Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 12, December-2016

Hybrid Cryptographic Algorithm for LTE Data Confidentiality

Eman Ashraf Mohammed
Electronics and Communications Dept
Faculuty Of Engineering
Mansoura University,Egypt

Nihal F. F. Areed
Electronics and Communications Dept
Faculuty Of Engineering
Mansoura University,Egypt

Ali Takieldeen
IEEE Senior Member,
Alexandria University
,Egypt

Rasheed M. El-Awady
Electronics and Communications Dept
Faculuty Of Engineering
Mansoura University,Egypt

Abstract **- A proposed encryption method with AES in Counter mode algorithm is used here . It is done by applying a new key to the stream cipher RC4 and XOR the output with the cipher output of block cipher AES after making a rotation. we combine the benefits of block cipher and stream cipher to produce a new mixing algorithm in order to increase security level of transmitted data over the air interface in LTE network. The algorithm is applied to three types of input data: text, image, audio files. Shown in MATLAB how the new algorithm works. Comparing the results of AES and the proposed system and there performance analysis based on Runtime of encryption and decryption . Demonstrated that it does not add significant time to the encryption and decryption processes as the algorithm becomes more complex and it increases the avalanche effect providing more resistance to attacks and strength the randomization of the algorithm .**

KeyWords - AES, Cryptography, Key, LTE, and RC4.

I. INTRODUCTION

New threats and vulnerabilities will continue to take place. So, It is almost impossible to make a 100% secure system because [1]. For providing better reliability, higher efficiency, more data capacity and lower cost than previous generation the Long Term Evolution (LTE) ,denoted also as 4G (Fourth Generation) of mobile communication, was developed by 3GPP (Third Generation Partnership project). The LTE launched on December, 2009 by TeliaSonera in Oslo and Stockholm. LTE is exposed to different kinds of risk in term of security and reliability[2]. Proceeding from this view, more efforts should be done to increase security level of LTE network.

LTE network has three sets of cryptographic algorithms:

- First set is EEA1/EIA1 which is based on SNOW 3G algorithm
- Second set is EEA2/EIA2 which is based on AES algorithm
- Third set is EEA3/EIA3 which is based on ZUC algorithm.

Therefore, our target is study block cipher AES encryption algorithm at counter mode and developing it.

The LTE system architecture works with heterogeneous wireless access network as is a flat network that contains fewer elements of nodes than 3G/UMTS and, the main components taking part in LTE security process including authentication and authorization are UE (User Equipment), eNB (Envolved Node B) and MME (Mobility Management Entity). Packet Data Control Plane (PDCP) layer is responsible for the ciphering and integrity protection in UE and eNB side[3]. Radio Resource Control (RRC) messages are integrity protected and ciphered but User Plane (UP) data is only ciphered[4].

Many types of different keys are used in LTE security , as shown in Fig. 1. In a given algorithm, Key is the main element to encrypt data [5]. Keys are important for lots of security mechanisms, KASME is a subscriber local master key which all the other keys are derived from . Also there is the constant master key (K)[6].

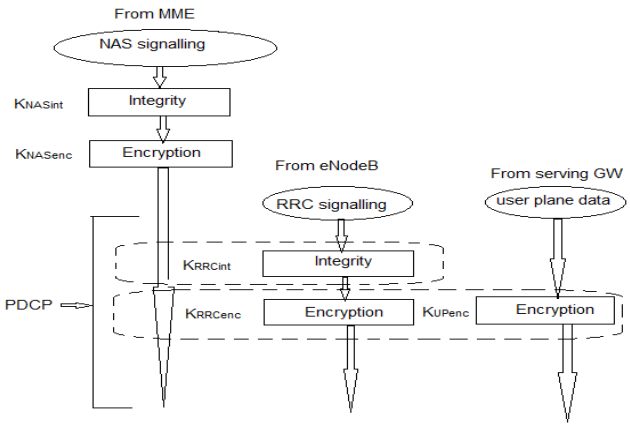


Fig -1. Security Keys in The Network [7]

II. ADVANCED ENCRYPTION STANDARD

AES, also called as Rijndael after its inventors Vincent Rijmen and Joan Daemen, uses 128-bit input blocks and can use three types of key length (128, 192 or 256 bits). For LTE encryption we use AES-128 at counter mode.

