Improved Mobile WiMax Image Privacy Using Novel Encryption Techniques

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

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

Abstract

Mobile WiMax security standards from IEEE specify some powerful standards-based security controls, including PKMv2 EAP-based authentication and over-the-air AES-based encryption. But encryption technique does not guarantee a powerful secure end-to-end image transmission, and, consequently, WiMax presents a range of security design and integration challenges. In this paper, two proposed chaos encryption techniques were described for image transmission over Mobile WiMax network as an enhancement of image security problem in Mobile WiMax. At first, a global overview of the Mobile WiMax security sublayer was given to determine the disadvantages of recently used encryption technique. Then three selected traditional techniques and our proposed encryption techniques were presented. Next, these techniques were applied to image to examine their robustness against cipher-image attacks such as cropping, noising, and JPEG compression. It was found that our techniques are more robust than AES and the selected techniques in the presence of cipher-image attacks.

Keywords: *Security Sublayer, Traditional Techniques, Proposed Techniques, and Cipher-Image Attacks.*

1. Introduction

Security has become a primary concern in order to provide protected communication in Wireless environment. IEEE Standards Board in 1999 Established, the IEEE 802.16 is a working group on Broad Wireless Access. It has many developing standards for the global deployment of broadband Wireless Metropolitan Area Networks. In December 2001, the first 802.16 standard was established, which was designed to specialize point to multipoint broadband wireless transmission in the 10-66 GHz spectrum with only a LOS capability. But with the lack of support for NLOS operation, this standard is not suitable for lower frequency applications [1]. Therefore in 2003, the IEEE 802.16a standard was published to accommodate this requirement. Then, after being revised several times, the standard was ended in the final standard: 802.16-2004 which corresponds to revision D. These standards define the BWA for stationary and nomadic use which means that end devices cannot move between BS but they can enter the network at different locations. In 2005, an amendment to 802.14-2004, the IEEE 802.16e was released to address the mobility which enables MS to handover between BSs while communicating [2]. This standard is often called “Mobile WiMax”. Based on the IEEE 802.16 standard, the WiMax is “a telecommunications technology that provides wireless transmission of data using a variety of transmission modes, from PMP links to portable and fully mobile internet access”. WiMax is a very promising technology with many key features over other wireless technologies. For instance, WiMax network has the capability of working on many bands: 2.3 GHz, 2.5 GHz, etc., and provides scalability and mobility with high data rates with NLOS operation. It also provides strong security and strong QoS guaranteed services for data, voice, video, etc. However, in order for WiMax to achieve a maturity level and become a successful technology, more research on security, especially for images, threats and solution to these threats need to be conducted [3], [4]. Digital image transmission over WiMax requires reliable, fast and robust secure system. The requirements to fulfill the security needs of digital images have led to the development of effective image encryption algorithms. Digital images possess some intrinsic features, such as bulk data capacity, redundancy of data, strong correlation among adjacent pixels, being less sensitive as compared to the text data, etc. As a result, traditional encryption algorithms, such as DES, IDEA, Blowfish, AES (the basic encryption technique in WiMax), are thereby not suitable for practical digital image encryption due to the weakness of low-level efficiency while encrypting images [5]. Fortunately, chaos-based image encryption algorithms have shown their superior performance. So, in this paper we propose two new chaos-based encryption techniques that can be used with WiMax instead of AES or other traditional techniques and compared together to determine their features against some of cipher-image attacks. The rest of the paper is organized as follows: an overview of WiMax security sublayer and its encryption technique (AES) are introduced in the next section. Section (3) discusses IDEA, Blowfish and DES as an example of traditional encryption techniques. Section (4) introduces two new proposed techniques based on chaotic maps. Section (5) presents security analysis. Section (6) concludes the paper.

2. Mobile WiMax Security Sublayer

Mobile WiMax security specifications can mainly be found within the MAC layer. Security within the MAC layer is called the security sublayer. Its goal is to provide access control and confidentiality of the data link. Fig. 1 shows Mobile WiMax security sublayer. The separate security sublayer provides authentication, secure key exchange, and encryption [5]. When two parties establish a link, they are protected via a set of protocols that ensure confidentiality and unique access of the authorized parties. The unique handshaking between the two entities; namely base station and subscriber station, is done at the MAC layer through security sublayer, which is based on the following concepts: (i) Security associations: it is a set of security information parameters that a BS and one or more of its client SSs share in order to support secure communications, (ii) Public key infrastructure (PKI): The WiMax standard uses the Privacy and Key Management Protocol (PKM) for securely transferring keying material between the base station and the mobile station which is responsible for privacy, key management, and authorizing an SS to the BS as shown in Fig. 2, (iii) Authentication: it is the process of validating a user identity and often includes validating which services a user may access, and (iv) Data privacy and integrity: WiMax uses the AES to produce ciphertext [6], [7].

