IMAGE ENCRYPTION USING THE 4TH GENERATION ZUC ALGORITHM [+]

Raya Majid Alsharfa [*]

Abstract:

In this research, its aim to increase the security level of the mobile systems for the Fourth Generation (4thG), and to study security of images to enhance the information security for users.Long Term Evolution is one of the mobile systems that used inFourth Generation (4thG) cellular networks. Long Term Evolution(LTE) is a modern and newest technology that is emerged to improve the security and service of communication. This work is an attempt to study the LTE security and dealing it with stream cipher algorithm which is called ZUC algorithm . Also, we applied the ZUC algorithm to encrypted image.

MATLAB software ver. 2013a is used in this work for the proposed image algorithm.

Keyword: ZUC algorithm , LTE , 4thG

تشفير الصور باستخدام خوارزمية الل (ZUC) للجيل الرابع

ريا ماجد حميد

المستخلص:

في هذا البحث ، الهدف منه هو زيادة مستوى الحماية في انظمة الموبايل للجيل الرابع (4G) ، ودراسة حماية الصور او زيادة امنية المعلومات للمستخدمين .

LTE (التطوير للمدى البعيد) وهي تقنية حديثة وجديدة ظهرت لتحسين مستوى الامن وخدمة الاتصالات . هذا العمل هو محاولة لدراسة امنية ال(LTE) وتعاملها مع خوارزمية ال (ZUC) ، وايضا طبقنا خوارزمية ال(ZUC) لتشفير المعلومات او بالأحرى تشفير الصور .

البرنامج المستخدم هو Matlab اصدار 2013a ، استخدم في هذا العمل للصور المقترحة للخوارزمية .

Introduction :

Due to extremely high demand of mobile phones among people, many Internet users use smart phones not only as a means of communication, but also as a way to organize work and monitor the progress of work and special services, that means all smart phones and computers are used to transfer important information, and especially, such as Messages (SMS), (MMS),... etc., therefore they must provide various applications and security services for protecting information and the communication [1].

[+] **Received on 8/9/2016, Accepted on 25/7/2017 .**

[*] **Assist. Lec. / Middle Technical University**

Long Term Evolution is one of the mobile systems that used inFourth Generation (4^{th}G) cellular networks. Also,it has many features that make them compete with other technologies in network of mobile, LTE providesusers with many applications with high experience, these applications are such as video generator programs,games,interactive TV andprofessional services,... etc [1].

The LTE ischaracterized in that it offers high security level of the 4^{th}G when compared to previous generations. In this work is an attempt to study the LTE security and dealing it with stream cipher algorithm which is called ZUC algorithm.

ZUC Stream Cipher Algorithm :

Protection and hiding of valuable information has a very old history [1]. The stream cipher ZUC is a word-oriented stream cipher, ZUC stream cipher is the heart of encryption and decryption algorithms used in cryptography. The structure ofZUC stream cipher is shown in Figure(1), and it consists of three layers Linear Feedback Shift Register(LFSR), BitReorganization layer(BR), Non-linear function(F) [3,4].