For encryption process, the steps are as shown in Fig. 2 [8].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 12, December-2016

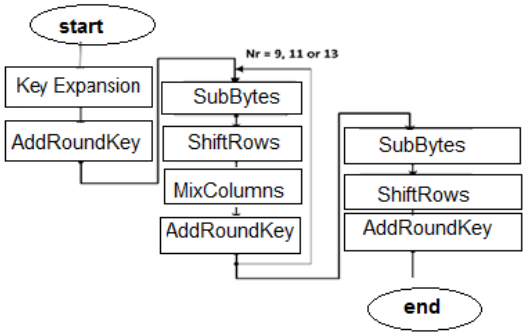


Fig -2 :AES Encryption Steps.

a) AES S-BOX

The S-box is the substitution box which serves as a lookup table. It is a matrix (square array of numbers) which is used in AES cryptographic algorithm.

b) AES Modes of Operation

The Federal Information Processing Standard (FIPS) approved five secure modes of operation supported by AES algorithm. The modes are [9]:

- Electronic Code Book Mode (ECB).
- Cipher Block Chaining Mode (CBC).
- Cipher Feedback Mode (CFB).
- Output Feedback Mode (OFB).
- Counter Mode (CTR) .

III. RC4 ALGORITHM

Symmetric key , stream cipher algorithm[10]. Both encryption and decryption process are done using the same algorithm[11]. Feeding in an encrypted message, it will produce the decrypted message output, and feeding in plaintext message, it will produce the encrypted version [12]. RC4 algorithm consists of two stages, as shown in Fig.3:

- Key-scheduling algorithm (KSA).
- Pseudo-random number generation algorithm (PRGA)[13][14][15].

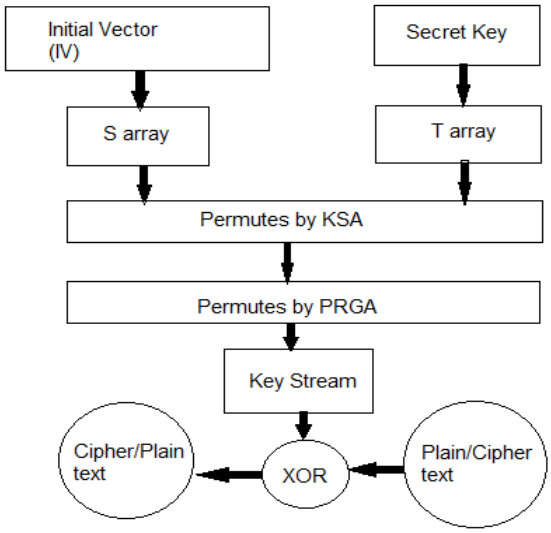


Fig -3: Encryption and decryption by RC4[16]

IV. EEA 2 CIPHERING MECHANISM

a) AES-Counter Mode

The EPS Encryption Algorithm (EEA2) is a stream cipher based on the block cipher AES-128 algorithm used in its Counter mode (CTR mode). The CTR mode can do that operation as a stream cipher. Using a suitable padding scheme, the last block must also be extended to match the cipher's block length[17].

On the network side, the encryption and decryption process takes place in the terminal and in the Radio Network Controller (RNC). This means the transferring of the cipher key (CK) from the core network to the radio access network. After the RNC has obtained CK it can switch on the encryption by sending an RRC Security Mode Command , a specific Radio Access Network Application Protocol (RANAP) message, to the terminal[17][18][19].

Only AES encrypt operation is used for both encryption and decryption process so the implementation of AES-CTR is smaller than other modes[17] .

The output is called Key- stream Block, XORing Key-stream block and plain text to get the result as Cipher Text, sending cipher text to the receiver. On the receiver side, a Key-stream Block is ready to get XORed with Cipher Text and get Plain Text back, as shown in Fig. 4.

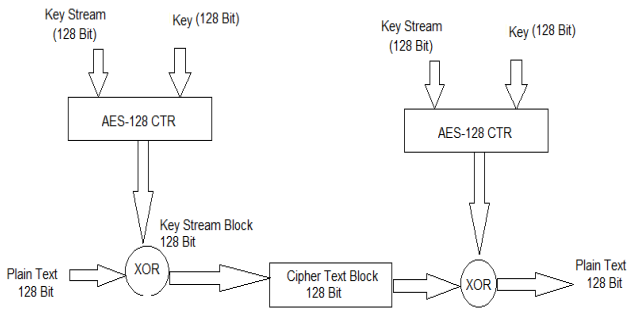


Fig -4 :EEA2 Encryption and decryption

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 12, December-2016

b) Key-Stream Generation

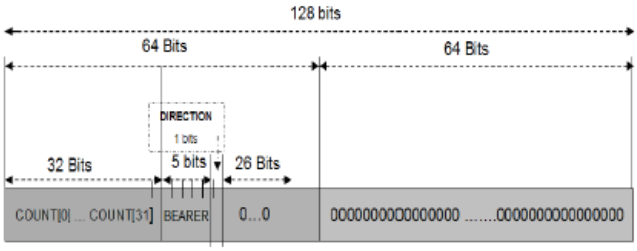


Fig -5:Key Stream T1[17]

