Novel Fast Encryption Algorithms for Multimedia 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

Security support is mandatory for any communication networks. For wireless systems, security support is even more important to protect the users as well as the network. Since wireless medium is available to all, the attackers can easily access the network and the network becomes more vulnerable for the user and the network service provider. Worldwide Interoperability for Microwave Access (WiMax) is going to be an emerging wireless technology nowadays. With the increasing popularity of Broadband internet, wireless networking market is thriving. In the IEEE 802.16e, security has been considered as the main issue during the design of the protocol. However, security mechanism of WiMax still remains an open research field. WiMax is relatively a new technology not deployed widely to justify the evidence of threats, risk and vulnerability in real situations. In this paper, a research is described three proposed chaos encryption techniques for multimedia transmission over Mobile WiMax physical and MAC layers. At first a global overview of the technology WiMax is given followed by an explanation of traditional encryption techniques used in WiMax. Then the proposed encryption techniques are presented with its chaos systems. Next, these techniques will be applied to different multimedia contents to compare between them and traditional techniques such as AES, IDEA, Blowfish and DES.

Keywords: *WiMax, MAC layer, PHY layer, Security and Encryption.*

1. Introduction

WiMax is the emerging broadband wireless technologies based on IEEE 802.16 standards [1]. The security sublayer of the IEEE 802.16d [1] standard defines the security mechanisms for fixed and IEEE 802.16e [2] standard defines the security mechanisms for mobile network. The security sublayer supports are to: (i) authenticate the user when the user enters in to the network, (ii) authorize the user, if the user is provisioned by the network service provider, and then (iii) provide the necessary encryption support for the key transfer and data traffic.

The IEEE 802.16e standard security architecture is based on PKMv2 (Privacy Key Management) protocol which provides a flexible solution that supports device and user authentication between a mobile station (MS) and the home connectivity service network (CSN). 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 IEEE 802.16e 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 data encryption and authentication algorithms, (ii) a key management protocol (PKM) providing the secure distribution of keying data from the BS to the MS [2]. The security sublayer of WiMax (IEEE 802.16e) standard for mobile communication depends on AES to encrypt MAC layer PDUs with different key sizes. According to the properties of multimedia; the traditional encryption algorithms that used in WiMax appear not to be ideal for the following reasons: (i) multimedia 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 digital image, adjacent pixels often have similar gray-scale values and strong correlations, or image blocks have similar patterns, while for video data, consecutive frames are similar and most likely only few pixels would differ from frame to frame. Such an extremely high data redundancy of multimedia makes the conventional ciphers fail to obscure all visible information. So in this research the traditional algorithms 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 with the transmission of different multimedia over WiMax layers.

The rest of the paper is organized as follows: The IEEE 802.16e standard overview is discussed in the next section. Section (3) discusses the traditional encryption techniques that used in the privacy sublayer. Section (4) discusses three new proposed techniques. Section (5) introduces experimental design. Section (6) presents results and discussion. Section (7) is the conclusion.

2. Mobile WiMax Overview

On July 2002, a study group called IEEE 802.16 Mobile WirelessMAN Task Group was initiated to produce an amendment covering the PHY and MAC layers for combined, fixed and mobile operations in the licensed band range. The amendment was approved in December 2005 and the new standard called IEEE 802.16e-2005was published in February 2006 [5, 6]. The scope of this standard is to provide mobility enhancement support for SS moving at the vehicular speed, in addition to corrections to 802.16-2004 fixed operation that was developed as IEEE 802.16-2004/Cor1-2005 and published along with IEEE 802.16e-2005. 802.16e (IEEE 802.16e-TG, 2006) introduces many changes to PHY and MAC layer protocols owing to mobility support, which required addressing new issues that were not required in 802.16-2004, such as handoff and power management.