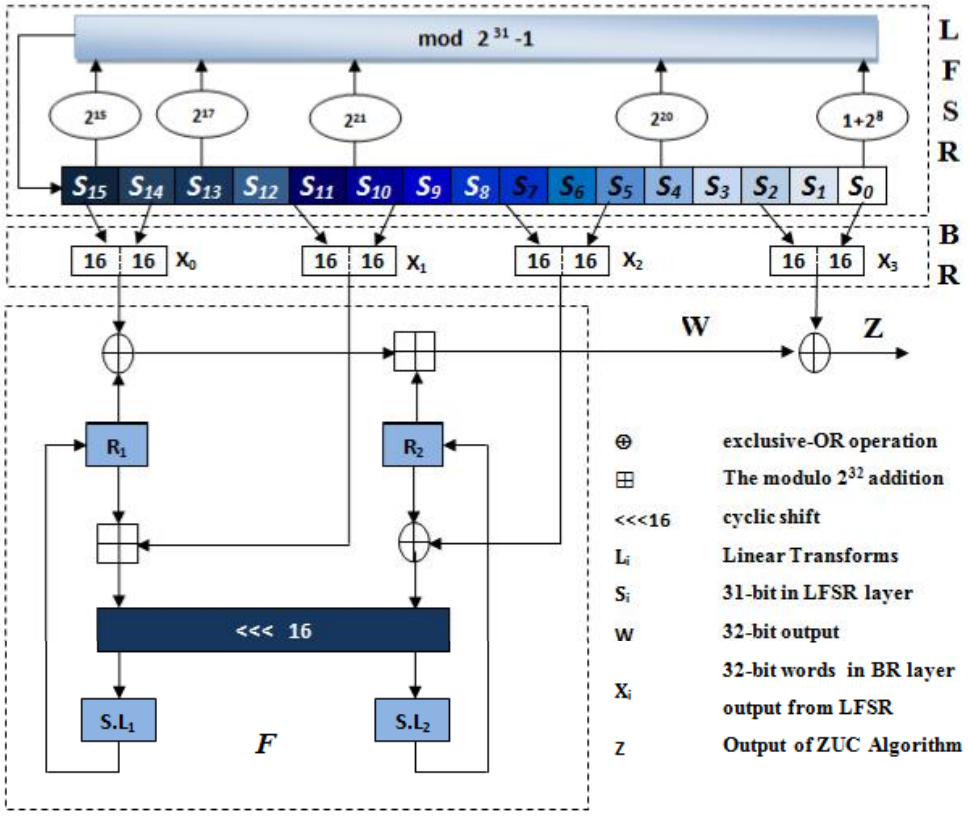

Figure (1) : The General Structure of ZUC [4]

Test Implementation for Ciphering Image Using the ZUC Algorithm :

Digital color image encryption is different from text encryption because of some inherent features of image such as huge data capacity and high correlation among the neighboring pixels [5]. That meansthat the ZUC and the proposed algorithmsare not effective

well with images. Hence, the algorithms should be combined with another image cipher algorithm to get a high security level.In this section, we apply the ZUC algorithm with image.

The encryption of images may be achieved by five steps as follow (see Figure (2)):

1- Inserting a certain image into program.
2- Dividing the image into three parts (Red image, Green image and Blue image).
3- Encryption of the three images which are obtained from step (2) by ZUC algorithm.
4- Mixing the three encrypted images which are obtained from step (3) to get colored image similar to origin image but it's encrypted.
5- Comparing the encrypted images which are obtained by ZUC with original image.

