Enhanced Diffusion Encryption for Video Transmission over Mobile WiMax Networks

M.A. Mohamed, F.W. Zaki and A.M. El-Mohandes

**Electronics and Communication Engineering, Faculty of Engineering-Mansoura University
Mansoura, Dakhlia, Egypt**

Abstract

As a promising broadband wireless technology, WiMax has many salient advantages over such as: high data rates, quality of service, scalability, security, and mobility. Many sophisticated authentication and encryption techniques have been embedded into WiMax but it still exposes to various attacks in. In this paper, three proposed chaos encryption techniques were described for video transmission over Mobile WiMax as an enhancement of multimedia security problem in Mobile WiMax which use AES algorithm. At first, a global overview of the technology WiMax was given to determine the disadvantages of recently used encryption algorithm with video transmission. Then the proposed encryption techniques were presented with its chaos systems. Next, these proposed techniques and AES were applied to video to compare between them. It was found that when Henon and Baker maps are combined in one technique, it will have high speed and more robust to statistical and differential attacks, so we can say that this technique enhances the diffusion properties for video encryption.

Keywords: *IEEE 802.16e, Security Sublayer, AES, Chaos and Encryption.*

1. Introduction

WiMax, also known as the IEEE 802.16 protocol, is the latest standard for wireless networks. It was established in 1999 to prepare specifications for broadband wireless metropolitan area networks. The first 802.16 standard was approved in December 2001 and was followed by three amendments: 802.16a, 802.16b and 802.16c. In 2004 the 802.16-2004 standard was released and the earlier 802.16 documents including the a/b/c amendments were withdrawn. An amendment to 802.16-2004, IEEE 802.16e-2005, addressing mobility, was concluded in 2005. This implemented a number of enhancements to 802.16-2004, including better support for Quality of Service, Security and the use of Scalable OFDMA, and is sometimes called "Mobile WiMax", after the WIMAX forum [1]. The security sublayer of the IEEE 802.16 standards defines different security mechanisms which support: (i) authenticate the user who enters in to the network, (ii) authorize the user, and then (iii) provide the necessary encryption support for the key transfer and data traffic. The IEEE 802.16 standards security architecture is based on PKM (Privacy Key Management) protocol which provides a flexible solution that supports device and user authentication between a mobile station and the home connectivity service network. Even though this standard brief the medium access control (MAC) and physical (PHY) layer functionality, it mainly concentrate on point-to-multipoint (PMP) networks. In the concern of security, mesh networks are more vulnerable than the PMP network. The goal of the Security Sublayer is to provide the mutual authentication for access control and confidentiality of the data link layer [2]. It has two component protocols: (i) an encapsulation protocol for multimedia encryption and authentication algorithms, (ii) a key management protocol (PKM) providing the secure distribution of keying data from the base station to the mobile station [2]. The security sublayer of Mobile WiMax standard depends on AES to encrypt MAC layer PDUs with different key sizes. According to the properties of video; the AES algorithm appears not to be ideal for the following reasons: (i) Videos are usually very large-sized and bulky, encrypting such bulky data with the traditional ciphers incurs significant overhead and it is too expensive for real-time multimedia applications, (ii) In the case of video frames, adjacent pixels often have similar gray-scale values and strong correlations, and consecutive frames are similar and most likely only few pixels would differ from frame to frame. Such an extremely high data redundancy of video makes the AES fail to obscure all visible information. So in this research AES algorithm are replaced by three proposed algorithms based on chaos systems and compared together to determine features of them such as speed, throughput, resist to statistical and differential attacks on selected frames of video. The rest of the paper is organized as follows: The Mobile WiMax overview is discussed in the next section. Section (3) discusses three new proposed techniques and AES. Section (4) introduces experimental design. Section (5) presents results and discussion. Section (6) is the conclusion.

2. Mobile WiMax: An Overview

The IEEE 802.16-2009 standard defines a generic reference model where major functional blocks (i.e.,

physical layer, security sublayer, MAC common part sublayer, and service specific convergence sublayer) and their interfaces, the premises of IEEE 802.16 entity, and a general network control and management system are specified. The IEEE 802.16m has modified this reference model by further classifying the MAC common part sublayer functions into two functional groups, resulting in a more structured approach to characterizing the data link layer functions and their interoperation. The earlier revisions and/or amendments of the IEEE 802.16 standard did not explicitly define any detailed protocol structure; rather, the functional elements in the specification were implicitly classified as convergence sublayer, MAC common part sublayer, security sublayer, and physical layer. While each of these layers and/or sublayers comprises constituent functions and protocols, no perspective was provided on how various components were interconnected and interoperated from a system standpoint. In fact, the IEEE 802.16 standards have never been developed with a system engineering approach; rather, they specify components and building blocks that can be integrated (obviously various combinations are potentially possible) to build a working and performing system. An example is the mobile WiMax system profiles where a specific set of IEEE 802.16-2009 features were selected to form a mobile broadband wireless access system [3]. In an attempt to improve the clarity of the previous IEEE 802.16 standards and to take a systematic approach in development of the advanced air interface, IEEE 802.16m has defined a protocol structure and the functional components are classified into different layers and sublayers, as well as differentiated based on data-plane or control-plane categories.