2.1 Mobile WiMax PHY Layer

The IEEE 802.16e operation is limited to licensed bands suitable for mobility below 6GHz. This may introduce a compatibility problem between 802.16-2004 and 802.16e, since the available licensed spectrum may need to be split between the two technologies. This standard defines a new PHY air interface “scalable-OFDMA (S-OFDMA)” besides those defined by 802.16-2004. S-OFDMA uses FFT size of 128, 512, 1024, or 2048 subcarriers. S-OFDMA uses this number of subcarriers to provide the ability to scale system bandwidth while at the same time the subcarrier separation and symbol duration remain constant as the bandwidth changes [7]. Thus, the BS determines the subcarrier used to adapt to its devices’ channel conditions. The AAS, space time code, and closed-loop MIMO modes are enhanced in 802.16e to improve coverage and data transmission rate [4]. Additionally, support for coordinated spatial division multiple access (SDMA) is introduced. The IEEE 802.16e includes an additional advanced low complexity coding option method, low-density parity check (LDPC) to provide for more flexible encoding. LDPC codes 6 bits for every 5 data bits with a rate of 5/6. This forces higher performance coding technique than the methods included in 802.16-2004 that provide 3/4 code rate [9], [10].

2.2 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 802.16e-2005 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. IEEE 802.16e-2005 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 [6], [8]. 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 802.16e supports best in class security features by adopting the best technologies available today [9], [10]. 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.

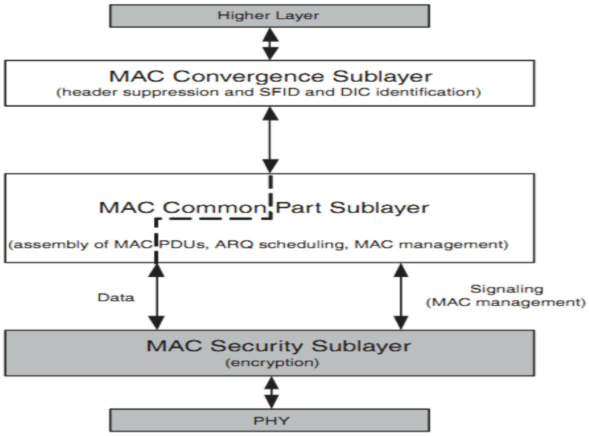
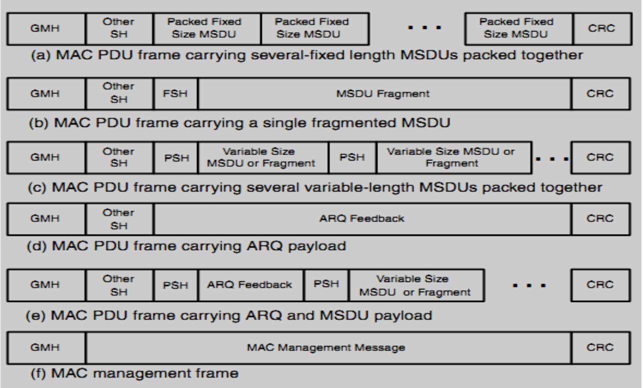


Fig. 1 WiMax protocol layers

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. 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.



(a) MAC PDU frame carrying several-fixed length MSDUs packed together

(b) MAC PDU frame carrying a single fragmented MSDU

(c) MAC PDU frame carrying several variable-length MSDUs packed together

(d) MAC PDU frame carrying ARQ payload

(e) MAC PDU frame carrying ARQ and MSDU payload

(f) MAC management frame

Fig. 2 Examples of various MAC PDU frames

3. Traditional Encryption Techniques

Encryption should be used for wireless systems to prevent over-the-air eavesdropping. Also needed at the link layer is access control to prevent unauthorized users from using network resources: precious over-the-air resources. Encryption is the method used to protect the confidentiality of data flowing between a transmitter and a receiver. Encryption involves taking a stream or block of data to be protected, called plaintext, and using another stream or block of data, called the encryption key, to perform a reversible mathematical operation to generate a ciphertext. The ciphertext is unintelligible and hence can be sent across the network without fear of being eavesdropped. The receiver does an operation called decryption to extract the plaintext from the ciphertext, using the same or different key. IEEE 802.6e privacy sublayer uses AES (Advanced Encryption Standard) as its basic encryption technique. So we will begin our explanation with this technique.

