Modified AES Algorithm Based on a New Chaotic System

Asst. Prof. Dr. Sadiq A. Mehdi[1] Donia Fadil Chalob/ M.Sc Student[2]

[1,2]dept. of Computer Science/ College of Education/ University of Al-Mustansiriyah.

sadiqmehdi71@yahoo.com donia_fadil@yahoo.com

Abstract:

The vast using of digital images in various areas such as military, commerce and others requires that the security of images transmitted over communication networks and the internet must be well-preserved. One of the most secure algorithms is Advanced Encryption Standard (AES) algorithm. However, this algorithm has a number of drawbacks, such as pattern appearance problem and very slow when used directly for encrypting images. This paper proposes a new modified of AES using a new chaotic system with three-dimension (3D) to make it suitable for images encryption. The chaotic sequence generated from the new chaotic system has been used as key in modified AES to overcome the problem overcome the problem of the key is unchanged in the entire encryption process in original AES and MixColumns operation is removed, since it consumes very long time in comparison to other operations, resulting in a great reduction in encryption and decryption time and improve the security level of AES algorithm as observed in the experimental results.

Keyword: AES algorithm, chaos, 3D chaotic system, image encryption, chaotic key.

خوارزمية AES المعدلة بالاعتماد على نظام فوضوي جديد

أ.م.د. صادق عبد العزيز مهدي[1] دنيا فاضل جلوب[2]
[1,2]قسم علوم الحاسبات/ كلية التربية/ الجامعة المستنصرية
donia_fadil@yahoo.com sadiqmehdi71@yahoo.com

المستخلص

الاستخدام الهائل للصور الرقمية في مجالات مختلفة مثل المجالات العسكرية والتجارية وغيرها، يتطلب الحفاظ جيدا على أمن الصور المرسلة عبر شبكات الاتصال والإنترنت. تعتبر خوارزمية التشفير القياسي المتقدم (AES) من أشهر خوارزميات التشفير و أكثرها امناً. مع ذلك، فأن هذه الخوارزمية لها عدة مساوىء مثل مشكلة ظهور الانماط وتستغرق الكثير من الوقت عند استخدامها مباشرة لتشفير الصور. هذا البحث يقترح تعديل جديد لخوارزمية AES بأستخدام نظام فوضوي جديد ثلاثي الابعاد لكي تكون مناسبة لتشفير الصور. تم استخدام السلسلة الفوضوية الناتجة عن النظام الفوضوي الجديد كمفتاح في خوارزمية AES المعدلة للتغلب على مشكلة ان المفتاح لا يتغير في عملية التشفير بأكملها في خوارزمية AES الأصلية وتم ازالة عملية MixColumns لأنها تستهلك وقتا طويلا جدا بالمقارنة مع العمليات الأخرى مما أدى إلى انخفاض كبير في وقت التشفير وحل التشفير وتحسين مستوى الأمنية لخوارزمية AES الأصلية كما ملاحظ في النتائج التجريبية.

الكلمات المفتاحية: خوارزمية AES، فوضوية، نظام فوضوي ثلاثي الابعاد، تشفير صورة، مفتاح فوضوي.

1- Introduction

With the continuing development of the internet and computer techniques, numerous data is transferred via the internet like images. Therefore, the security of data has turned out to be very essential. The typical method of protection is encryption techniques, which convert the data from the plain form to an unintelligible form to be protected from unauthorized access [1]. Numerous data encryption algorithms have been suggested, as example Advanced Encryption Standard (AES) and Data Encryption Standard (DES) algorithms. The small key length of DES makes it more vulnerable to various attacks. Besides security issue, DES is a low efficiency encryption algorithm because of its slowness. AES