2.1 Mobile WiMax MAC Layer

The primary task of the WiMax MAC layer is to provide an interface between the higher transport layers and the physical layer. The MAC layer takes packets from the upper layer these packets are called MAC service data units (MSDUs) and organizes them into MAC protocol data units (MPDUs) for transmission over the air. For received transmissions, the MAC layer does the reverse. IEEE 802.16m MAC design includes a convergence sublayer that can interface with a variety of higher-layer protocols, such as ATM, TDM Voice, Ethernet, IP, and any unknown future protocol. Given the predominance of IP and Ethernet in the industry, the WiMax Forum has decided to support only IP and Ethernet at this time. Besides providing a mapping to and from the higher layers, the convergence sublayer supports MSDU header suppression to reduce the higher layer overheads on each packet [12], [13]. IEEE 802.16em MAC design includes also two additional sublayers; common part sublayer and privacy sublayer. The MAC common part sublayer is the core functional layer which provides system access, bandwidth allocation, connection establishment, and connection maintenance. It receives data from various CSs classified to particular connection identifier CIDs. QoS is applied to transmission and scheduling of data over the PHY layer.

The WiMax MAC is designed from the ground up to support very high peak bit rates while delivering quality of service similar to that of ATM and DOCSIS. The WiMax MAC uses a variable length MPDU and offers a lot of flexibility to allow for their efficient transmission. For example, multiple MPDUs of same or different lengths may be aggregated into a single burst to save PHY overhead. Similarly, multiple MSDUs from the same higher layer service may be concatenated into a single MPDU to save MAC header overhead. Conversely, large MSDUs may be fragmented into smaller MPDUs and sent across multiple frames. Privacy sublayer of IEEE 802.16m supports best in class security features by adopting the best technologies available today [7], [8]. Support exists for mutual device/user authentication, flexible key management protocol and strong traffic encryption, control and management plane message protection and security protocol optimizations for fast handovers. Encryption done on the MAC PDUs formed from the MAC SDUs and passes them over to the physical layer. Fig. 1 shows the structure of WiMax protocol layers that includes MAC layer and PHY layer. Fig. 2 shows examples of various MAC PDU (packet data unit) frames. Each MAC frame is prefixed with a generic MAC header (GMH) that contains a connection identifier (CID), the length of frame, and bits to qualify the presence of CRC, subheaders, and whether the payload is encrypted and if so, with which key [4], [8]. The MAC payload is either a transport or a management message. Besides MSDUs, the transport payload may contain bandwidth requests or retransmission requests. The type of transport payload is identified by the subheader that immediately precedes it. Examples of subheaders are packing subheaders and fragmentation subheaders. WiMax MAC also supports ARQ, which can be used to request the retransmission of non-fragmented MSDUs and fragments of MSDUs. The maximum frame length is 2,047 bytes, which is represented by 11 bits in the GMH.

2.2 Mobile WiMax Security Sublayer

The security architecture of IEEE 802.16m consists of the MS, the BS, and the Authenticator, as shown in Fig. 3. Within the MS and BS, the security functions are classified into two logical categories: (i) a security management entity; and (ii) encryption and integrity. The security management entity includes the following functions: (i) Overall security management; (ii) Extensible

Authentication Protocol (EAP) encapsulation/de-encapsulation for authentication; (iii) PKM control functions through key generation/derivation/distribution, and key state management; (iv) Authentication and Security Association (SA) control; and (v) Location privacy. Encryption and integrity protection entity consists of the following functions: (i) User data encryption and authentication; (ii) Management message authentication; and (iii) Protection of management message confidentiality.

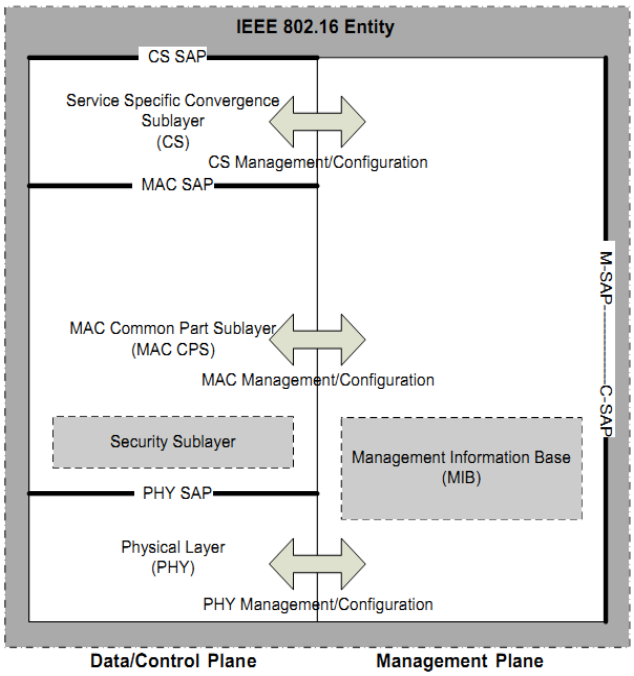

Fig. 1 WiMax Protocol Layers.