3.1 AES Algorithm

AES is a data encryption standard adopted by the National Institute of Standards as part of FIPS 197 and is specified as a link-layer encryption method to be used in WiMax. AES is based on the Rijndael algorithm, which is a block-ciphering method believed to have strong cryptographic properties. The AES algorithm operates on a 128-bit block size of data, organized in a 4 × 4 array of bytes called a state. The encryption key sizes could be 128, 192, or 256 bits long; WiMax specifies the use of 128-bit keys [11].
AES algorithm divided into nine rounds in each round four operations are performed on a plaintext: (i) SubBytes operation, (ii) ShiftRows operation, (iii) MixColumns operation and (iv) AddRoundKey operation. Before these rounds an AddRoundKey operation is applied to the state matrix and after these rounds three operations are applied to the output of the algorithm: (i) SubBytes operation, (ii) ShiftRows and finally (iii) AddRoundKey operation.

3.2 IDEA Algorithm

IDEA (International Data Encryption Algorithm) is a block cipher; it operates on 64-bit plaintext blocks. The key is 128 bits long. This algorithm is a symmetric key algorithm. As with all the other block ciphers we've seen, IDEA uses both confusion and diffusion. The design philosophy behind the algorithm is one of "mixing operations from different algebraic groups." Three algebraic groups are being mixed, and they are all easily implemented in both hardware and software (XOR, Addition modulo (2^{16}) and Multiplication modulo (2^{16} + 1)). IDEA has eight rounds total where in each round the four sub-blocks are XORed, added, and multiplied with one another and with six 16-bit subkeys [12]. Between rounds, the second and third sub-blocks are swapped. Finally, the four sub-blocks are combined with four subkeys in an output transformation.

3.3 Blowfish Algorithm

Blowfish is a 64-bit block cipher with a variable-length key. The algorithm consists of two parts: (i) Key expansion and (ii) Data encryption. Key expansion converts a key of up to 448 bits into several subkey arrays totaling 4168 bytes. Data encryption consists of a simple function iterated 16 times. Each round consists of a key dependent permutation, and a key-and data-dependent substitution. All operations are additions and XORs on 32-bit words. The only additional operations are four indexed array data lookups per round. Blowfish uses a large number of subkeys. These keys must be pre-computed before any data encryption or decryption. The P-array consists of 18 × 32-bit subkeys: P1, P2... P18. Four 32-bit S-boxes have 256 entries each: S(1)(0), S(1)(1),..., S(1)(255) & S(2)(0), S(2)(1),..., S(2)(255) & S(3)(0), S(3)(1),..., S(3)(255) & S(4)(0), S(4)(1),..., S(4)(255) [13].

3.4 DES Algorithm

DES is a block cipher; it encrypts data in 64-bit blocks. A 64-bit block of plaintext goes in one end of the algorithm and a 64-bit block of ciphertext comes out the other end. DES is a symmetric algorithm: The same algorithm and key (which consists of 56 bits) are used for both encryption and decryption [12]. At its simplest level, the algorithm is nothing more than a combination of the two basic techniques of encryption: confusion and diffusion. The fundamental building block of DES is a single combination of these techniques, based on the key. This is known as a round. DES has 16 rounds; it applies the same combination of techniques on the plaintext block 16 times.

4. Proposed Algorithms

Multimedia data 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, multimedia is encrypted by shuffling samples and then changing these values by applying different chaotic maps to create an encrypted data [12], [16].

The idea of using chaos for data encryption is certainly not new and can be traced to the classical Shannon's paper [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.

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.

4.1 The First Proposed Algorithm

The multimedia samples values are rearranged using 2D CAT map that is defined by Eq. (1) and then the values of pixel are changed using 1D logistic map [14], [15] that is defined by Eq. (2).

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

Where a and b are random number from 0 to 256 according to 256 bits key.

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

The initial value X_0 depends on 256 bits key and generated by a special algorithm.

4.2 The Second Proposed Algorithm

The multimedia samples values are rearranged using 2D Henon map [16] that is defined by Eq. (3) and then the values of pixel are changed using two 1D logistic maps that is defined by Eq. (2).

$$\begin{aligned} X_{n+1} &= 1 + Y_n - 1.4X_n^2 \\ Y_{n+1} &= 0.3X_n \end{aligned} \qquad (3)$$

The initial values Y_0 and X_0 depends on 128 bits key and generated by a certain algorithm.