algorithm is the winner of encryption competition standard held by the National Institute of Standard and Technology (NIST) as an alternative of DES [2]. However, there are a number of drawbacks in AES, such as high computation, pattern appearance issue and so slow when used directly for encrypting images because of intrinsic features of images which are large volumes, high redundance and high correlations among image pixels. Consequently, there is a need to propose new encryption algorithms [3]. Chaos has been presented to cryptography thanks to its randomness, sensitivity to initial conditions and parameters, mixing property and ergodicity that are close to diffusion and confusion in cryptography. These features make chaos an excellent choice for building cryptographic systems and approved chaotic systems to be promising alternate for the conventional cryptographic algorithms [4]. Several attempts have been made in literature toward AES algorithm enhancement based on chaos. **Ali Abdulgader et al.** [5] introduced an approach that overcomes the fixed S-box disadvantage and enhances the performance of AES to be suitable for image encryption, especially if the image is large. Besides, the MixColumns transformation is swapped by using chaos map and XOR operation in order to reduce the high computation in MixColumns transformation. The proposed method offers low correlation coefficient and providing better enciphering speed and acceptable security. **Yufen Feng et al.** [6] presented an improved AES algorithm based on 2D Henon and Chebyshev chaotic map which can randomly generate an independent round key. Two sets of chaotic key stream are generated from each of Henon map and Chebyshev map, the four groups of key stream generated from Henon and Chebyshev map perform XOR operation, respectively, to generate two intermediate keys, then generate a target key via XOR operation of the intermediate keys and this is the AES key. This proposed algorithm overcomes the weak point of the initial key is unchanged in the whole encryption process when using the original AES algorithm.

2- Advanced Encryption Standard (AES)

AES is a symmetric block cipher capable of encrypting and decrypting data in blocks of 128-bits using a flexible key length of 128-bits, 192-bits or 256-bits respectively, which referred as AES-128, AES-192 or AES-256 according to the key length. AES operations are achieved on an array of 4*4 bytes known as the State that modified at every stage of encryption or decryption operation. In the same way, the key is represented in a square array of bytes, where the key is extended into a matrix of key scheduled words. Every word is four bytes, so the whole key schedule is 44 words when using 128-bits key. AES involves a number of rounds N,

where the number of rounds relies on the key size, 10 rounds for a 16-bytes key, 12 rounds for a 24-bytes key and 14 rounds for a 32-bytes key. The first N-1 rounds contain four transformations which are SubBytes, ShiftRows, MixColumns and AddRoundKey that would be described consequently. The final round encloses just three transformations. An initial transformation which is AddRoundKey exists before the first round that could be considered as Round 0. In the decryption process, the three operations SubBytes, ShiftRows and MixColumns in the encryption process are reversed in the decryption operation. The inverse of AddRoundKey stage is done via XORing the exact round key to the block. [7]

2-1 SubBytes/ Inverse SubBytes Transformation

In this operation, all the bytes in the State are substituted with another different bytes via an 8-bits table called the S-box. The SubBytes operation is the nonlinear step in AES algorithm and hence provides the confusion requirement in the encryption process. In the decryption process, Inverse S-box table instead of S-box is used for implementing Inverse Sub-Byte operation. [8]

2-2 ShiftRows/ Inverse ShiftRows Transformation

The bytes of every row in the State are circular shifted to the left by different amount of offset. The 1st row in the State is unchanged, the 2nd row is shifted by one-byte, the 3rd row is shifted by two-bytes and finally the 4th row is shifted by three-bytes. In the decryption, Inverse ShiftRows transformation performs the circular shift to the right for each of the last three rows by a one byte rotating to the right for the 2nd row and so on. [7]

2-3 MixColumns/ Inverse MixColumns Transformation

The MixColumns transformation treats every column as a four-term polynomial, where the columns are considered as polynomials over Galois field GF (2^8), every column which consists of four bytes is multiplied by a special 4*4 array defined as below:

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$$

The multiplication performed on this array isn't a normal multiplication. Rather, the multiplication is performed over GF. The ShiftRows and MixColumns transformations together provide diffusion in AES. Inverse MixColumns is achieved via multiplication over GF by another known matrix defined as below [9]:

$$\begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix}$$

2-4 AddRoundKey/ Inverse AddRoundKey Transformation

Every byte of the State array is added to a corresponding byte in the round key. This addition is merely an XOR operation accomplished bitwise between the key and the State. The State is added with the sub key corresponding to the current round which had been already produced via key expansion and make another State. The inverse of the round key operation is exactly the same operation. [7]

2-5 AES Key Expansion

The key expansion operation generates a number of sub-keys from the initial key for every round to be used in the AddRoundKey transformation. For AES-128, 44words will be generated, where each word equal four bytes. When the words are indexed from 0 to 43.The first four words (W0, W1,W2,W3) are filled with the given cipher key and columns in locations that are a multiple of 4 (W4, W8, W12… W40) will be generated by three operations which are: [7]