3. Proposed Algorithms and AES Standard

The frames of any video have strong correlation among adjacent samples. However, it is very important to disturb the high correlation among these samples to increase the security level of the encrypted data. So, simple and strong algorithms have been proposed. In these proposed algorithms, video is encrypted by shuffling samples and then changing these values by applying different chaotic maps to create an encrypted data [9], [15]. The idea of using chaos for data encryption is certainly not new and can be traced to the classical Shannon's paper in 1952. Even though he does not use the word chaos, he proposes mixing, measure preserving transformations which depend on their arguments in a sensitive way. Actually any encryption algorithm based on chaos systems divided into two phases: (i) Permutation and (ii) Diffusion. These phases also compose very good encryption schemes with not only high security but also fast speed.

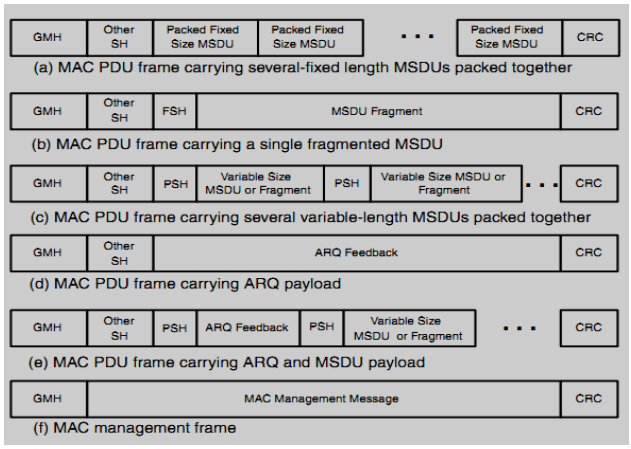

Fig. 2 Examples of Various MAC PDU Frames.

Chaos theory plays an active role in modern cryptography. As the basis for developing a crypto-system, the advantage of using chaos lies in its random behavior and sensitivity to initial conditions and parameter settings to fulfill the classic Shannon requirements of confusion and diffusion. To meet a great demand for real-time secure multimedia transmission, a variety of chaos based encryption algorithms have been proposed. These algorithms have shown some exceptionally good properties in many concerned aspects regarding security, complexity, speed, computing power, computational overhead and its hardware implementation is suitable for embedded devices which have tight constraints on power consumption, hardware resources and real-time parameters, etc. [11]

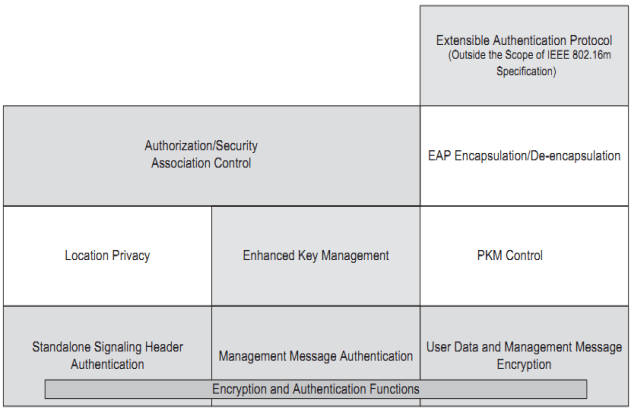

Fig. 3 Functional blocks of IEEE 802.16m security architecture.

3.1 The First Proposed Algorithm

The frame's samples are rearranged using 2D CAT map that is defined by Eq. (1) and then these values are changed using 1D logistic map [10] that is defined by Eq. (2). We use simple process for diffusion so we XORed n^{th} sample by $(X_n * 10^5)$ mod 256 [15].

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} ab+1 & a \\ b & 1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} (mod\ N) \quad (1)$$

$$X_{n+1} = 4 \times X_n \times (1 - X_n) \quad (2)$$

where a and b are random number from 0 to 256 and the initial value X_0 is random value from 0 to 1 and all depend on 256 bits key. The encryption steps are as follows:

1. Randomly generate a and b from 0 to 256 using the encryption key.
2. Convert each frame to YC_bC_r color domain.
3. Perform the two-dimensional Cat map on Y-component only: Use a and b as control parameters to perform the discrete cat map on two-dimensional coordinates of each pixel according to Eq. (1), generating shuffled version of Y and convert it to one dimensional data has M pixels.
4. Randomly generate X_0 as an initial input number in (0, 1) using the encryption key.
5. Compute the logistic map according to Eq. (2) for M times, and start to record X_{i+1} from $(M+1)^{th}$ iteration until we have M values.
6. XORed each pixel with $Z_i = (X_n * 10^5) \bmod 256$ to diffuse its values.
7. Convert diffused data to two dimensional array and recombine it with C_bC_r components.
8. Reconstruct the frame from its YC_bC_r domain to be transmitted.