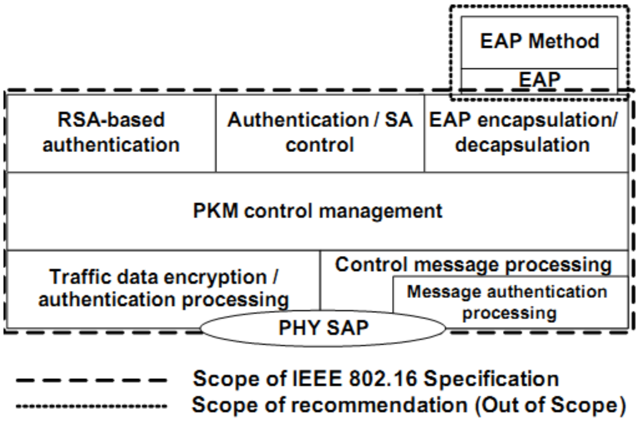
EAP Method
EAP
RSA-based authentication
Authentication / SA control
EAP encapsulation/ decapsulation
PKM control management
Traffic data encryption / authentication processing
Control message processing
Message authentication processing
PHY SAP
Scope of IEEE 802.16 Specification
Scope of recommendation (Out of Scope)

Fig. 1 Mobile WiMax Security Sublayer.

AES algorithm with 128 bits key is the recommendation of Mobile WiMax security sublayer, since it can perform stronger protection from theft of service and data across broadband wireless mobile network. Besides CCM-Mode and ECB-Mode AES algorithm, supported in Mobile WiMax, supports three more AES algorithms: CBC-Mode AES, CTR-Mode AES and AES-Key-Wrap [2], [12]. The AES cipher is almost identical to the block cipher Rijndael. The Rijndael block and key size vary between 128, 192 and 256 bits. However, the AES standard only calls for a block size of 128 bits. Hence, only Rijndael with a block length of 128 bits is known as the AES algorithm. AES does not have a Feistel structure and encrypts all 128 bits in each iteration. This is one reason why it has a comparably small number of rounds (nine rounds). AES consists of so-called layers. Each layer manipulates all 128 bits of the data path. The data path is also referred to as the state of the algorithm [13]. There are only three different types of layers: (i) Key Addition layer, (ii) Byte Substitution layer, and (iii) Diffusion layer which includes two operations; ShiftRows and MixColumns. Each round of AES, with the exception of the first, consists of all three layers. Moreover, the last round does not make use of the MixColumns transformation, which makes the encryption and decryption scheme symmetric.

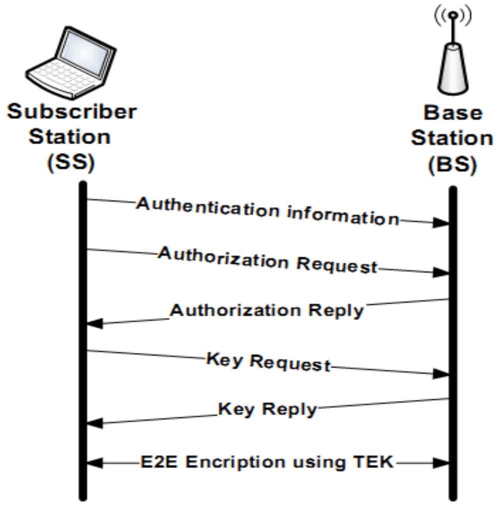

Fig. 2 Authentication and Authorization of PKM.

3. Other Traditional Encryption Techniques

The term traditional encryption techniques refers to encryption techniques which have become well-known over time, and already standardized and used in many applications by several organizations, such as DES, IDES, Blowfish, and AES.

3.1 DES Technique

DES is a Feistel cipher with 16 rounds, except that before and after the main Feistel iteration a permutation is performed. This permutation appears to produce no change to the security [12], but it was there to make the original implementation easier to fit on the circuit board. DES uses a block of plaintext that consists of 64 bits and a key has 56 bits, but is expressed as a 64-bit string. The 8th, 16th, 24th, ..., and 64th bits are parity bits, arranged so that each block of 8 bits has an odd number of 1s. This is for error detection purposes. The output of the encryption is a 64-bit ciphertext. The DES algorithm starts with a plaintext of 64 bits, and consists of three stages: (i) initial permutation,

(ii) confusion and Feistel function, and (iii) final permutation [13].

3.2 IDEA Technique

The first incarnation of the IDEA cipher, by Xuejia Lai and James Massey, surfaced in 1990. It was called PES. The next year, after Biham and Shamir's demonstrated differential cryptanalysis, the authors strengthened their cipher against the attack and called the new algorithm IPES. IPES changed its name to IDEA in 1992. IDEA 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. Between rounds, the second and third sub-blocks are swapped. Finally, the four sub-blocks are combined with four subkeys in an output transformation [14].