4.3 The Third Proposed Algorithm

The multimedia samples values are rearranged using 2D Baker map [16] that is defined by Eq. (4) and then the values of pixel 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 $N_i \leq r$, $r < (N_i + n_i)$ and $0 \leq s < N$ is mapped to a new location using Eq. (4).

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

Where for the second and third proposed algorithms we used two 1D logistic map and 2D Henon map to do a diffusion process according to Eq. (5).

$$D_n = Y_n \times (B_n + X_n)\ mod\ 256 \qquad (5)$$

5. Experimental Design

In this paper different algorithms will be used to encrypt multimedia in WiMax privacy sublayer such as AES, IDEA, Blowfish, DES, three proposed algorithms. 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) the performance of traditional cryptosystems (i.e. IDEA and Blowfish) will be examined in WiMax to encrypt multimedia. AES algorithm will be taken as a reference of comparison; (ii) encryption algorithms based on chaotic maps have been proposed to encrypt multimedia data; (iii) security level of the proposed algorithms has been examined by using the correlation among image element; (iv) comparison among the different encryption algorithms have been made in terms of the encryption time and throughput to encrypt different data types, and (v) the performance of these encryption algorithms will be examined when the encrypted data transmission through the IEEE 802.16e PHY layer.

5.1 IEEE 802.16e PHY Layer Parameters

WiMax PHY Layer includes various functional stages: (i) Bit-level processing (randomization, FEC encoding, interleaving and symbol mapping), (ii) S-OFDMA symbol-level processing (subchannelization pilot insertion, IFFT and cyclic prefix) and (iii) Digital IF processing (single antenna and multi-antenna digital up converter (DUC), advanced crest-factor reduction (CFR) and digital predistortion (DPD)). The standard defines two types of parameters, the primitive parameters, that will be specified by users or system requirements and the derived parameters, defined in terms of the primitive ones. S-OFDMA parameters are given in Table 1.

5.2 IEEE 802.16e MAC Layer Parameters

The model of MAC frame structure takes into account MAC-header, CRC, broadcast MAC management messages. The scheduling is based on a fair queuing algorithm where all SSs are treated equally; ARQ is also disabled.

Table 1: S-OFDMA Parameters

Type	***Parameters***	***value***
Primitive	Channel Bandwidth (BW)	20 MHz
	Number of data Subcarriers (N_{data})	1440
	Number of pilot Subcarriers (N_{pilot})	240
	Left guard interval	184
	Right guard interval	184
	Guard Time/Useful symbol Time(G)	1/16
	IFFT points (N_{FFT})	2048
	Number of used subcarriers (N_{used})	1680
Derived	Sampling frequency (f_s)	ceil(N_{used}×BW/2)
	Subcarrier Spacing (Δf)	$\Delta f = f_s / N_{FFT}$
	Useful symbol time (T_b)	$T_b = 1 / \Delta f$
	CP time (T_g)	$T_g = G \times T_b$
	S-OFDMA symbol time (T_s)	$T_s = T_b + T_g$
	Sampling time (T)	$T = 1 / f_s$

6. 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 recovered data. For image it is of joint photographic expert group (JPEG) format of gray scale style and resolution 256×256 with 64 KB size. 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. The audio file that we used is of Microsoft WAV format with 256 KB size, 8 bits per sample and 48 KHz sampling frequency.

6.1 Results of Image Data

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 digital images under the statistical attacks, and the differential attacks. Statistical analysis is shown by a test on the histograms of the encrypted images and on the correlation coefficients between pixels in the same place in the plain and cipher images: (i) Histograms of encrypted images: Histograms may reflect the distribution information of the pixel values of an image. An attacker can analyze the histograms of an encrypted image by using some attacking algorithms to get some useful information of the original image. The histograms of plain image and its corresponding encrypted images have been analyzed as shown in Fig. 3-10.