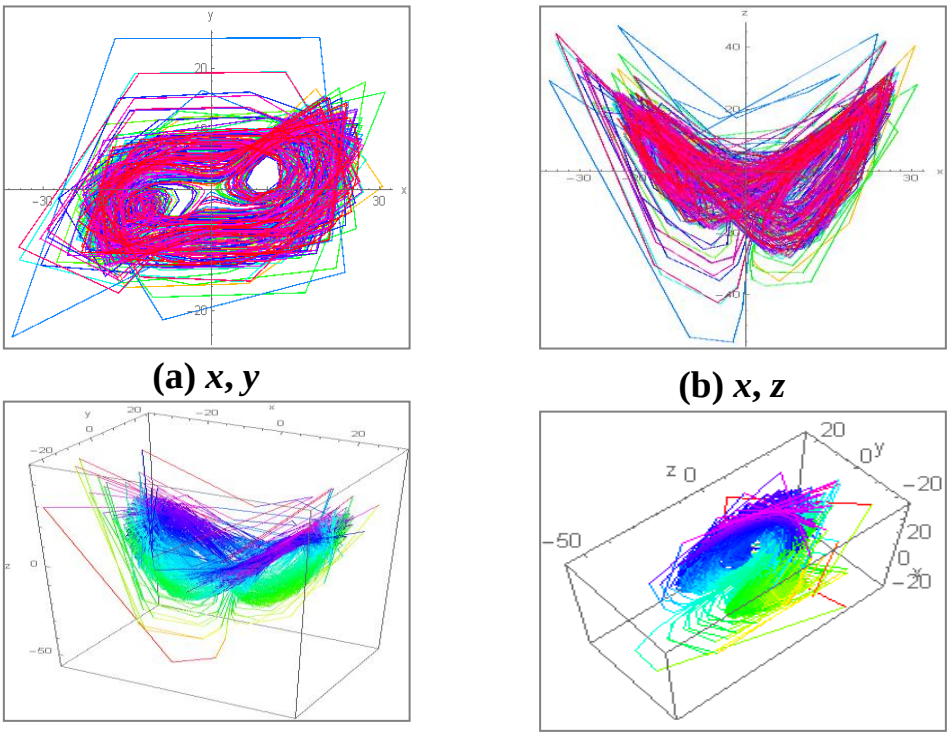
- RotWord: RotWord performs one rotating permutation to the left on a word.
- SubWord: SubWord substitutes individual bytes of a word using the S-box.
- XOR the result from RotWord and SubWord operations with word Wi-4 and with a defined constant from Rcon matrix.

3- Construction of a New 3D Chaotic System

A chaotic system is a special dynamical nonlinear system, 3D chaotic system has more complex dynamic properties than lower dimensional chaotic systems. Lyapunov Exponent is a numerical indicator to judge if the system is chaotic. A positive Lyapunov Exponent means chaos and positive Lyapunov Exponents more than one means hyper chaotic [10]. In this paper, a new chaotic system is constructed, which obtained by the following three first order differential equations:

$$\begin{aligned} \frac{dx}{dt} &= ay - bx \\ \frac{dy}{dt} &= -cxz \qquad \ldots (1) \\ \frac{dz}{dt} &= -d + exy + fsin(y) \end{aligned}$$

In which (*x, y, z and t)* ∈ R and called the system states, where *a, b, c, d, e* and *f* are positive constant parameters. When the values of *a*= 9, *b*=2, *c*= 0.2, *d*= 42, *e*= 1.1, *f*= 33 and the initial conditions are *x*(0) = -0.07, *y*(0) = 5 and *z*(0) = 0, the system shows a chaotic behavior and the Lyapunov Exponents are obtained as: LE_1 = 1.27325, LE_2 = 0.01566 and LE_3 = −3.28925. The chaotic attractors are shown in Figure (1).



(a) *x, y* **(b) *x, z***

(c) *x, y, z* **(d) *x, z, y***

Fig. (1): Phase portrait of the new chaotic system
(a), (b) two-dimension view. (c), (d) three-dimension view.