3.2 The Second Proposed Algorithm

The frame's samples are rearranged using 2D Henon map [11] that is defined by Eq. (3) and then these values are changed using two 1D Logistic maps that is defined by Eq. (2). Each logistic map generate a different random sequence Y and X used to diffuse samples according to Eq. (5). Where Y and X are an integer numbers generated from the fractional numbers that generated from two 1D Logistic maps using the following transformation: $X_n = (X_n * 10^6) \bmod 256$ and $Y_n = (Y_n * 10^6) \bmod 256$ [15].

$$X_{n+1} = 1 + Y_n - 1.4X_n^2 \quad and \quad Y_{n+1} = 0.3X_n \quad (3)$$

where the initial values Y_0 and X_0 are random numbers depends on 128 bits key. The encryption steps are as follows:

1. Randomly generate the initial values of Henon map (X_0 and Y_0) using the encryption key.
2. Convert each frame to YC_bC_r color domain.
3. Perform the two-dimensional Henon map on Y-component only: Use X_0 and Y_0 as control parameters to perform the discrete Henon map on two-dimensional coordinates of each pixel according to Eq. (3), generating shuffled version of Y has M pixels distributed on R × C matrix.
4. Randomly generate two initial inputs for Logistic map in (0, 1) using the encryption key.
5. Compute the logistic map two times according to Eq. (2), firstly for R times, and start to record X_{i+1} from $(R+1)^{th}$ iteration until we have R values, and second for C times, and start to record X_{i+1} from $(C+1)^{th}$ iteration until we have C values.
6. Diffuse each pixel using the generated random values in step 5 as a two keys applied to Eq. (5).
7. Convert diffused data to two dimensional array and recombine it with C_bC_r components.
8. Reconstruct the frame from its YC_bC_r domain to be transmitted.

3.3 The Third Proposed Algorithm

The frame's samples are rearranged using 2D Baker map [11] that is defined by Eq. (4) and then these values are changed using 2D Henon map that is defined by Eq. (3). We used discretized generalized Baker map in which multimedia sample (r, s), with $N_i \le r$, $r < (N_i + n_i)$ and $0 \le s < N$ is mapped to a new location using Eq. (4).

$$B(r,s) = \left(\frac{N}{n_i}(r - N_i) + s \bmod \frac{N}{n_i}, \frac{n_i}{N}\left(s - s \bmod \frac{N}{n_i}\right) + N_i\right) \quad (4)$$

We used the random values generated by 2D Henon map to do a diffusion process according to Eq. (5). The values Y_n and X_n generated by Eq. (3) are fractional and to convert them to integer values we do the following transformation: $X_n = (X_n * 256) \bmod 256$ and $Y_n = (Y_n * 256) \bmod 256$.

$$D_n = Y_n \times (B_n + X_n) \bmod 256 \quad (5)$$

The encryption steps are as follows:

1. Convert each frame to YC_bC_r color domain.
2. Perform the two-dimensional Baker map on Y-component only: Use Eq. (4) to perform the discrete Baker map on two-dimensional coordinates of each pixel, generating shuffled version of Y has M pixels distributed on R × C matrix.
3. Randomly generate two initial inputs for Henon map using the encryption key.
4. Compute the Henon map according to Eq. (3), firstly for M/2 times, and start to record X_{i+1} and Y_{i+1} from $(M/2+1)^{th}$ iteration until we have R values of X, and C values of Y.
5. Diffuse each pixel using the generated random values in step 5 as a two keys applied to Eq. (5).
6. Convert diffused data to two dimensional array and recombine it with C_bC_r components.

7. Reconstruct the frame from its YC_bC_r domain to be transmitted.

3.4 AES Algorithm

In 1997, the National Institute of Standards and Technology put out a call for candidates to replace DES. Among the requirements were that the new algorithm should allow key sizes of 128, 192, and 256 bits, it should operate on blocks of 128 input bits, and it should work on a variety of different hardware, for example, 8-bit processors that could be used in smart cards and the 32-bit architecture commonly used in personal computers. Speed and cryptographic strength were also important considerations. In 1998, the cryptographic community was asked to comment on 15 candidate algorithms. Five finalists were chosen: MARS (from IBM), RC6 (from RSA Laboratories), Rijndael (from Joan Daemen and Vincent Rijmen), Serpent (from Ross Anderson, Eli Biham, and Lars Knudsen), and Twofish (from Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson). Eventually, Rijndael was chosen as the Advanced Encryption Standard [16]. The other four algorithms are also very strong, and it is likely that they will be used in many future cryptosystems. The AES algorithm consists of 10 rounds (when the key has 192 bits, 12 rounds are used, and when the key has 256 bits, 14 rounds are used). Each round has a round key, derived from the original key. There is also a 0^{th} round key, which is the original key. A round starts with an input of 128 bits and produces an output of 128 bits. There are four basic steps, called layers, which are used to form the rounds: (i) SubBytes; (ii) ShiftRows; (iii) MixColumns and (iv) AddRoundKey Transformations.