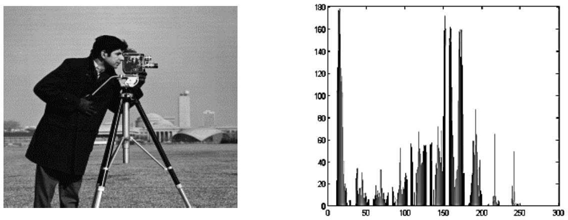


Fig. 3 Original Image and Its Histogram

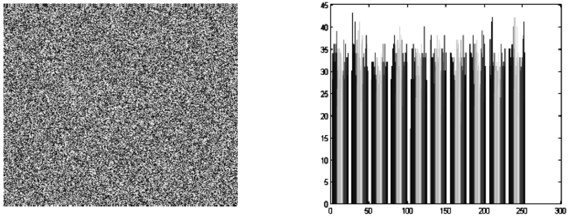


Fig. 4 Encrypted image of AES and Its Histogram

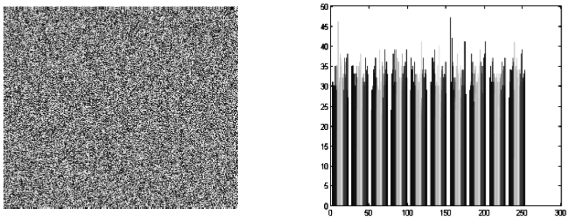


Fig. 5 Encrypted image of IDEA and Its Histogram

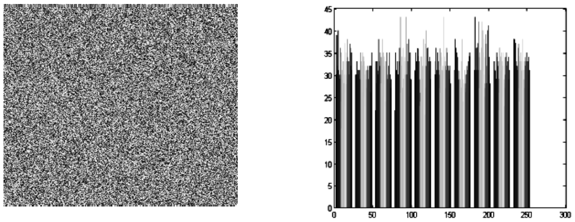


Fig. 6 Encrypted image of Blowfish and Its Histogram

It can be seen that, the histogram of the encrypted image of all algorithms is fairly uniform so these algorithms are secure against statistical analysis attack, and (ii) Correlation of two adjacent pixels: To test the correlation between two vertically adjacent pixels, two horizontally adjacent pixels, and two diagonally adjacent pixels in plain-image and cipher-images, respectively, the procedure is as follows: First, randomly select 1000 pairs of two adjacent pixels from an image. Then, calculate their correlation coefficient using the following two formulas:

$$cov(x,y) = E(x - E(x)) \times E(y - E(y))$$
$$r_{xy} = cov(x,y) \,/\, \sqrt{D(x)D(y)} \qquad (6)$$