It is required that Key- stream T has to be 128-bit long For CTR mode stream ciphering at EEA2 algorithm. Therefore, Key-stream T1, T2, T3…Ti… is constructed as follows[17]:

- COUNT-C: Frame dependent input used to synchronize the sender and the receiver.
- BEARER : Service bearer identity.
- DIRECTION : Direction of the transmission.
- LENGTH : Number of bits to be encrypted decrypted.

The least significant 64 bits of T1 are padded with all zeros so as to get a 128-bit long key stream to be suitable for a 128 bit AES algorithm, as shown in Fig 5. Then the counter is incremented every round.

V. PROPOSED SYSTEM ENCRYPTION ALGORITHM CIPHERING MECHANISM

The steps of the encryption process of the proposed algorithm, as we make a .hypered mixing algorithm of AES and RC4, are:

- Applying the key stream to the AES with 128 bit key (ck1) and get a key stream block1.
- XORing Key stream block1 and plain text to get the result as cipher text block1.
- Doing a rotation to get rotated output, Applying another key (ck2) to RC4 algorithm to get key stream block2.
- XORing key stream block2 with the rotated output to get cipher text block2, as shown in Fig.6.

The steps of decryption process are:

- XORing the cipher text block2 with key stream block2 to get the rotated output.
- Derotate the data to get cipher text block1.
- XORing it with the key stream block1 and get the plaintext again.

a) *Generation of cipher key2 (CK2)*

The used LTE keys and ck2:

```
ksH      ={'54' '49' 'c6' '4d' '20'
'00' '00' '00' '00' '00' '00' '00'
'00' '00' '00' '00'};

CK1H     ={'0a' 'f1' '8b' 'd6' 'd9'
'b0' '8b' '08' '32' '4e' '77' '6b'
'd8' 'd1' '81' '77'};
```

```
KUPencH ={'2b' '5e' '15' '26' '28'
'a5' 'd2' 'a6' 'a5' 'f7' '58' '78'
'09' 'cc' '4f' '2c'};

KRRCencH={'73' '7e' 'e6' '32' '87'
'77' 'db' '65' '7c' '9a' '9c' '4a'
'd8' '26' '3a' '44' };
```

By XORing the LTE keys (KUPenc, KRRCenc) to get the new key CK2 , as shown in Fig.7.

- KRRCenc key is used to encrypt RRC signalling traffic.
- KUPenc key is used to encrypt UP traffic.[13][6].

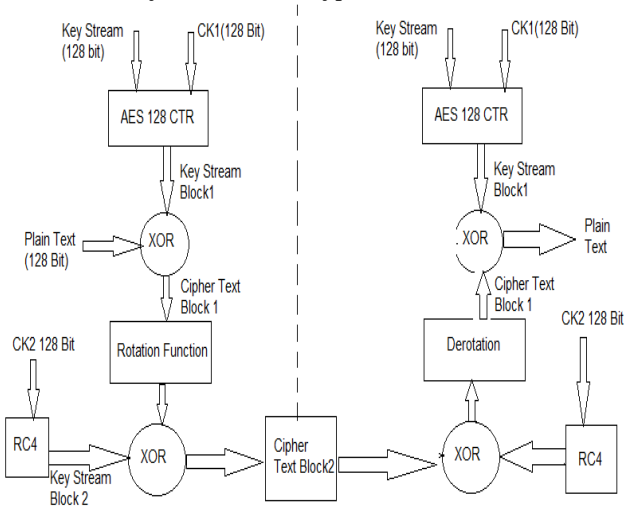


Fig -6: Encryption and decryption of proposed system

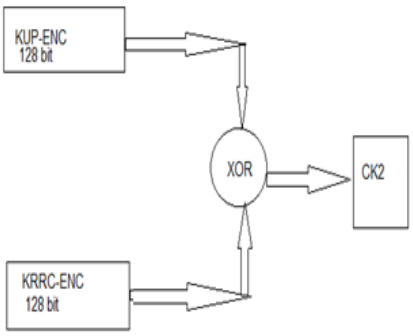


Fig -7 :Generation of Cipher Key2 (CK2)