4. Experimental Design

In this paper three different proposed algorithms will be used to encrypt video in WiMax privacy sublayer instead of AES algorithm. These algorithms have been implemented by MATLB 2010b. The personal laptop is used in all programs and tests was Intel(R) Core™ 2Duo CPU 2.00GHz with 6.00MB cash, 4.00GB of memory and 320GB hard disk capacity. The following tasks that will be performed are shown as follows: (i) proposed encryption algorithms based on chaotic maps have been proposed to encrypt video in Mobile WiMax; (ii) using AES also to encrypt the same video file as the main encryption technique used by WiMax security sublayer; (iii) the diffusion robustness of the proposed algorithms and AES algorithm are examined in the presence of statistical and differential attacks, and (iv) comparison among the different encryption algorithms have been made in terms of the average encryption-decryption elapsed time and throughput to encrypt video frames.

5. Results and Discussion

The performance of the discussed encryption algorithms was evaluated using a set of quantitative parameters: (i) elapsed time; (ii) throughput rate, and (iii) correlation between the original data and the encrypted data. For video we used 132 frame of audio/video interleaved (AVI) format with 24.7 MB size and each frame has a resolution 256×256. A good encryption scheme should resist all kinds of known attacks, such as statistical and differential attack. The security of the proposed algorithms is investigated for video under the statistical attacks, and the differential attacks.

5.1 Statistical Analysis

Statistical analysis is shown by a test on the histograms of the encrypted frames of video and on the correlation coefficients between pixels in the same place in the plain and cipher frames.

1) *Histograms of encrypted images*: Histograms may reflect the distribution information of the pixel values of a video frames. An attacker can analyze the histograms of an encrypted video frames by using some attacking algorithms to get some useful information of the original video. The histograms of selected plain frames and its corresponding encrypted frames have been analyzed as shown in Fig. 4-13.

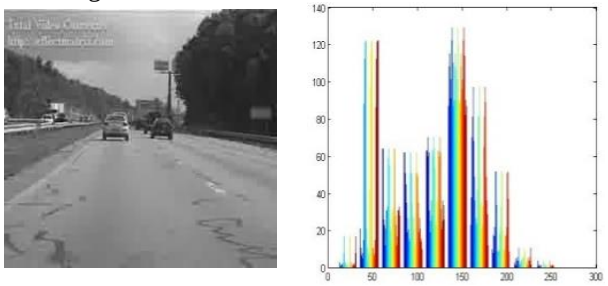

Fig. 4 The First Frame and Its Histogram.

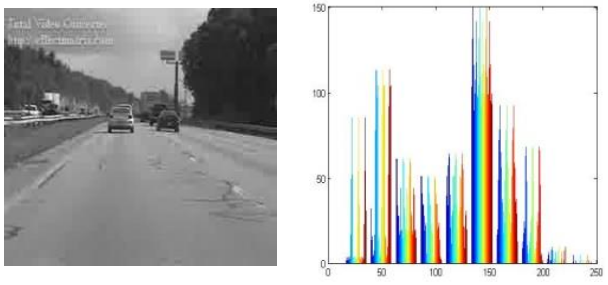

Fig. 5 The Second Frame and Its Histogram.

It can be seen that, the histogram of the encrypted image of all algorithms is fairly uniform so these algorithms are secure against statistical attack.

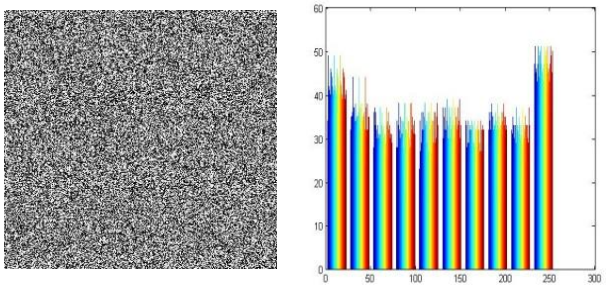

Fig. 6 The Encrypted First Frame by Proposed_1, and Its Histogram.

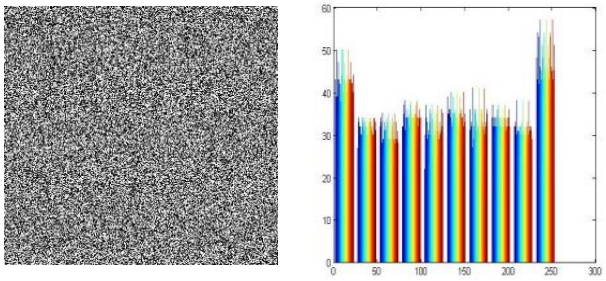

Fig. 7 The Encrypted Second Frame by Proposed_1, and Its Histogram.