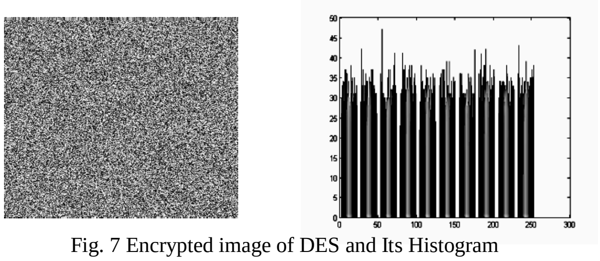


Fig. 7 Encrypted image of DES and Its Histogram

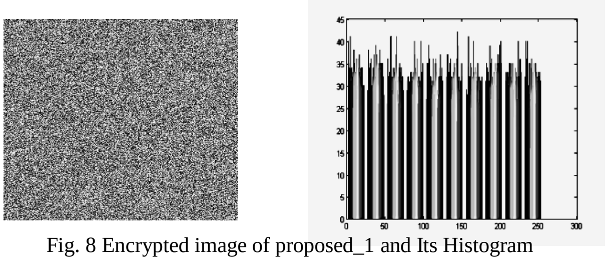


Fig. 8 Encrypted image of proposed_1 and Its Histogram

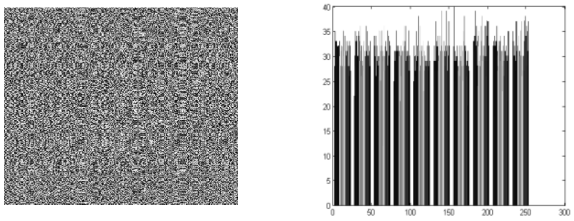


Fig. 9 Encrypted image of proposed_2 and Its Histogram

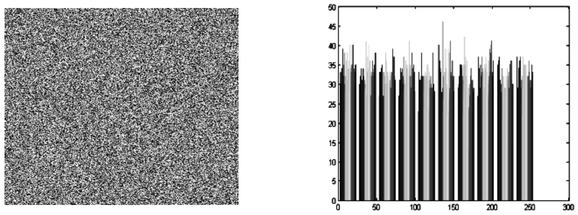


Fig. 10 Encrypted image of proposed_3 and Its Histogram

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 image. In Table 2 correlation coefficient results when used these algorithms, it can be seen that the two adjacent pixels in the plain image are highly correlated. On the other hand, all proposed algorithms and DES have very weak or no correlation with the original image. AES, IDEA and blowfish have a low correlation coefficient between pixels in the same place in the plain and the cipher images which means that they resist to statistical attacks.

Table 2: Correlation among image elements for algorithms

Image	Adjacent Pixels Orientation		
	Vertical	Horizontal	Diagonal
Plaintext	0.9547	0.9269	0.8995
AES	0.0159	0.0317	0.0086
IDEA	0.0201	0.029	0.013
Blowfish	0.035	0.0464	0.002
DES	0.002	0.0439	0.0106
Proposed_1	0.0015	0.028	0.0327
Proposed_2	0.0045	0.0073	0.0234
Proposed_3	0.0341	0.0072	0.0154

In general, a desirable property for an encrypted image is being sensitive to the small changes in plain-image (e.g., modifying only one pixel). Opponent can create a small change in the input image to observe changes in the result. By this method, the meaningful relationship between original image and encrypted image can be found. If one small change in the plain-image can cause a significant change in the cipher-image, 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 Number of Pixels Change Rate (NPCR). To calculate NPCR, consider two ciphered images C_1 and C_2, whose corresponding plain images 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 image 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. NPCR is calculated using Eq. (7)

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

where W is width and H is height of C_1 or C_2. Test is performed on one-pixel change influence on Cameraman image of size 256×256. The results for proposed and traditional algorithms are given in Table 3.

Table 3: NPCR results for different encryption algorithms

Image	Number of Pixels Change Rate (NPCR)
AES	97.579 %
IDEA	98.599 %
Blowfish	96.395 %
DES	99.6 %
Proposed_1	99.6 %
Proposed_2	99.6 %
Proposed_3	98.88 %

For proposed_1, proposed_2 and DES NPCR=99.6%, which indicts that a swiftly change in the original image, the ciphered image will be significantly changed. Also proposed_3 and IDEA is highly sensitive to small changes in plain image. But AES and Blowfish have less sensitivity than other algorithms. Generally, these results show that the proposed_1, proposed_2 and DES algorithms have a very powerful diffusion.

6.2 Encryption Results of Others Multimedia

We found that any video data consists of a certain number of frames which have same properties as images. So from the last results we can determine that all proposed algorithms have very powerful diffusion and resist to statistical attacks. But in case of audio and speech data we can test the performance of algorithms by (i) checking the frequency domain of encrypted data to know the amount of randomization caused by the algorithm on data to create ciphertext, (ii) the average elapsed time for both encryption and decryption and (iii) throughput. The frequency domain of audio data and encrypted audio data according to all algorithms are shown in Fig. 11-18, and the elapsed time and throughput for all algorithms applied to image, video and audio are shown in Fig. 19-24.