VI. PERFORMANCE OF EEA2 VS PROPOSED SYSTEM WITH AND WITHOUT TURBO ENCODER IN AWGN

Simulating the performance of encrypted data of EEA2 system and proposed system using the system model as shown in Fig 8.The encoded bits are modulated using Quadrature Phase Shift Keying (QPSK) modulation and transmitted through the Additive White Gaussian Noise Channel (AWGN). Since AWGN is a random noise generator, Calculating Bit Error Rate (BER).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 12, December-2016

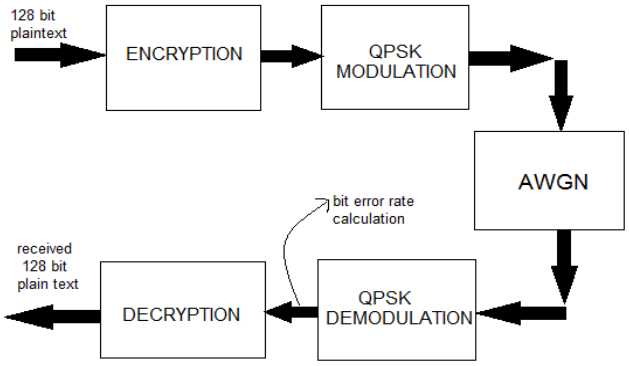


Fig -8: Implementation method without turbo encoder

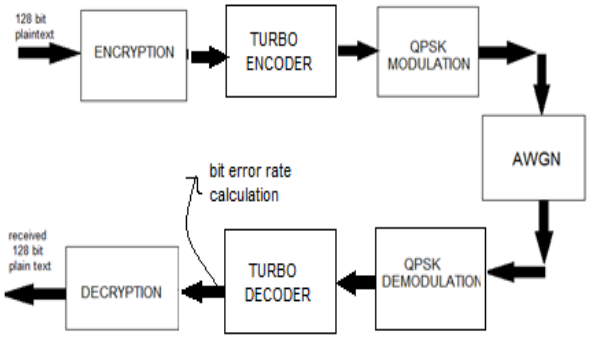


Fig -9:Improved performance with turbo encoder

When redundancy bits is sent along with data bits by the transmitter along the wireless channel, this is called channel-coding, as shown in Fig. 9 . These redundancy bits are used by the receiver for error detection and correction. the errors are caused by the channel[20]. The LTE turbo encoder consists of two parallel convolutional encoders separated by an internal interleaver. A turbo coding of a base rate of 1/3 is used for LTE . The output of the turbo encoder is composed of three streams. The bits of the first stream are Systematic bits. The bits of the second and third streams, that is the outputs of the two constituent encoders, are usually referred to as Parity 1 and Parity 2 bit streams, respectively. turbo codes can have a BER performance better than other coders[20]. From the results it is shown that there is up to 0.3 dB improvement between the old and new system in both the two cases, as shown in Fig. 10,and Fig. 11. As shown in Fig. 12 we expect a 5 dB improvement in the results. This means that in order to get a better performance we need to use channel coding algorithm.