4- Proposed Algorithm

In this proposed algorithm, a plain image is passed to the transformations that already exist in the original AES, which are SubBytes, ShiftRows and AddRoundKey, there are two AddRoundKey in this proposed algorithm named as First AddRoundkey and Second AddRoundkey. First AddRoundkey is applied using the chaotic sequences generated from the chaotic system (1) and Second AddRoundkey is applied using a normal cipher key. In First AddRoundkey, each block of the plain image is encrypted with completely different chaotic key while in Second AddRoundkey the initial normal key is unchanged in the entire encryption process as in the original AES. The MixColumns transformation is removed because it consumes very long time in comparison to the other

operations. Chaotic masks will be generated from chaotic sequences of chaotic system (1), where each mask will be divided into blocks of size 4*4 bytes to be used as changing key in modified AES. The decryption process applies operations of the encryption process in reverse order. Figures (2) and (3) demonstrate the encryption and decryption process of proposed algorithm.

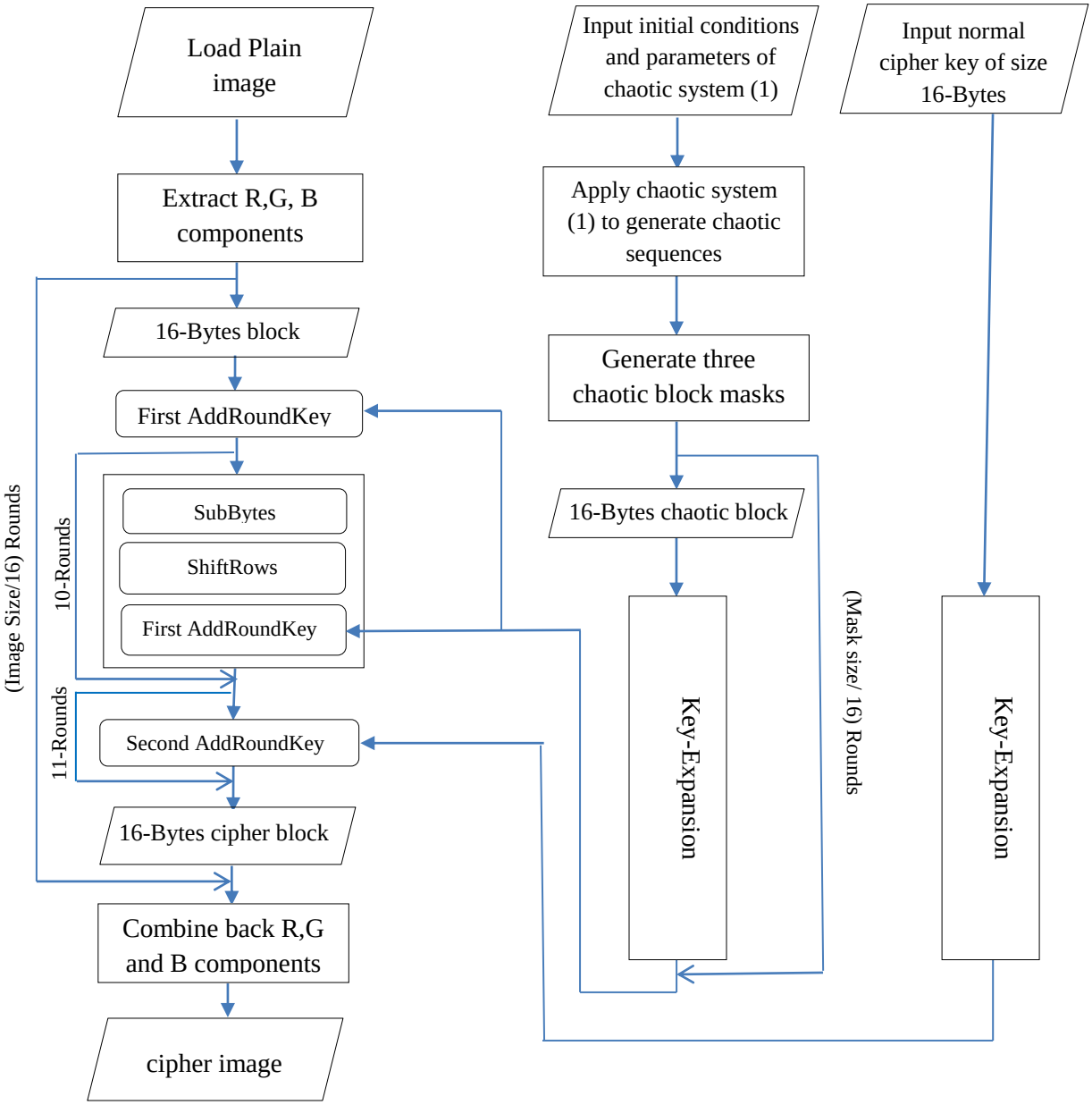


Fig. (2): Encryption process of proposed algorithm.