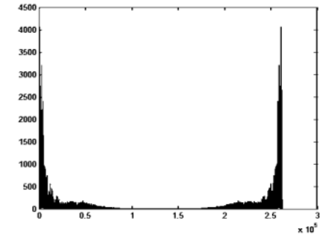


Fig. 11 Frequency domain of audio data

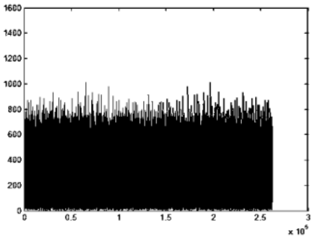


Fig. 12 Frequency domain of AES encrypted data

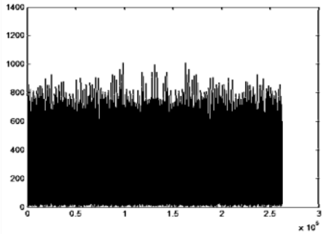


Fig. 13 Frequency domain of IDEA encrypted data

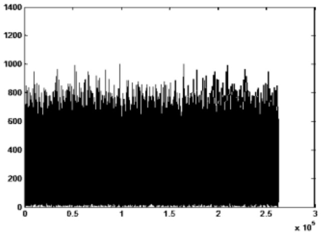


Fig. 14 Frequency domain of Blowfish encrypted data

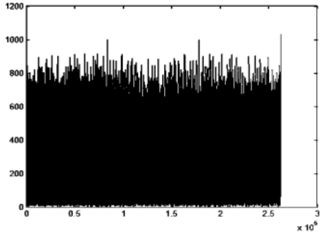


Fig. 15 Frequency domain of DES encrypted data

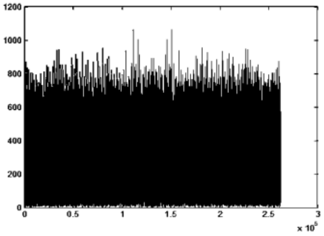


Fig. 16 Frequency domain of Proposed_1 encrypted data

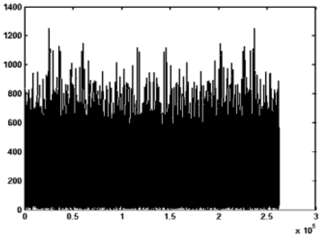


Fig. 17 Frequency domain of Proposed_2 encrypted data

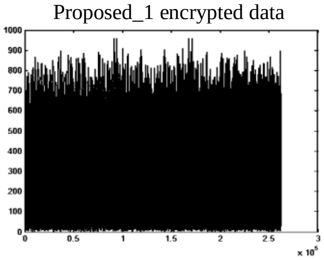


Fig. 18 Frequency domain of Proposed_3 encrypted data

It can be seen that, proposed_3 is better than other algorithms in throughput and encryption time followed by proposed_2, proposed_1, blowfish, IDEA, AES and DES. The image, video and audio sizes are often larger than text. Consequently, the traditional encryption algorithms need longer time to encrypt multimedia data than encryption algorithms based on chaotic systems.

7. Conclusion

This paper presents the performance of selected traditional encryption algorithms (i.e. IDEA, Blowfish and DES) and three proposed algorithms based on chaotic maps to encrypt different data types in IEEE 802.16e. Security level of proposed algorithms is examined anti statistical and differential attacks. The results verify and prove that all of the proposed algorithms are highly secure and that Blowfish is better than IDEA, AES and DES in terms of average elapsed time and throughput. For multimedia better performances are achieved for proposed_1 and proposed_2 when compared among other algorithms. We have already mentioned several reasons as to why we need multimedia specific cryptosystems. Most of traditional cryptosystems were designed specifically to secure and encrypt text messages. Digital multimedia data, however, have much different properties, which make them less suitable for many traditional cryptosystems. Multimedia data includes images, videos, speech and audio which 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 image has high redundancy. Finally, the adaptive security is proposed in this paper to secure different data types in IEEE 802.16e.