3.3 Blowfish Technique

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 [14]. 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).

4. Proposed Techniques

Digital images 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 images. So, simple and strong techniques have been proposed [8]. In these proposed techniques, image is encrypted by shuffling pixels and then changing their values by applying different chaotic maps to create an encrypted data [5], [10]. 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. 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 image transmission, a variety of chaos based encryption algorithms have been proposed. Recently, some chaos-based image encryption algorithms were broken due to their weakly secure encryption mechanism. To overcome the drawbacks such as weak security in chaos-based image encryption algorithms [8], we turn to find some improved chaos-based image encryption techniques with good diffusion mechanism and highly secure against cipher image attacks.

4.1 The First Proposed Technique

The pixels are rearranged using 2D Henon map [11] that is defined by Eq. (1) and then these pixels are changed using two 1D Logistic maps [9] that is defined by Eq. (2). Each Logistic map generate a different random sequence Y and X used to diffuse pixels. Where Y and X are an integer numbers generated from the fractional numbers that generated from two 1D Logistic maps using the following transformation: $X_n = (X_n \times 10^6) \bmod 256$ and $Y_n = (Y_n \times 10^6) \bmod 256$. The encryption steps are as follows:

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

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

1. Randomly generate the initial points of Henon map (x_0 and y_0) using the encryption key that has 256 bits.
2. Perform the two-dimensional Henon map on the image: Use x_0 and y_0 as control parameters to perform the discrete Henon map on two-dimensional coordinates of each pixel, generating shuffled version of the image has M pixels distributed on R×C matrix.
3. Randomly generate two initial inputs for the two Logistic maps in the range from 0 to 1 using the same encryption key.
4. 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.

5. Diffuse each pixel using the generated random values in step 4, after converting them to integers, as a two keys applied to Eq. (3).
6. The diffused data is the final encrypted image.

$$Cipher_n = K1_n \times (Plain_n + K2_n) \bmod 256 \qquad (3)$$

4.2 The Second Proposed Technique

The pixels are rearranged using 2D discretized Baker map that is defined by Eq. (4) and then these pixels are changed using 2D Henon map that is defined by Eq. (1). We used discretized Baker map in which pixel at (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) [10]. We used the random values generated by 2D Henon map to do a diffusion process according to Eq. (3). The values Y_n and X_n generated by Eq. (1) are fractional and to convert them to integer values we do the following transformation: $X_n = (X_n \times 256) \bmod 256$ and $Y_n = (Y_n \times 256) \bmod 256$. The encryption steps are as follows:

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

1. Perform the two-dimensional discretized Baker map on the image: Use Eq. (4) to perform the discretized Baker map on two-dimensional coordinates of each pixel, generating shuffled version of the image has M pixels distributed on R×C matrix.
2. Randomly generate two initial inputs for Henon map using the encryption key that has 256 bits.
3. Compute the Henon map according to Eq. (1), 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.
4. Diffuse each pixel using the generated random values in step 3, after converting them to integers, as a two keys applied to Eq. (3).
5. The diffused data is the final encrypted image.

5. Security Analysis

The aim of this work is to propose a new image encryption technique that has a higher robustness against cipher-image attacks than traditional techniques, especially AES which used in Mobile WiMax system. Cipher-image attack means that the opponent performs image processing like cropping, noising, compression, etc., on the cipher-images. The opponent can just damage the cipher-images if he does not need to know the secret. In such a case, the cryptosystem's robustness against such a kind of malicious attacks is very important.

5.1 Experimental Design

In this paper two different proposed and three different traditional encryption techniques will be used to encrypt images 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 techniques based on chaotic maps have been proposed to encrypt image in Mobile WiMax; (ii) using AES, DES, IDEA and Blowfish also to encrypt the same image in Mobile WiMax; (iii) the robustness of all techniques are examined in the presence of cipher-image attacks such as JPEG compression, salt and pepper noise, speckle noise, histogram equalization, gamma correction, median filter and cropping attacks.

5.2 Results and Discussion

The robustness of the discussed encryption techniques against cipher-image attacks was evaluated using PSNR, which can be calculated using Eq. (5), between the original image and the decrypted image. In our work, we used "cameraman" image, it is of joint photographic expert group (JPEG) format of gray scale style and resolution 256×256 with 64 KB size. Tables 1-2 show the results of tests to cipher-image attacks and Fig. 3-20 show the decrypted images of all techniques under different types of cipher-image attacks.

$$PSNR = 10 \times \log_{10}((2^8 - 1)^2 / MSE) \qquad (5)$$

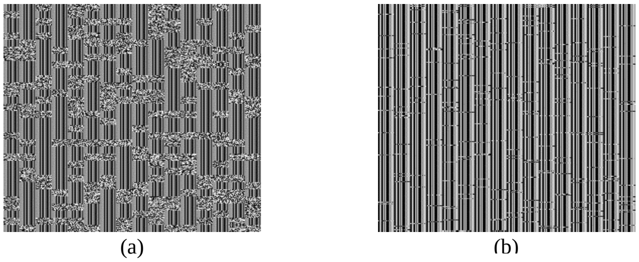

Fig. 3 AES Decrypted Images: (a) JPEG Compression and (b) Histogram Equalization.