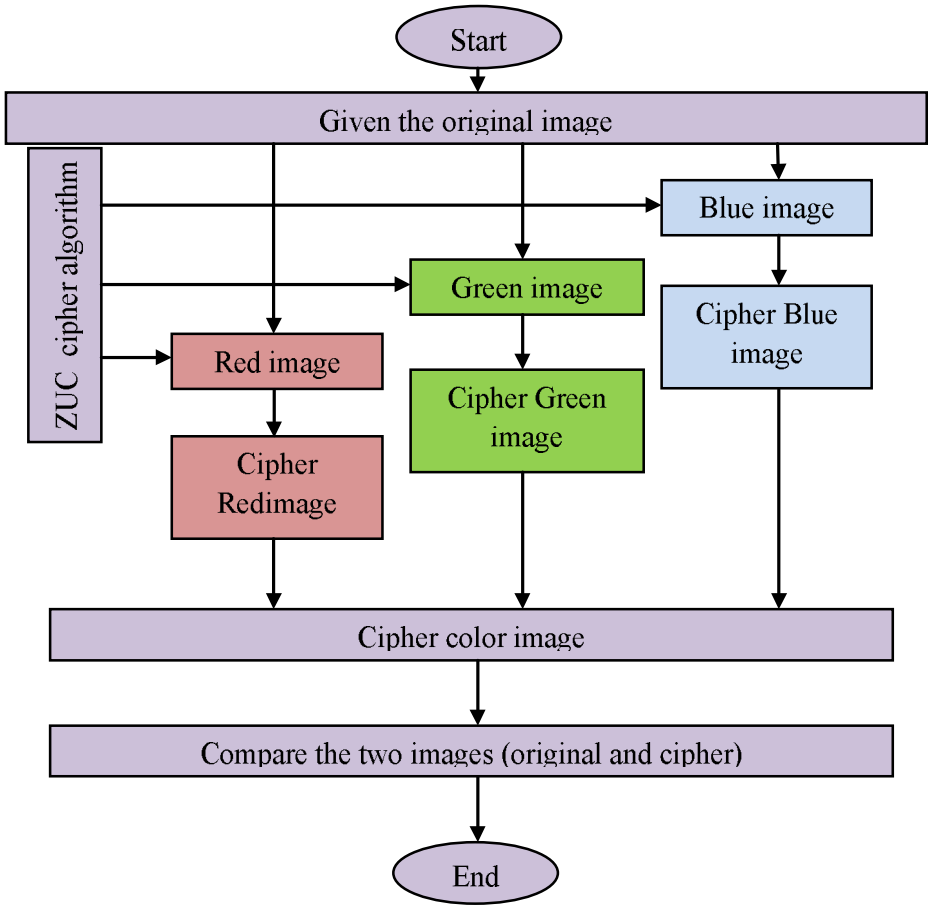

Figure (2) : The Flowchart of Image Ciphering

This part presents the original image (which is sketched by a drawing software) and splits the image to (Red, Green and Blue) image andencrypts each of the three images using the ZUC algorithm as shown in Figure (3).

Figure (3) :The Original Image Before Ciphering

In Figure (4), the Red image and Red image after encrypted can be seen.

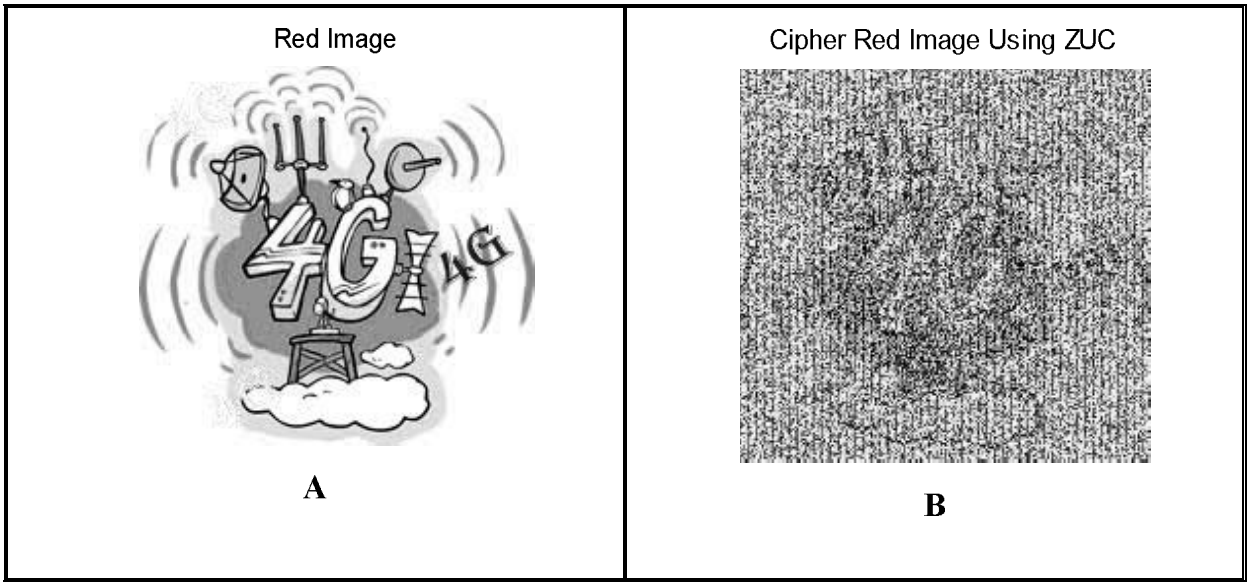

Figure (4) : A: Red Image **B: Ciphering the Red Image using ZUC**

In the Figure (5), the Green image and Green image after encrypted can be seen. Also, in Figure (6), the Blue image and Blue image after encrypted can be seen.