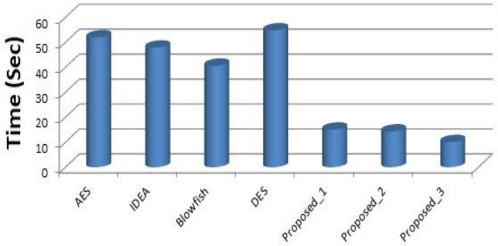


Fig. 19 Average elapsed time of different encryption algorithms for image file

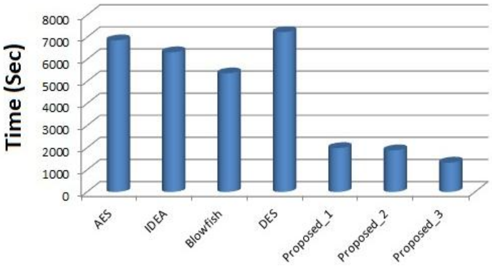


Fig. 20 Average elapsed time of different encryption algorithms for video file

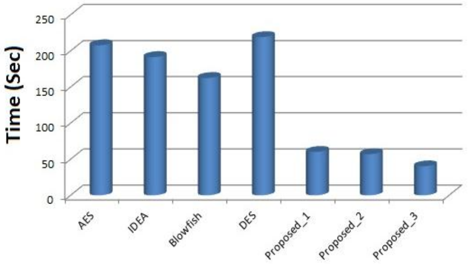


Fig. 21 Average elapsed time of different encryption algorithms for audio file

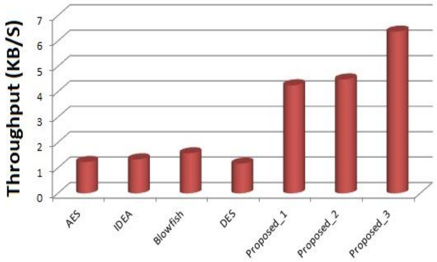


Fig. 22 Throughput of different encryption algorithms for image file

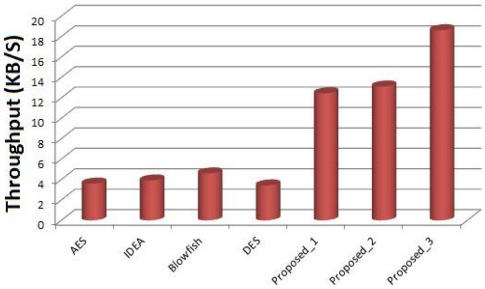


Fig. 23 Throughput of different encryption algorithms for video file

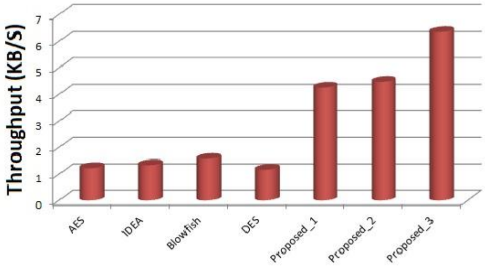


Fig. 24 Throughput of different encryption algorithms for audio file

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] T. Cooklev, Wireless Communication Standards—A Study of IEEE 802.11, 802.15 and 802.16,NewYork: IEEE Press, 2004.

[4] 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.

[5] L. Nuaymi, WiMAX Technology For Broadband Wireless Access, Chichester, UK: Wiley, 2007.

[6] J. Andrews, A. Gosh, and R. Mohammed, Fundamentals of WiMAX, Understanding Broadband Wireless Access Networking: Pearson-Prentice Hall, 2007.

[7] ALTERA, "A Scalable OFDMA Engine for WiMAX", Application note 412, version 2.1, May 2007.

[8] F. Ohrtman, WiMAX Handbook Building 802.16 Wireless Networks, United States of America: McGraw-Hill, 2005.

[9] M. Katz, F. Fitzek, WiMAX Evolution: Emerging Technologies and Applications, John Wiley & Sons, 2009.

[10] M. Ma, Current Technology Developments of WiMax Systems: Springer, 2009.

[11] Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, 2001.

[12] B. Furht, E. Muharemagic, D. Socek, MULTIMEDIA ENCRYPTION AND WATERMARKING, USA: Springer, 2005.

[13] B. Schneier, Applied Cryptography: John Wiley & Sons, Inc., 1996.

[14] M. SaberiKamarposhti, I. AlBedawi, and D. Mohamad, "A New Hybrid Method for Image Encryption using DNA Sequence and Chaotic Logistic Map", Australian Journal of Basic and Applied Sciences, Vol. 6, No. 3, 2012, pp. 371-380.

[15] 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.

[16] L. Kocarev, and S. Lian, Chaos-Based Cryptography, Verlag Berlin Heidelberg: Springer, 2011.

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.