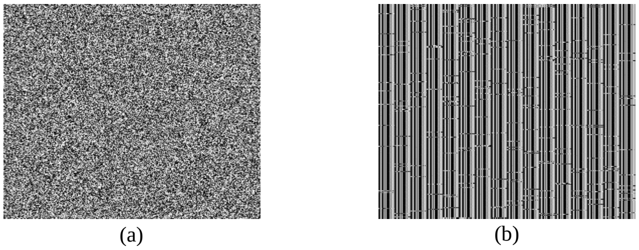

Fig. 4 AES Decrypted Images: (a) 3×3 Median Filter and (b) Gamma Correction.

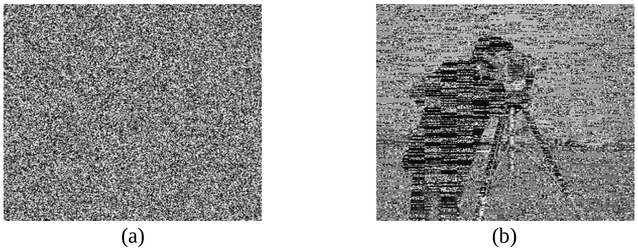
(a) (b)

Fig. 5 AES Decrypted Images: (a) Speckle Noise and (b) Salt & Pepper Noise.

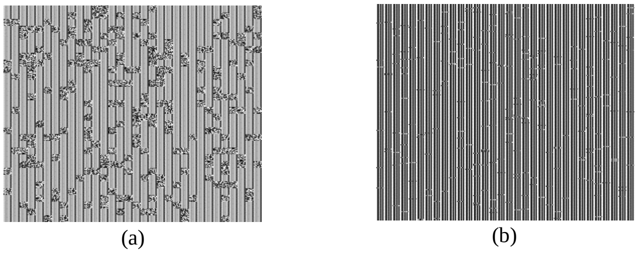
(a) (b)

Fig. 6 DES Decrypted Images: (a) JPEG Compression and (b) Histogram Equalization.

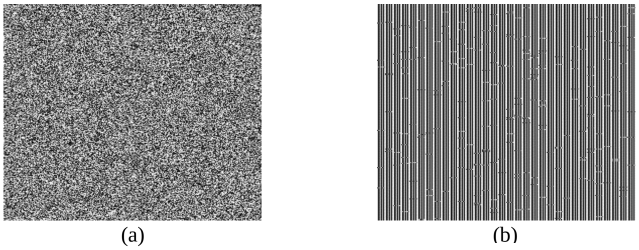
(a) (b)

Fig. 7 DES Decrypted Images: (a) 3×3 Median Filter and (b) Gamma Correction.

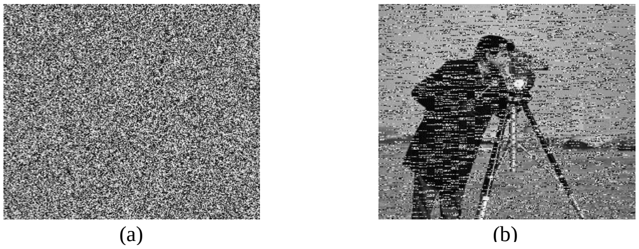
(a) (b)

Fig. 8 DES Decrypted Images: (a) Speckle Noise and (b) Salt & Pepper Noise.

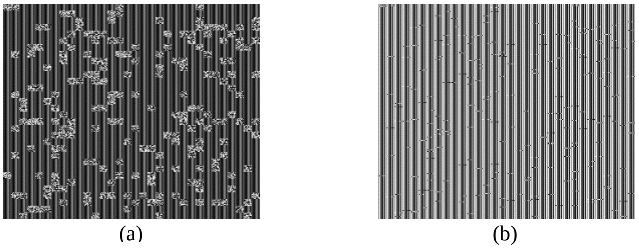
(a) (b)

Fig. 9 IDEA Decrypted Images: (a) JPEG Compression and (b) Histogram Equalization.

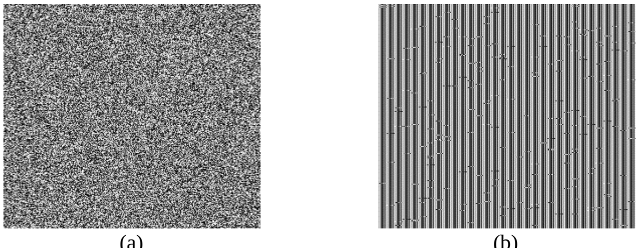
(a) (b)

Fig. 10 IDEA Decrypted Images: (a) 3×3 Median Filter and (b) Gamma Correction.