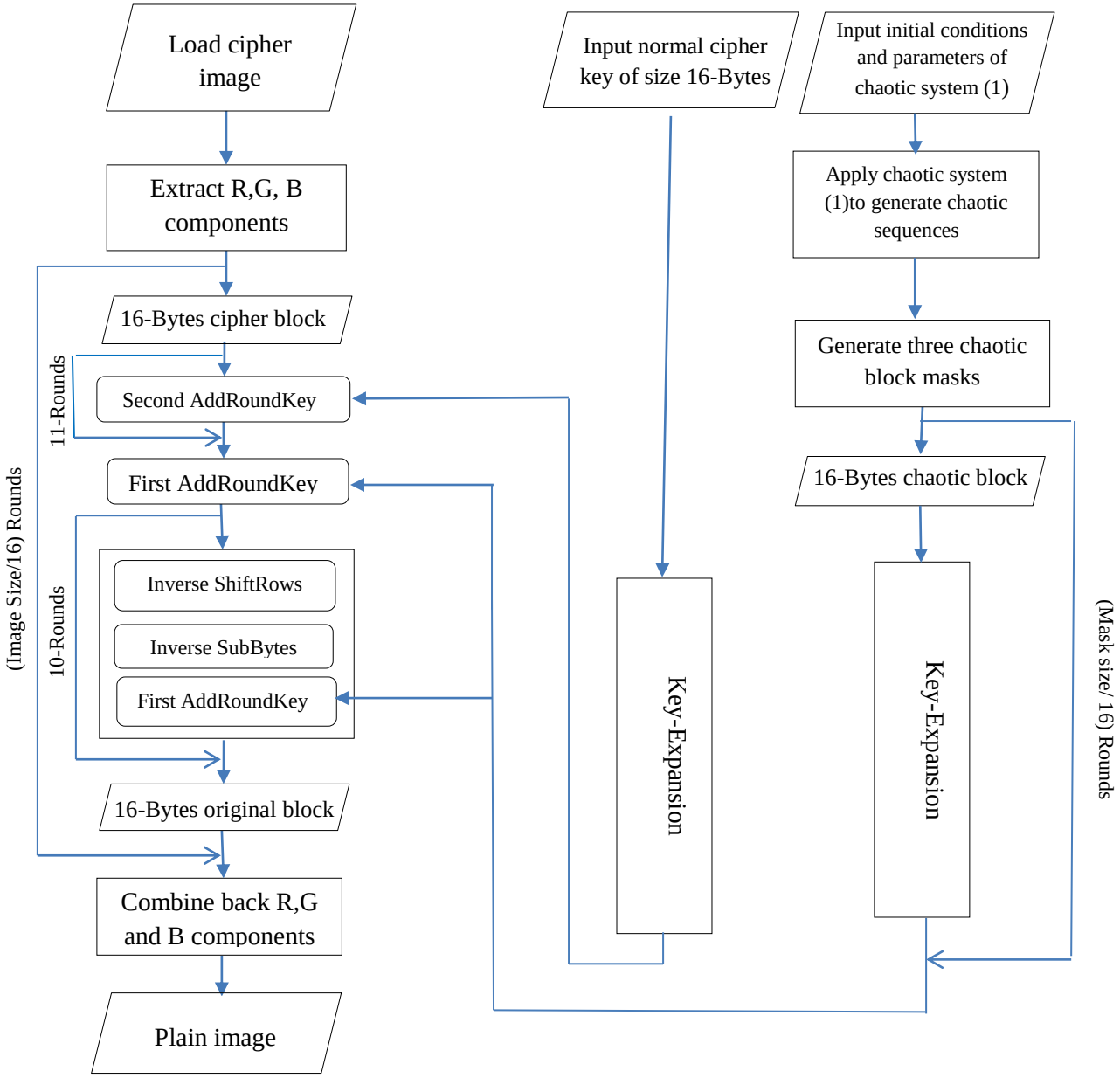


Fig. (3): Decryption process of proposed algorithm.