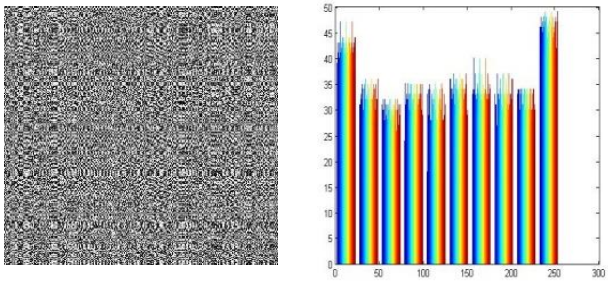

Fig. 8 The Encrypted First Frame by Proposed_2, and Its Histogram.

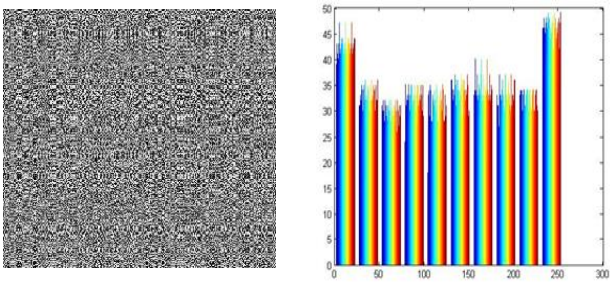

Fig. 9 The Encrypted Second Frame by Proposed_2, and Its Histogram.

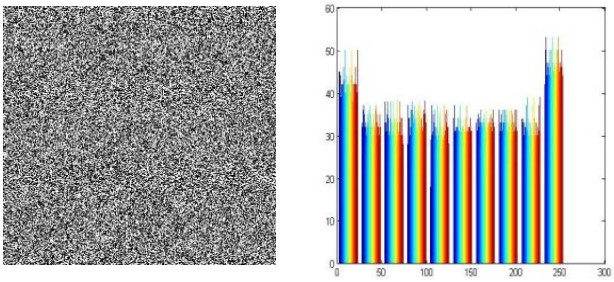

Fig. 10 The Encrypted First Frame by Proposed_3, and Its Histogram.

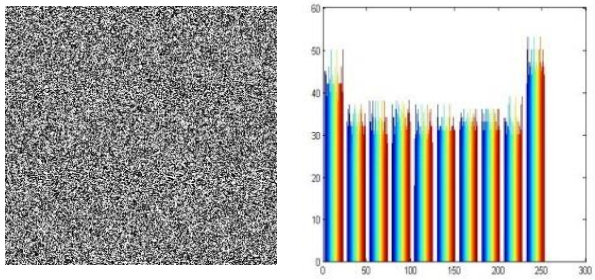

Fig. 11 The Encrypted Second Frame by Proposed_3, and Its Histogram.

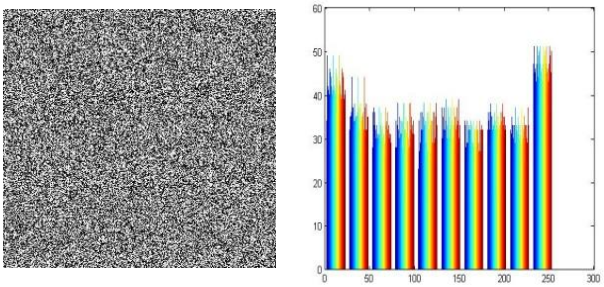

Fig. 12 The Encrypted Second Frame by AES, and Its Histogram.

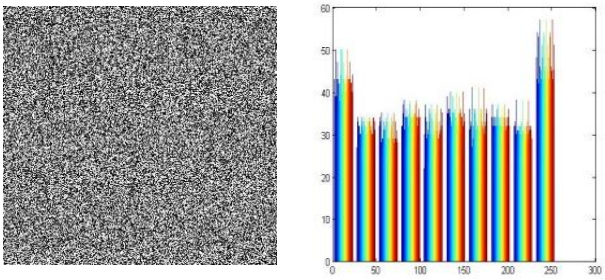

Fig. 13 The Encrypted Second Frame by AES, and Its Histogram.

2) *Correlation of Two Adjacent Pixels of Frame*: To test the correlation between two vertically adjacent pixels, two horizontally adjacent pixels, and two diagonally adjacent pixels in plain-frames and cipher-frames, respectively, the procedure is as follows: First, randomly select 1000 pairs of two adjacent pixels from a frame. Then, calculate their correlation coefficient using the following two formulas:

$$r_{xy} = cov(x,y)/\sqrt{D(x)D(y)}$$

$$cov(x,y) = E\{(x - E(x)) \times (y - E(y))\} \qquad (6)$$

where E(x) is the estimation of mathematical expectations of x, D(x) is the estimation of variance of x, and cov(x, y) is the estimation of covariance between x and y considering x and y are pixel values of two adjacent pixels in the frame. In Table 1 correlation coefficient results when used these algorithms, it can be seen that the two adjacent pixels in the plain frame are highly correlated. On the other hand, the second and third proposed algorithms have approximately no correlation with the original frame,

while AES and the first proposed algorithms have weak correlation which means that all of these algorithms resist to statistical attacks but these results also show that the second and third proposed algorithms have a strong diffusion than AES and the first proposed algorithms.