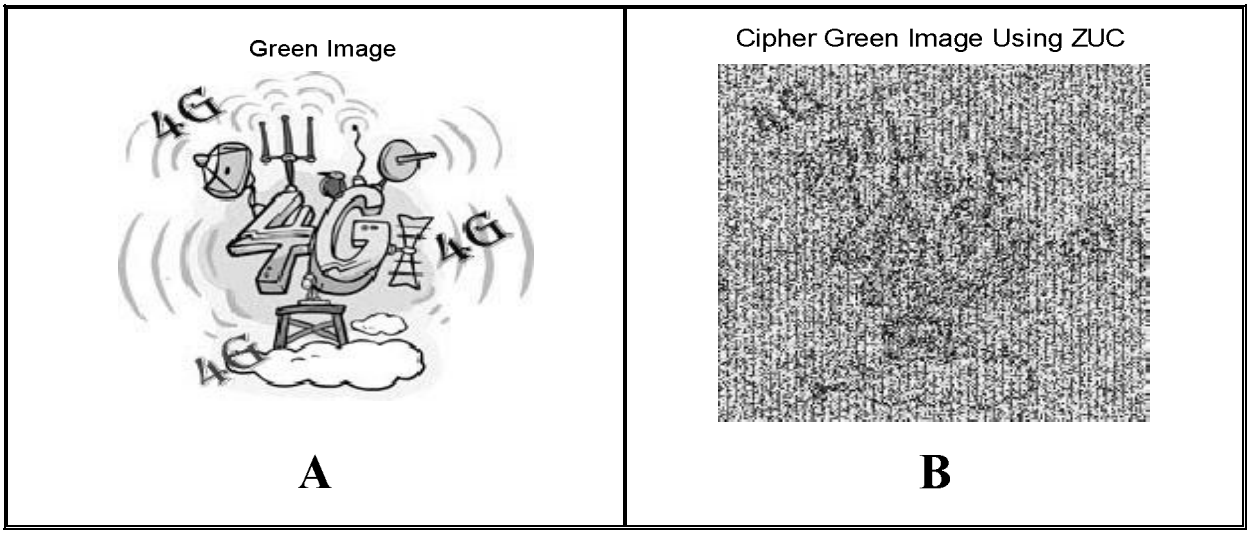

Figure (5) : A: Green Image **B: Ciphering the Green Image using ZUC**

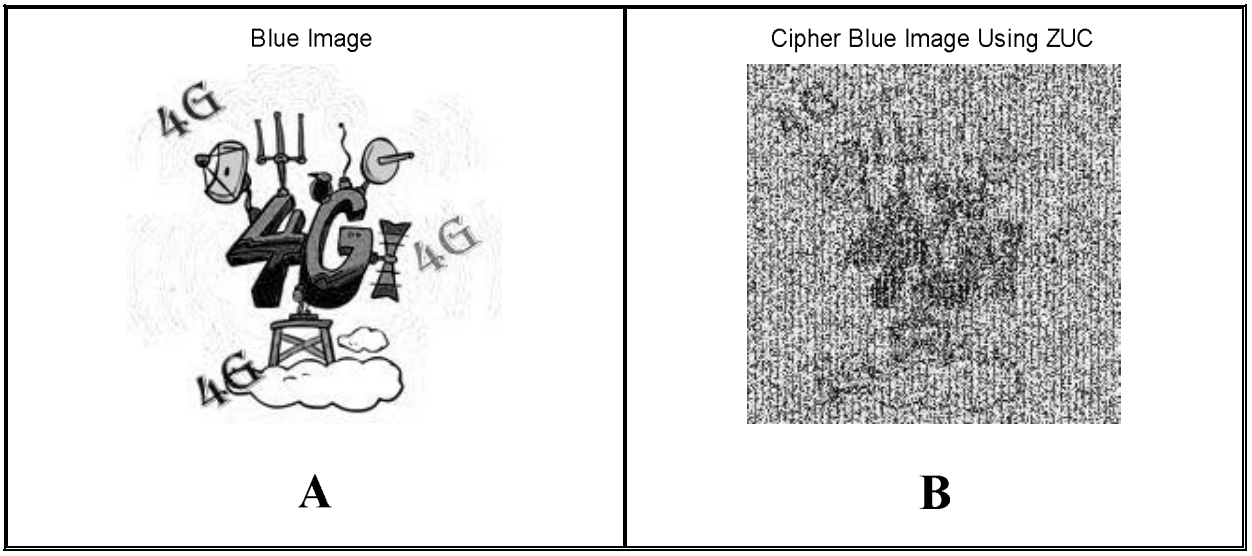

Figure (6) : A: Blue Image **B: Ciphering the Blue Image using ZUC**

After using the ZUC algorithm to encrypted (Red, Green and Blue) images, the disappearance of image features can be noted, it is not a high level of security but a good level to hide features images.

