.

[14] H. Zhai, Q. Gao, C. Liang, R. Yu, and S. Liu, "A Dual-band High-gain Base Station Antenna for WLAN and WiMAX Applications," *IEEE Antennas and Wireless Propagation Letters*, DOI 10.1109/LAWP.2014.2321503, 2014.

[15] W. Xiumin, G. Tingting, L. Jun, S. Chen and H. Fangfei, "Efficient Multi-rate Encoder of QC-LDPC Codes Based on FPGA forWIMAX Standard," *Chinese Journal of Electronics*, Vol. 26, No. 2, Mar. 2017.

[16] M.A. Mohamed, F.W. Zaki and R.H. Mosbeh, "Simulation of WiMAX Physical Layer: IEEE 802.16e," *International Journal of Computer Science and Network Security IJCSNS*, Vol.10 No.11, November 2010, pp 49-55.

[17] Neha Rathore, Dr. Sudhir Kumar, Abhishek Choubey "OFDM Performance evaluation of WIMAX MAC layer :IEEE- 802-16e," *International Journal of Electronics & Communication Technology IJECT*, Vol. 2, No. 3, Sept. 2011.

[18] A. G. Wadday, A.S. Abdullah and S. A. Alseyab, "Turbo and Convolution Codes Assisted Space Time Block Code-Spatial Modulation," *Future Communication Networks (ICFCN) International Conference*, 01 June 2012.

[19] M. Vaidehi and B. Justus Rabi, "Enhanced MixColumn Design for AES Encryption," *Indian Journal of Science and Technology*, Vol. 8, No. 35, DOI: 10.17485/ijst/2015/v8i35/82302, December 2015, pp. 1-7.

[20] S.M. Wadi, N. Zainal and A. Abdulgader, "Grey Scale Image Hiding Method Based on Decomposition Operation," *IEEE Student Conference on Research & Development* 2013, Putrajay, Malaysia.