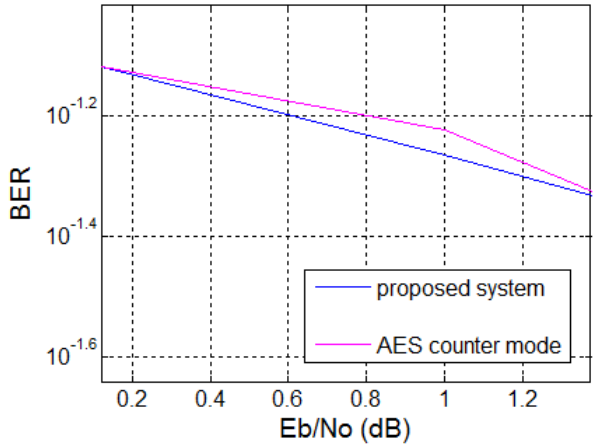


Fig -10: Bit error rate performance without channel coding

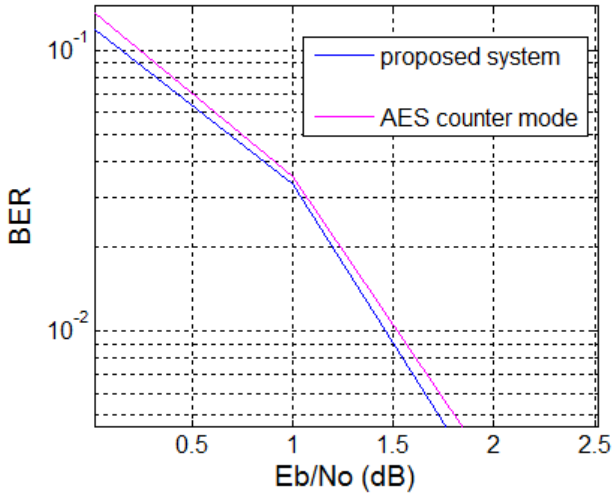


Fig -11: Bit error rate performance with turbo coding

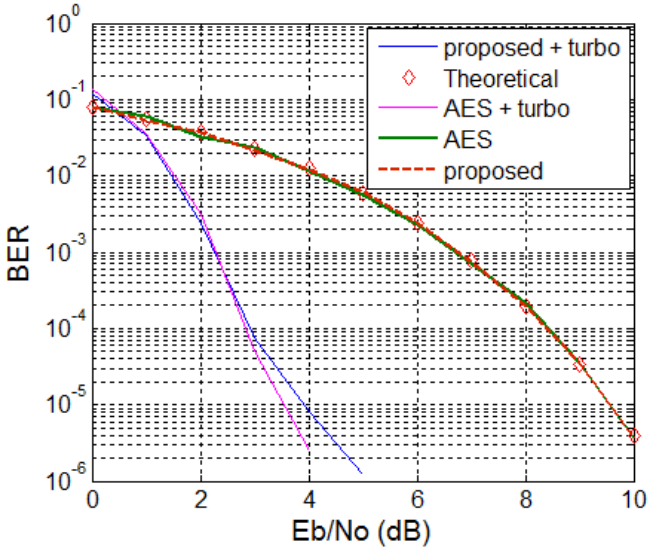


Fig -12: Performance of EEA2 VS proposed with turbo VS. without turbo encoder in AWGN

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 12, December-2016

VII. EXPERIMENTAL RESULTS

The results carried based on encryption and decryption time. As high data rate is required for 4G networks[9] . So the proposed encryption algorithm must cope up with this speed . The results are as shown below.

a) Case study 1#text :

For a text file which consists of 149 bytes, the number of bits is 1280

- **Encryption results:**

output of AES-counter mode:

Ü]ìóÄÏ±ÅøÄkI÷7';ÎAâèõ>¡S7ûz¬P„ÍÑ'kª•Sé/^Y*lðFìT³ö‹TÇ-^ æyU áöé®Úvá×´óæwA"½MìÃguÈ□wDÒ«¦é£g=GóC¡àJ'¤£@ ÌÖ•y±u<¦oí|W¥",´å□ñªú¡KØ'ò¸Jäl¼QÈ-nâG'

output of proposed system :

1°Õì´Rê>vyAß□,ÖW²□ýd"³Å[À,[ÒsLÊ□Q3Aá;¸"ñw%õm¯äƒ|P ¯Šÿ„%=º ü[¼Ò^vìEŸš¨^ä8Õgàlµ¾×yöÓúf¼ûAQ‰wQcÈßŸÓ M,JÇ.,1t+z=`±-e¡ã¢Ò6P)þ□Î§:y7Gªz¿fÊÐ‰

- Decryption results:

The purpose of LTE security is to provide a powerful defence mechanism against possible threats from the internet imposed by various types of attacks.

b) Case study 2#image :

For Image file which consists of 14.6 KB, the number of bits is 119,603.2

Fig -13:Original image, Encrypted AES image, Encrypted image of proposed system, Decrypted image