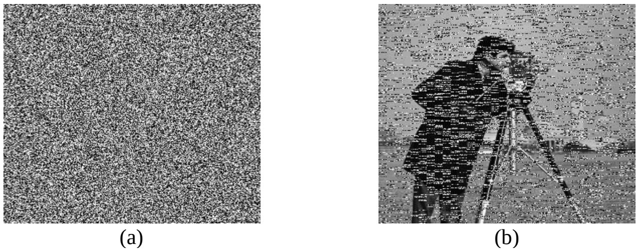
(a) (b)

Fig. 11 IDEA Decrypted Images: (a) Speckle Noise and (b) Salt & Pepper Noise.

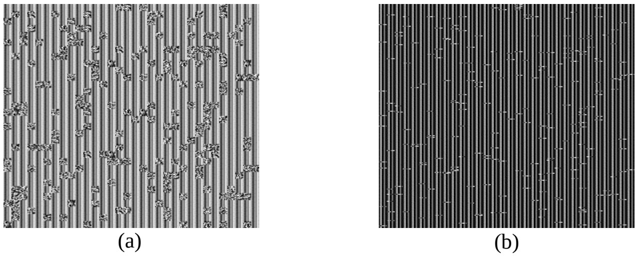
(a) (b)

Fig. 12 Blowfish Decrypted Images: (a) JPEG Compression and (b) Histogram Equalization.

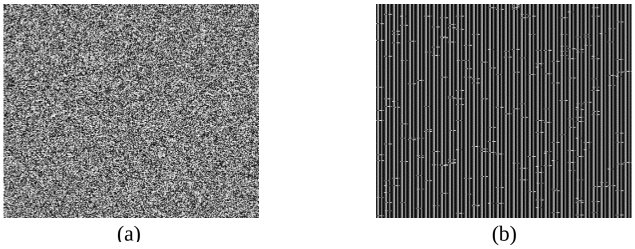
(a) (b)

Fig. 13 Blowfish Decrypted Images: (a) 3×3 Median Filter and (b) Gamma Correction.

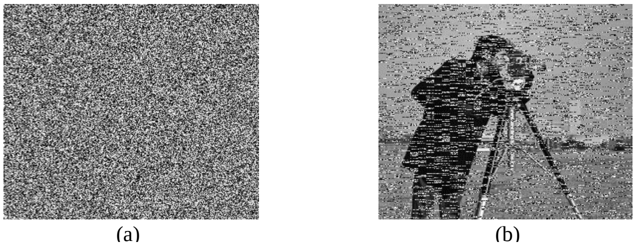
(a) (b)

Fig. 14 Blowfish Decrypted Images: (a) Speckle Noise and (b) Salt & Pepper Noise.

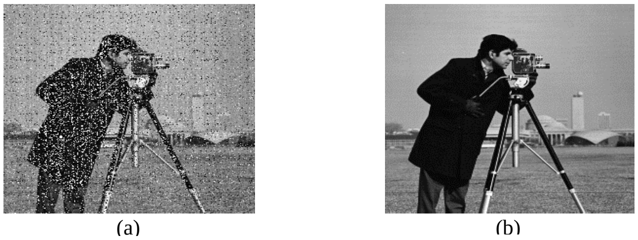

Fig. 15 Pro_1 Decrypted Images: (a) JPEG Compression and (b) Histogram Equalization.

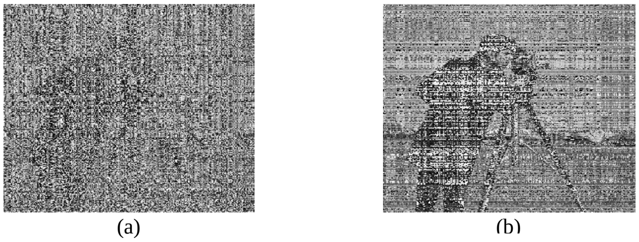

Fig. 16 Pro_1 Decrypted Images: (a) 3×3 Median Filter and (b) Gamma Correction.

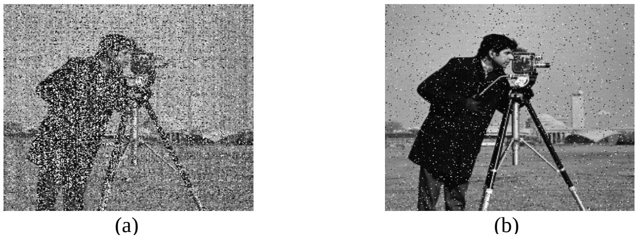

Fig. 17 Pro_1 Decrypted Images: (a) Speckle Noise and (b) Salt & Pepper Noise.