Table 1: Correlation among Frame Elements for all Algorithms.

		Adjacent Pixels Orientation		
		Vertical	***Horizontal***	***Diagonal***
Frame 1	***Plaintext***	0.9768	0.9452	0.8995
	Proposed_1	0.0331	0.026	0.0327
	Proposed_2	0.0055	0.0073	0.0234
	Proposed_3	0.0015	0.0076	0.0154
	AES	0.0259	0.0348	0.0386
Frame 2	***Plaintext***	0.9872	0.9665	0.9011
	Proposed_1	0.0249	0.032	0.0402
	Proposed_2	0.0049	0.0082	0.0225
	Proposed_3	0.0018	0.0064	0.0126
	AES	0.0231	0.0302	0.0397

5.2 Differential Analysis

In general, a desirable property for an encrypted video frames is being sensitive to the small changes in plain-frames (e.g., modifying only one pixel). Opponent can create a small change in the input frames to observe changes in the result. By this method, the meaningful relationship between original video and encrypted video can be found. If one small change in the plain-video frames can cause a significant change in the cipher-video frames, with respect to diffusion and confusion, then the differential attack actually loses its efficiency and becomes practically useless. The common measure was used for differential analysis is NPCR. To calculate NPCR, consider two ciphered frames C_1 and C_2, whose corresponding plain frame have only one pixel difference? The values of each pixels in C_1 or C_2 is labeled $C_1(i, j)$ or $C_2(i, j)$ respectively. If we define a bipolar array D with the same size as frame C_1 or C_2, with D(i, j) being determined by $C_1(i, j)$ and $C_2(i, j)$: if $C_1(i, j) = C_2(i, j)$ then D(i, j) = 0, otherwise D(i, j) = 1. Then calculating NPCR (Number of Pixels Change Rate) by

$$NPCR = \left(\left(\sum_{i,j} D(i,j)\right)/(W \times H)\right) \times 100\% \qquad (7)$$

where W is width and H is height of C_1 or C_2. Test is performed on one-pixel change influence on video. The results for our proposed algorithms and AES are given in Table 2. For the second and third proposed algorithms; NPCR is approximately 99.6% in both frames, which indicts that a swiftly change in the original video, the ciphered video will be significantly changed. Also the first proposed and AES algorithms are highly sensitive to small changes in plain video, but less than the second and third proposed algorithms. Also, from these results we can indicate that the second and third proposed algorithms have a very powerful diffusion.

Table 2: NPCR Results for Different Encryption Algorithms.

Frame 1	**(NPCR)**	**Frame 2**	**(NPCR)**
Proposed_1	98.38 %	***Proposed_1***	98.18 %
Proposed_2	99.646 %	***Proposed_2***	99.594 %
Proposed_3	99.65 %	***Proposed_3***	99.63 %
AES	97.579 %	***AES***	97.193 %

5.3 Algorithms Speed and Throughput

After measuring the ability of the proposed algorithms against statistical and differential attacks, now we measure their overall processing time, which includes initial processing, final processing, encryption and decryption times, and their throughput, which defines the number of encrypted bytes per second, to compare between them. The results of time and throughput are shown in Fig. 14 – 15. It can be seen that, the third proposed algorithm is better than other algorithms in throughput and overall processing time followed by the second proposed, the first proposed and AES algorithms.

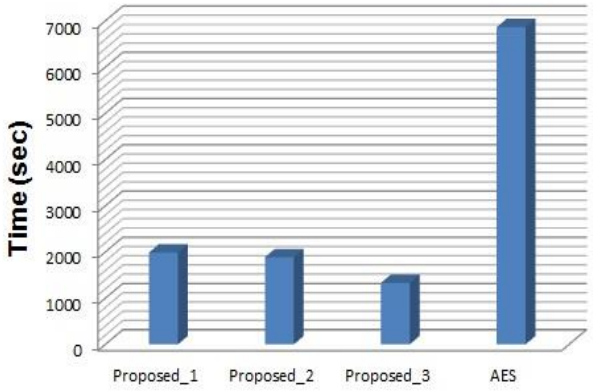

Fig. 14 Average Elapsed Time for all Algorithms.

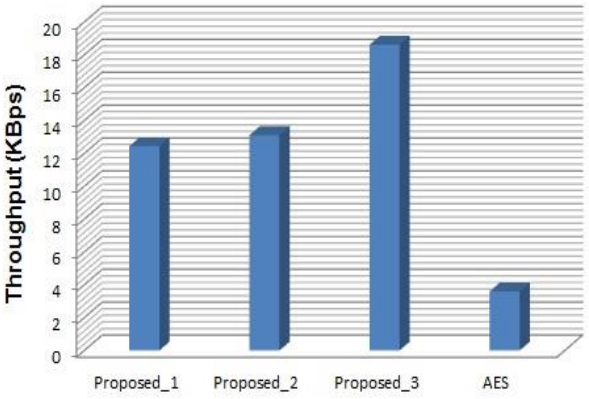

Fig. 15 Throughput for all Algorithms.