5- Experiment Results

A series of experiments are performed using the proposed algorithm in order to encrypt two color images of JPEG format and size of (256*256) bytes. These images are shown in Figure (4) with their color components. Also, a comparison is made between the experiment results of proposed algorithm and original AES. The experiments are implemented by using

MATLAB R2013a programming language and using a computer with Intel(R) Core (TM) i7-5500U CPU @ (2.40) GHz, 8 GB memory and windows 7 operating system.

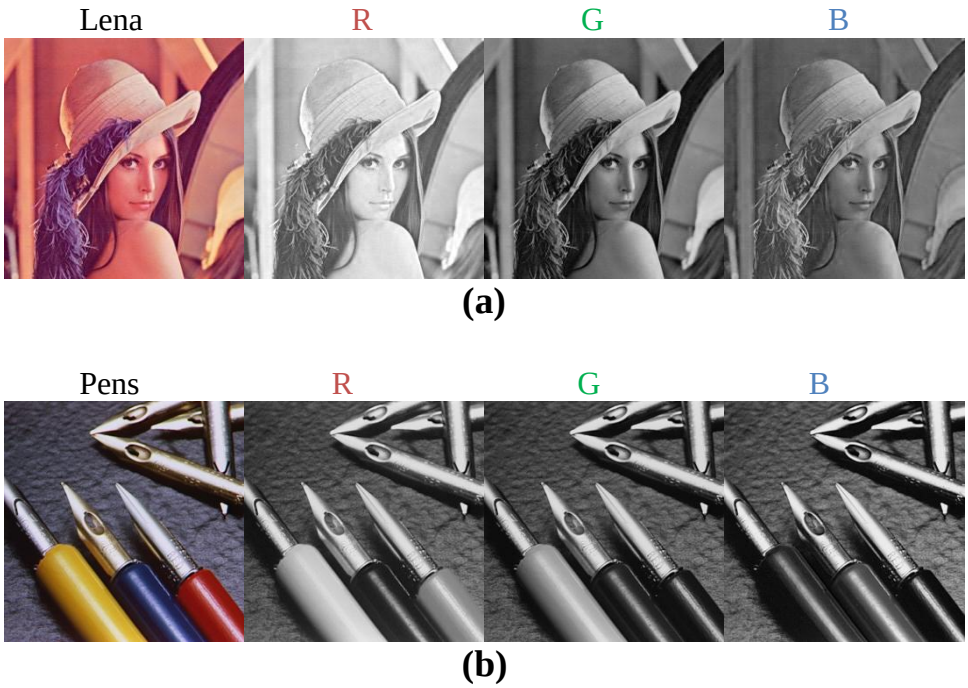


Fig. (4): (a) Lena image with its RGB components (b) Pens image with its RGB components.

5-1 Key Space Analysis

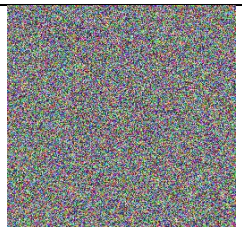
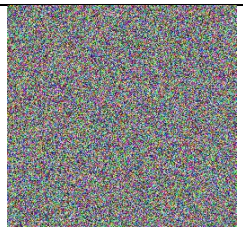
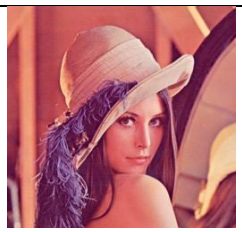
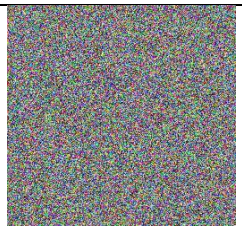
The key size should be larger than 2^{100} in order to prevent brute force attack, which is a process of break a cryptosystem via exhaustively seeking all probable keys [11]. The key size of the proposed algorithm is calculated from the parameters and initial conditions of chaotic system (1), where if the precision of each is 10^{-14} then the key size would be 10^{126} which is approximately equal to 2^{398}, in addition to the key size of original AES. Thus, the brute force attack is impractical on the proposed algorithm.