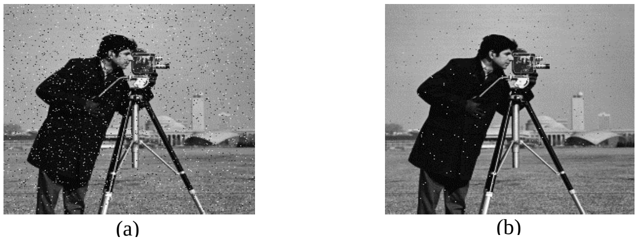

Fig. 18 Pro_2 Decrypted Images: (a) JPEG Compression and (b) Histogram Equalization.

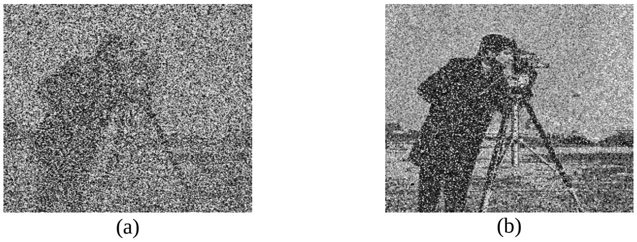

Fig. 19 Pro_2 Decrypted Images: (a) 3×3 Median Filter and (b) Gamma Correction.

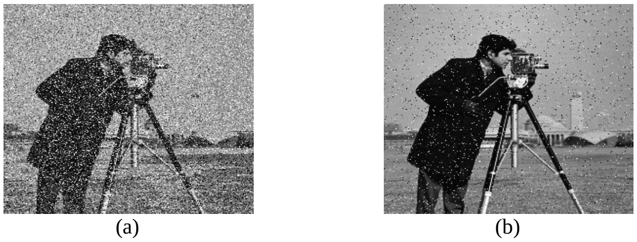

Fig. 20 Pro_2 Decrypted Images: (a) Speckle Noise and (b) Salt & Pepper Noise.

From the last figures and Tables 1-2, we can see that the proposed algorithms are robust than the traditional algorithms in salt and pepper noise attack. The traditional algorithms have no security in the presence of JPEG compression attack, gamma correction attack, histogram equalization attack, speckle noise attack, and median filter attack. The second proposed algorithm has a high robustness against all attacks, except the histogram equalization attack, followed by the first proposed algorithm. The first proposed algorithm is the most robust algorithm against the histogram equalization attack followed by the second proposed algorithm. For cropping attack, we examined three types of cropping: (i) crop 129×129 pixels from the top left corner of the cipher-image, (ii) crop 129×129 pixels from the bottom right corner of the cipher-image, and (iii) crop 137×137 pixels from the center of the cipher-image. The resulted images from the decryption process of the cropped cipher-images using all encryption algorithms are shown in Fig. 21 – 31.

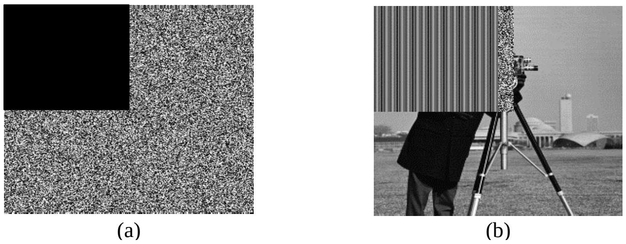

Fig. 21 (a) Top Left Corner Cropped Cipher-Image and (b) AES Decrypted Image.

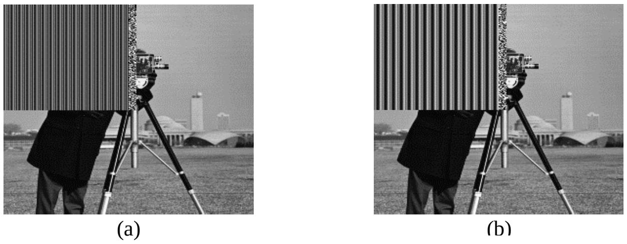

Fig. 22 (a) DES Decrypted Image and (b) IDEA Decrypted Image.

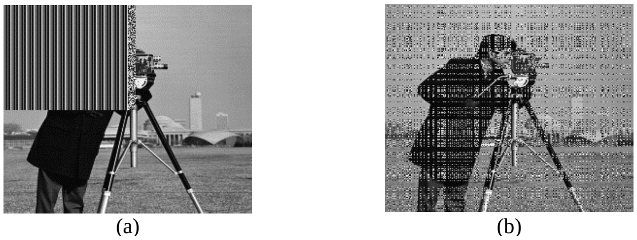
(a) (b)

Fig. 23 (a) Blowfish Decrypted Image and (b) Pro_1 Decrypted Image.