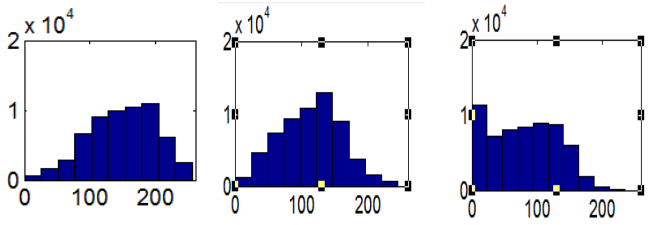


Fig -14: Histogram of original Image: red ,green ,blue

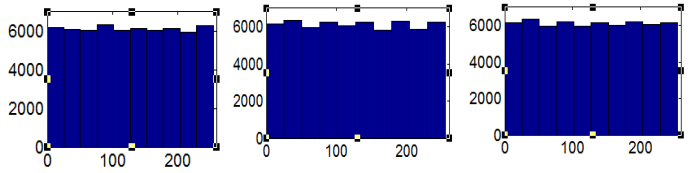


Fig -15: Histogram of AES Image: red ,green ,blue

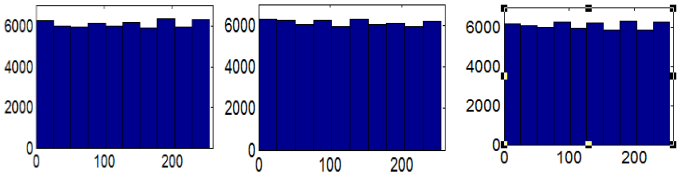


Fig -16: Histogram of proposed system Image: red ,green ,blue

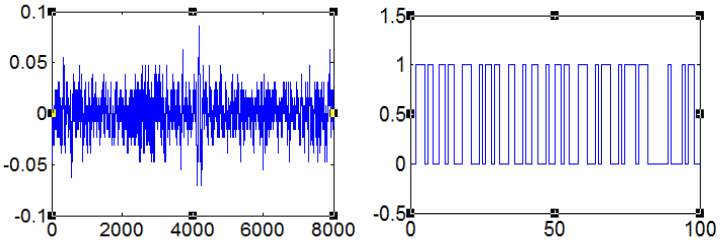
c) Case study 3#audio :

For Audio file which consists of 39.1 KB, the number of bits is 320384

Pulse Code Modulation :

The PCM samples the original audio at 8000 bits per second, which is the sampling frequency, as shown in Fig.15, in 8 bits of input and quantizes them into 256 levels (2^8). the bit rate is the sampling frequency multiplied by the number of bits. Then, calculate the maximum value of amplitude of the audio input signal. The quantization step size is two times the

maximum value of the amplitude. The step size is divided by the number of levels. We set the sampling frequency according to the Nyquist's criterion and the audio signal as a maximum frequency of 4 KHz[21]. Then, we quantize the signal. Then, we send the signal to the Decimal to Binary Stream Transformation function dec2bin () in MATLAB .



International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 12, December-2016

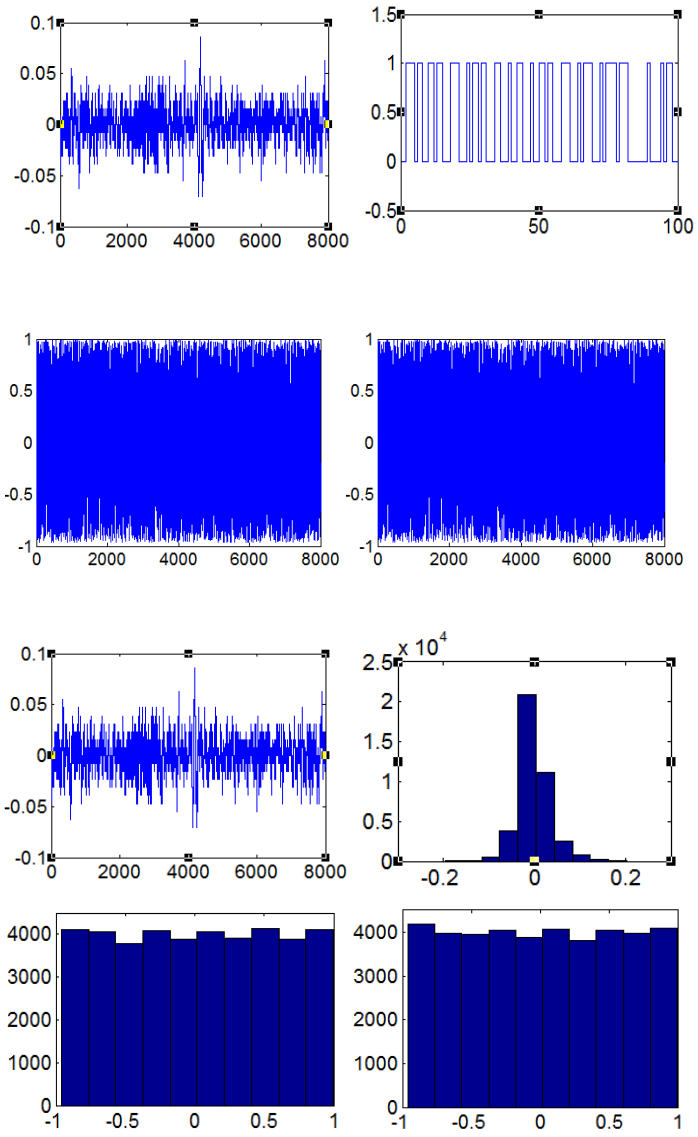


Fig -16: original signal, encoded signal, AES signal, proposed system signal, decrypted audio signal, histogram of original audio, histogram of AES signal, histogram of proposed system output