5-2 Key Sensitivity Analysis

A secure encryption algorithm has a sensitivity toward the encryption keys in both encryption and decryption operations. When encrypting an image, a small change of keys obtains two different encrypted images and when decrypting an image, if an incorrect key is used, different image is obtained [12]. The test of key sensitivity for the proposed algorithm is applied on each of the two test images, where the value of initial condition y(0) of chaotic system (1) is slightly changed

from y(0) = 5 into y(0) = 5.00000000000001 and Table (1) illustrates that the decrypted image by using a tiny changed key is completely different from the original image even with a tenuous difference of 10^{-14}, which means that the proposed algorithm has high sensitive when any change may occur in the key.

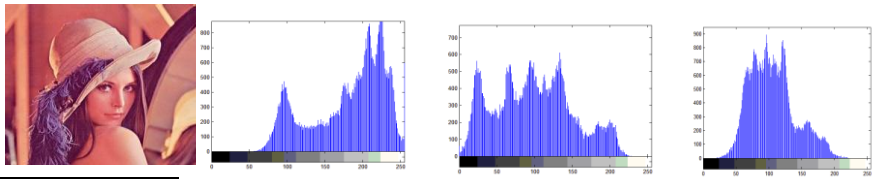
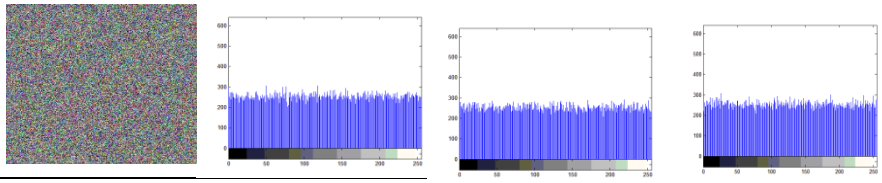
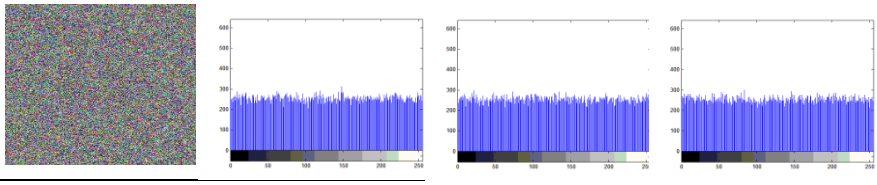
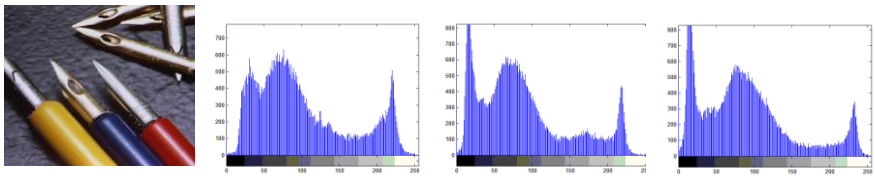
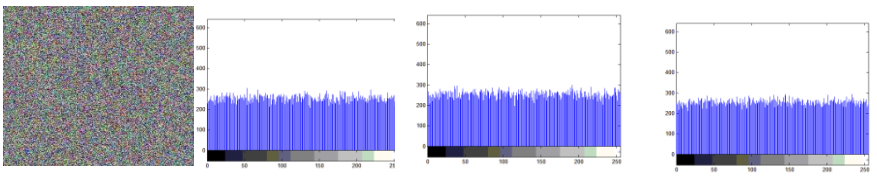
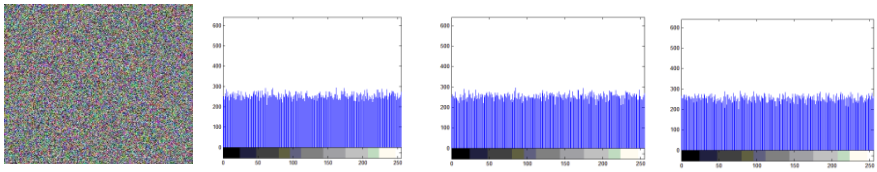
Table (1) Key sensitivity result

Original image		
Encrypted image with $y(0)= 5$		
Decrypted image using correct key, $y(0) = 5$		
Decrypted image using incorrect key, $y(0) =$ 5.00000000000001		

5-3 Histogram Analysis

A histogram of an image demonstrates the distribution of image pixels by graphing the number of pixels at every color intensity component. The histogram of the cipher image must be fairly uniform and different from the corresponding histogram of the plain image and therefore doesn't give any clue for employing any statistical analysis on the encrypted image [12]. Table (2) obviously illustrates that the histogram of the encrypted image via using the original AES and proposed algorithm is nearly the same and has uniform distribution and different from the histogram of the original image.