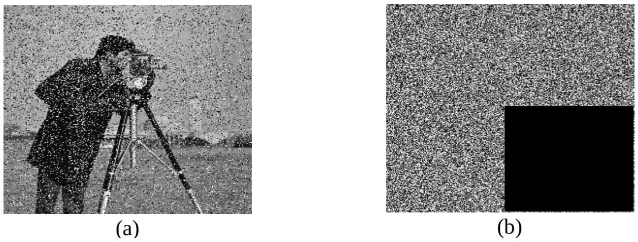
(a) (b)

Fig. 24 (a) Pro_2 Decrypted Image and (b) Bottom Right Corner Cropped Cipher-Image.

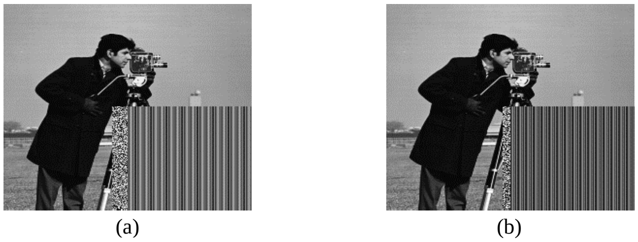
(a) (b)

Fig. 25 (a) AES Decrypted Image and (b) DES Decrypted Image.

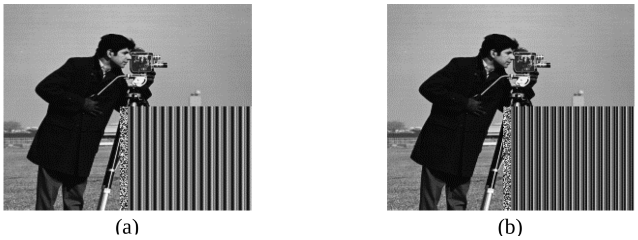
(a) (b)

Fig. 26 (a) IDEA Decrypted Image and (b) Blowfish Decrypted Image.

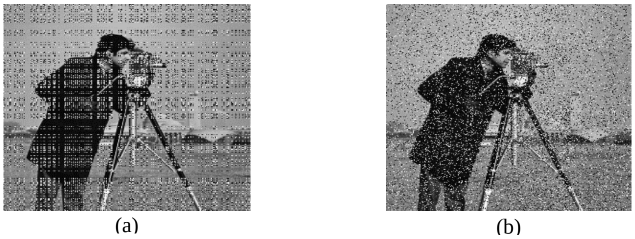
(a) (b)

Fig. 27 (a) Pro_1 Decrypted Image and (b) Pro_2 Decrypted Image.

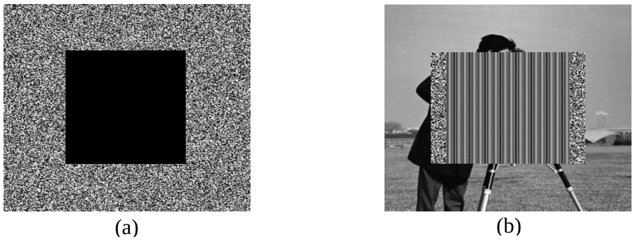
(a) (b)

Fig. 28 (a) Centered Cropped Cipher-Image and (b) AES Decrypted Image.

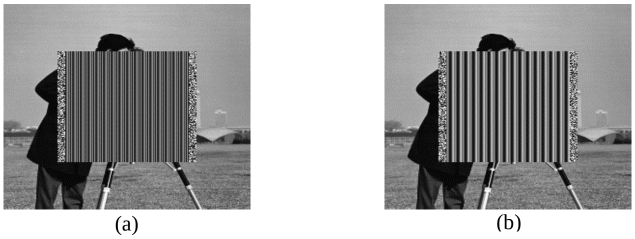
(a) (b)

Fig. 29 (a) DES Decrypted Image and (b) IDEA Decrypted Image.

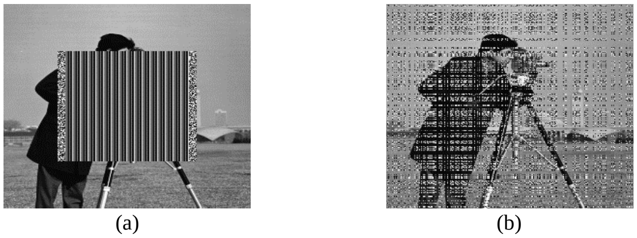
(a) (b)

Fig. 30 (a) Blowfish Decrypted Image and (b) Pro_1 Decrypted Image.

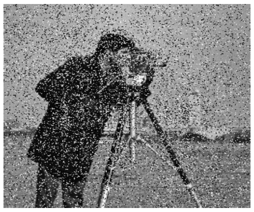

Fig. 31 Pro_2 Decrypted Image.

From these results we can see that the information of the cropped area is completely distorted in all algorithms except the proposed algorithms, so it can be called that the proposed algorithms resist all types of cropping attacks.