VIII. TIME RESULTS

Shown that the new enhancement of the algorithm did not add a significant time to the encryption and decryption process ,So it could be neglected

TABLE -1: Encryption time(in seconds)

	Text	Image	Audio
AES-CTR	0.008726	0.02932	0.271153
Proposed System	0.009641	0.090121	1.322274

TABLE -2: Decryption time(in seconds)

	Text	Image	Audio
AES-CTR	0.000291	0.072353	0.14045
Proposed System	0.00518	0.154736	0.330997

IX. AVALANCHE EFFECT

For any cryptographic algorithm, the avalanche effect is the most desirable property coined by Horst Feistel. There must be significant change in the output of any cryptographic algorithm when the input (plaintext or key) is changed slightly. The change of about 50% makes the algorithm truly random [22]. A random bit in the key is changed and percentage change in the cipher is outputted. Repeating the previous process for several combinations of plaintext-key (10). Averaging the results over all different plaintext-key combinations.

plain text={'35' '88' '2a' 'a9' 'b1' '83' 'c1' 'bd' '8b' 'aa' '4b' 'a1' '91' '26 ' '7b' '36'};

	Ck1	Cipher text	
change	0a 8b 6b d8 d9 b0 8b 08 36 4e 32 d1 81 77 77 fb	89 a8 26 c2 cf c7 c0 39 39 85 c5 b2 f7 49 96 d3	Avalenche effect
1 bit change in ck1	0a 8b 6b d8 d9 b0 8b 08 86 4e 32 d1 81 77 77 fb	d8 e1 c8 f9 e4 ac e0 ab d8 e3 27 77 52 86 17 c7	% 51

TABLE -3: Example of avalanche effect of AES-CTR mode system

$$\text{Avalanche effect} = \frac{\text{number of flipped bits in ciphered text}}{\text{number of bits in ciphered text}}$$

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 12, December-2016

[22]

TABLE -4: Example of avalanche effect of proposed system

Change	Ck1		Ck2	Cipher text	Avalanche effect
	0a 8b 6b d8 d9 b0 8b 08 36 4e 32 d1 81 77 77 fb		58 00 fb 24 af d9 ae c3 37 bd cd ae 33 b8 94 59	a2 ce 31 c5 f3 ca 34 f2 80 84 10 f3 38 26 84 f8	
1 bit change in ck1	0a 8b 6b d8 d9 b0 8b 08 86 4e 32 d1 81 77 77 fb		58 00 fb 24 af d9 ae c3 37 bd cd ae 33 b8 94 59	a6 87 b9 ef d8 a1 fa bd 61 f3 f2 63 d9 e9 05 20	**% 52**
1 bit change in ck2	0a 8b 6b d8 d9 b0 8b 08 36 4e 32 d1 81 77 77 fb		58 00 fb 24 af d9 ae c3 37 bd cd ae 53 b8 94 59	eb b6 f3 ca 64 b2 d5 91 d7 e0 11 de b9 ev 53 d0	**% 52**
1 bit change in ck1& ck2	0a 8b 6b d8 d9 b0 8b 08 86 4e 32 d1 81 77 77 fb		58 00 fb 24 af d9 ae c3 37 bd cd ae 53 b8 94 59	ef ff 95 79 f4 d9 93 03 36 b5 f3 82 c1 b1 d2 a2	**% 67**

X. CONCLUSIONS

This study allows more complex proposed algorithm for the encryption in the security process. Shown in MATLAB how the new algorithm works in comparison with the original algorithm. Demonstrated that, As the algorithm becomes more complex, it does not add significant time to the encryption and decryption processes and increases the avalanche effect of the proposed system which made it more resistance to attacks. The proposed algorithm and the method behind it can be employed in any system that takes advantage of LTE- advanced technology. Future work will be done by performing more tests and comparing the results to those of other proposed solutions, planning to investigate the efficiency of the proposed algorithm , using the quantum cryptography, or using 256 bit cipher key.

REFERENCES

[1] Y. Park and T. Park, “A survey of Security Threats on 4G Networks”, IEEE Globecom Workshop on Security and Privacy in 4G Networks, November 2007, Washington, DC.