The Figure (7)shows the final output the colored images after encrypted, and also the shape that contains the original image before encryption to enable us to compare them.

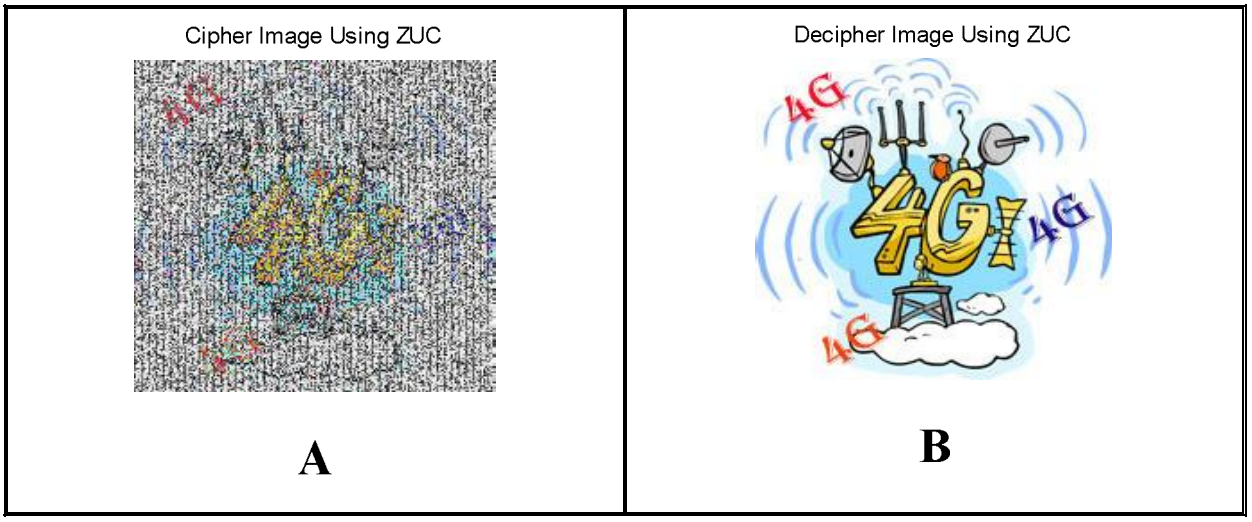

Figure (7) : A: Cipher Image Using ZUC Algorithm
B: Decipher Image Using ZUC Algorithm

Conclusion :

In the entire process of the previous test using MATLAB software (Matlab code), a code is added to the main program to deal with all sizes of images if the encrypted images use ZUC algorithms even if the ZUC algorithms are not used to encrypt images, but has been applied as part of its work.

Reference:

1- SomnathS.Berad," *Hardware Implementation of ZUC Stream Cipher*", International Journal of Innovative Research in Science, Engineering and Technology , Volume 3, Special Issue 4, April 2014.

2- GhizlanceOrhanou, "The New LTE Cryptographic Algorithms EEA3 and EIA3", IJAMIS, No. 6, 2013.

3- A.VijayaBhaskar and C.RavishankarHanuman,*"ZUC Stream Cipher Using Feedback Carry Shift Register"*, International Journal of Engineering Science and Technology, Vol. 4, No.06, ISSN : 0975-5462, June 2012.

4- N.Seddigh, B. Nandy, R. Makkar and J.F. Beaumont, *" Security Advances and Challenges in 4G Wireless Networks"*, 8th Annual International Conference on Privacy, Security and Trust ,IEEE,2010.

5- Hai Cheng, Chunguang Huang, Qun Ding and Shu-Chuan Chu, *"An Efficient Image Encryption Scheme Based on ZUC Stream Cipher and Chaotic Logistic Map"*, Conference on Intelligent Data analysis and its Applications, Springer, Volume 2, 2014.