6. Conclusion

An efficient image encryption techniques based on chaotic maps, such as 1D Logistic, 2D Henon and 2D Baker maps, are proposed in this paper. The proposed techniques and selected traditional encryption techniques were used to encrypt images in Mobile WiMax system instead of its standard AES technique. The performance analyses including robustness against malicious attacks, such as cropping, nosing, JPEG compression, are carried out numerically and visually. The results verify and prove that all of the proposed techniques are highly secured than all other traditional techniques. For cropping attack, proposed_1 and proposed_2 algorithms are robust. For histogram equalization proposed_1 is better than proposed_2, while proposed_2 is better than proposed_1 in the presence of other attacks. Traditional algorithms have no security against all attacks except salt and pepper noise attack. From this conclusion, we can say that when Mobile WiMax standard uses the new proposed image encryption techniques, the privacy of transmitted images is actually enhanced against cipher-image attacks.

Table 1: PSNR (dB) between Original and Decrypted Images using AES, IDEA and Blowfish Techniques under Different Attacks.

	AES	**IDEA**	**B.F**
JPEG Compression With CR 50%	8.84	8.75	8.91
Salt and Pepper Noise With d = 0.05	7.92	12.98	7.89
Histogram Equalization	7.72	8.15	7.76
Median Filter With h = 3×3	8.39	8.38	8.41
Gamma Correction (γ = 0.5)	7.71	8.12	7.81
Gamma Correction (γ = 1.5)	7.73	8.16	7.77
Speckle Noise With V = 0.04	8.41	8.38	8.42

Table 2: PSNR (dB) between Original and Decrypted Images using DES, Proposed_1 and Proposed_2 Techniques under Different Attacks.

	DES	**Pro_1**	**Pro_2**
JPEG Compression With CR 50%	8.76	14.19	17.8
Salt and Pepper Noise With d = 0.05	7.31	21.51	23.49
Histogram Equalization	7.08	43.95	29.93
Median Filter With h = 3×3	8.36	9.14	9.44
Gamma Correction (γ = 0.5)	7.18	9.44	10.84
Gamma Correction (γ = 1.5)	7.09	10.15	12.57
Speckle Noise With V = 0.04	8.46	11.41	13.91

References

[1] L. Korowajczuk, LTE, WIMAX AND WLAN NETWORK DESIGN, OPTIMIZATION AND PERFORMANCE ANALYSIS, CelPlan Technologies, Inc., Reston, VA, USA: Wiley, 2011.

[2] S. Ahmadi, Mobile WiMAX A Systems Approach to Understanding IEEE 802.16m Radio Access Technology, USA: Elsevier Inc., 2011.

[3] A.M. Taha, H.S. Hassanein, and N.A. Ali, LTE, LTE-ADVANCED AND WiMAX, Canada: Wiley, 2012.

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

[5] J. Qayyum, M. Lal, F. Khan, and M. Imad, “SURVEY & ASSESSMENT OF WIMAX, ITS SECURITY THREATS AND THEIR SOLTUIONS”, International Journal of Video & Image Processing and Network Security, Vol. 11, No. 3, 2011, pp. 36-47.

[6] R. K. Jha, and U. D. Dalal, “A Journey on WiMAX and its Security Issues”, International Journal of Computer Science and Information Technologies, Vol. 1, No. 4, 2010, pp. 256-263.

[7] A. Kaushik, “Mobile WiMAX Security, Architecture and Assessment”, International Journal of Electronics and Computer Science Engineering, Vol. 1, No. 1, 2011, pp. 7-14.

[8] R. Ye, and W. Zhou, “A Chaos-based Image Encryption Scheme Using 3D Skew Tent Map and Coupled Map Lattice”, I. J. Computer Network and Information Security, Vol. 1, 2012, pp. 38-44.

[9] N. Sethi, and D. Sharma, “A NOVEL METHOD OF IMAGE ENCRYPTION USING LOGISTIC MAPPING”, International Journal of Computer Science Engineering, Vol. 1, No.2, 2012, pp. 115-119.

[10] Y. Mao, G. Chen, and S. Lian, “A NOVEL FAST IMAGE ENCRYPTION SCHEME BASED ON 3D CHAOTIC BAKER MAPS”, International Journal of Bifurcation and Chaos, Vol. 14, No. 10, 2004, pp. 3613-3624.

[11] M. Prasad, and K. L. Sudha, “Chaos Image Encryption using Pixel shuffling”, Computer Science & Information Technology, Vol. 2, 2011, pp. 169-179.

[12] C. Paar, and J. Pelzl, Understanding Cryptography, Verlag Berlin Heidelberg: Springer, 2010.

[13] W. Trappe, and L. C. Washington, Introduction to Cryptography with Coding Theory, USA: Pearson Education Inc., 2006.

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

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.