[2] Anastasios N. Bikos, Nicolas Sklavos, "LTE/SAE Security Issues on 4G Wireless Networks," IEEE Security & Privacy, vol. 11, no. 2, pp. 55-62,March-April 2013

[3] Apostolis Salkintzis. "Network Architecture", Broadband Wireless Mobile, 10/30/2002

[4] Siwach, Gautam, and Amir Esmailpour. "LTE Security potential vulnerability and algorithm enhancements", 2014 IEEE 27th Canadian Conference on Electrical and Computer Engineering (CCECE), 2014.

[5] Masoumeh Purkhiabani and Ahmad Salahi “Enhanced Authentication and Key Agreement Procedure of next Generation 3GPP Mobile Networks” , January 2012

[6] Forsberg, . "EPS Authentication and Key Agreement", LTE Security Horn/LTE Security, 2012.

[7] P. Lescuyer, T Lucidarme, “Evolved Packet System (EPS) - The LTE and SAE Evolution of 3G UMTS”, John Wiley & Sons, Ltd, 2008.

[8] FIPS Publication 197, “Advanced Encryption Standard (AES)”, U.S. DoC/NIST, November 26, 2001.

[9] Kaul, Vikas, Prerana Choudhari, and S K Narayankhedkar. "Security enhancement for data transmission in 4G networks", 2014 5th International Conference - Confluence The Next Generation Information Technology Summit (Confluence), 2014.

[10] Hisham A. Kholidy. "A New Accelerated RC4 Scheme Using Ultra Gridsec and HIMAN and use this Scheme to Secure HIMAN Data", 2009 Fifth International Conference on Information Assurance and Security, 08/2009

[11] Stošic, Lazar, and Milena Bogdanovic. "RC4 stream cipher and possible attacks on WEP", International Journal of Advanced Computer Science and Applications, 2012.

[12] Allam Mousa and Ahmad Hamad ,“Evaluation of the RC4 Algorithm for Data Encryption”, International Journal of Computer Science and Applications, Vol 3,No. 2, June 2006

[13] Dan Forsberg, Gunther horn, Wolf-Dietrich Moeller, Valtteri Niemi, “LTE Security”, 2nd ed., John Wiley and Sons Ltd, 2013.

[14] Pradeep J. Sonawane, Umesh S. Bhadade. "Synthesis and Simulation of FPGA Based Hardware Design of RC4 Stream Cipher", 2015 International Conference on Computational Intelligence and Communication Networks (CICN), 2015

[15] Subhadeep Banik, Takanori Isobe" Cryptanalysis of the Full Spritz Stream, Cipher" Fast Software Encryption, pp.63-77, · March 2016

[16] https://www.researchgate.net/figure/275716296_fig1_Figure-1-Encryption-and-decryption-by-RC4 [accessed Aug 22, 2016]

[17] Ghizlane ORHANOU, Said EL HAJJI, Youssef BENTALEB and Jalal LAASSIRI, “EPS Confidentiality and Integrity mechanisms Algorithmic Approach”, IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 4, No 4, July 2010

[18] LTE Security: Encryption Algorithm Enhancements ,Mayur Solanki, Seyedmohammad Salehi,and Amir Esmailpour,2013

[19] Niemi. "UMTS Security Features in Release 1999", Universal Mobile Telecommunications System Security, 11/11/2003

[20] Dr Houman Zarrinkoub, “Understanding LTE with matlab from mathematical modeling to simulation and prototyping”, John Wiley and Sons Ltd, 2014

[21] Basavarasu, Srinivasa Rao, "Voice and image encryption, and performance analysis of counter mode advanced encryption standard forWiMAX" (2013).

[22] Akash Kumar Mandal1, Mrs. Archana Tiwari2, “Analysis of Avalanche Effect in Plaintext of DES using Binary Codes”, IJETTCS International Journal of Emerging Trends and Technology in Computer Science Issues, Vol. 1, Issue 3, pp.166-171, october 2010

[23] Jorg J. Bucholz, “MATLAB Implementation of the Advanced Encryption Standard”, December, 2001. http://buchholz.hs-bremen.de

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 12, December-2016

BIOGRAPHIES

Nihal Fayez Areed assist prof. at communication and electronics dept. received the PhD degree of communication engineering . Her current research interests are in Electromagnetic fields Antennas and wavepropagation Photonic Bandgap devices Fiber optics

Ali Taki El-Deen (IEEE senior member) received the PhD degree in Electronics and Communications Engineering in "Encryption and Data Security in Digital Communication Systems".

Eman Ashraf Mohammed received BSc in Electronics and Communications, Master student.