6. Conclusion

This paper presents the performance of three proposed algorithms based on chaotic maps to encrypt video in Mobile WiMax networks instead of AES algorithm. Security level of the proposed algorithms was examined anti-statistical and anti-differential attacks. The results verify and prove that the second and third proposed algorithms have a very powerful diffusion than AES, which used by Mobile WiMax standard until this moment, and that the third proposed algorithm provided a good performance results with respect to the second proposed, the first proposed and AES algorithms, respectively, in terms of overall processing time and throughput. So we can conclude that in the case of video encryption, better performances were achieved by using the third proposed algorithm when compared among other algorithms. We had already mentioned several reasons as to why we need video specific cryptosystems. Most of traditional, such as AES, cryptosystems were designed specifically to secure and encrypt text messages. Video, however, has much different properties, which make it less suitable for many traditional cryptosystems. Videos are usually very large sized and bulky. When encrypting such bulky data, the performance overhead that is introduced with some of the traditional ciphers is generally increased for real-time applications because of the decrypted data has high redundancy. Finally, three adaptive security techniques were proposed in this paper to secure video in Mobile WiMax networks and two of them enhance the performance of encryption with their powerful diffusion.

References

[1] IEEE 802.16-2004, "IEEE Standard for Local and Metropolitan Area Networks —Part 16: Air Interface for Fixed Broadband Wireless Access Systems," IEEE Press, 2004.
[2] IEEE 802.16-2005, "IEEE Standard for Local and Metropolitan Area Networks —Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems," IEEE Press, 2005.
[3] W. Fan, A. Ghosh, C. Sankaran, and S. Benes, WiMAX system performance with multiple transmit and multiple receive antennas, Proceedings of IEEE VTC07, Ireland, 2007, pp. 2807–2811.
[4] L. Nuaymi, WiMAX Technology For Broadband Wireless Access, Chichester, UK: Wiley, 2007.
[5] J. Andrews, A. Gosh, and R. Mohammed, Fundamentals of WiMAX, Understanding Broadband Wireless Access Networking: Pearson-Prentice Hall, 2007.
[6] ALTERA, "A Scalable OFDMA Engine for WiMAX", Application note 412, version 2.1, May 2007.
[7] M. Katz, F. Fitzek, WiMAX Evolution: Emerging Technologies and Applications, John Wiley & Sons, 2009.
[8] M. Ma, Current Technology Developments of WiMax Systems: Springer, 2009.
[9] K. Thaiyalnayaki and R. Dhanalakshmi, A CHAOS ENCRYPTED VIDEO WATERMARKING SCHEME FOR THE ENFORCEMENT OF PLAYBACK CONTROL, IJAET, Vol. 4,Issue 1, pp. 165-175, 2012.
[10] Z. Su, J. Jiang, S. Lian, D. Hu, C. Liang, and G. Zhang, "Selective Encryption for G.729 Speech Using Chaotic Maps", International Conference on Multimedia Information Networking and Security, 2009, pp. 488-492.
[11] L. Kocarev, and S. Lian, Chaos-Based Cryptography, Verlag Berlin Heidelberg: Springer, 2011.
[12] N. Abu Ali, A.M. Taha, and H.S. Hassanein, LTE, LTE-Advanced and WiMAX: Towards IMT-Advanced Networks, Wiley, 2012.
[13] R.C. Hincapie and J.E. Sierra, Advanced Transmission Techniques in WiMAX, University Campus STeP Ri, Slavka Krautzeka 83/A: In Tech, 2012.
[14] L. Korowajczuk, LTE, WiMAX and WLAN Network Design, Optimization and Performance Analysis, Wiley, 2011.
[15] M. Rahman, A. Hossain, H. Mouftah, A. El-Saddik, and E. Okamoto, Chaos-cryptography based privacy preservation technique for video surveillance, Multimedia Systems, Vol. 18, No. 2, pp. 145-155, 2012.
[16] Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, 2001.

Mohamed Abdel-Azim received the PhD degree in Electronics and Communications Engineering from the Faculty of Engineering-Mansoura University-Egypt by 2006. After that he worked as an assistant professor at the electronics & communications engineering department until now. He has 27 publications in various international journals and conferences. His current research interests are in multimedia processing, wireless communication systems, and field programmable gate array (FPGA) applications.

Fayez Wanis Zaki was a Head of Electronics and Communication Engineering Department at Faculty of Engineering-Mansoura University-Egypt in the period from 2004 to 2007. He is a Professor Emeritus at Electronics and Communication Engineering Department at Faculty of Engineering-Mansoura University-Egypt until now.

Awny El-Mohandes received the B.Sc. in Electronics and Communications Engineering from the Faculty of Engineering-Mansoura University-Egypt by 2008. Currently he is pursuing his Master Degree in Mansoura University-Egypt. He worked as a demonstrator at the electronics & communications engineering department until now.