Table (2) Histogram analysis results

Image	Histogram		
	R	G	B
Original			
Encrypted using original AES			
Encrypted using proposed algorithm			
Original			
Encrypted using original AES			
Encrypted using proposed algorithm			

5-4 Correlation Coefficients Analysis

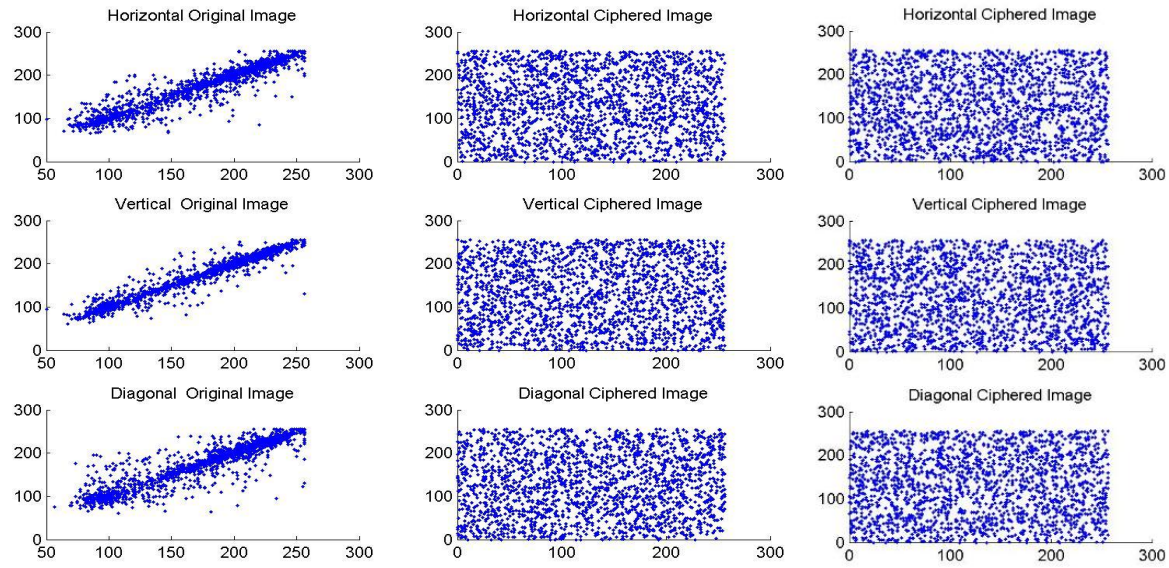
Correlation coefficient is a statistical computation in a range between −1and+1, which measures the robustness of the association between two variables of data. The Correlation coefficient measurement is known by the equation below:

$$r = \frac{\sum_m \sum_n (A_{mn} - \overline{A})(B_{mn} - \overline{B})}{\sqrt{(\sum_m \sum_n (A_{mn} - \overline{A})^2)(\sum_m \sum_n (B_{mn} - \bar{B})^2)}} \quad \dots (2)$$

In which A and B are matrices of similar size, where ($\bar{A} = mean(A)$, $\bar{B} = mean(B)$) and mn represent the total number of samples. A zero correlation indicates complete independence and -1 or 1 represents complete dependence. A strong encryption system should have a correlation coefficient near to zero [13]. Table (3) presents the correlation coefficients of the encrypted images which encrypted via using original AES and the proposed algorithm in horizontal, vertical and diagonal direction. From the observation of Table (3), correlation coefficients of the encrypted image of Lena using the proposed algorithm is more close to zero than the original AES in two directions and encrypted image of Pens using the proposed algorithm is more close to zero than the original AES in one direction. Figures (5) and (6) show the correlation coefficients of pixels distribution horizontally, vertically and diagonally for original and ciphered images using original AES and proposed algorithm.

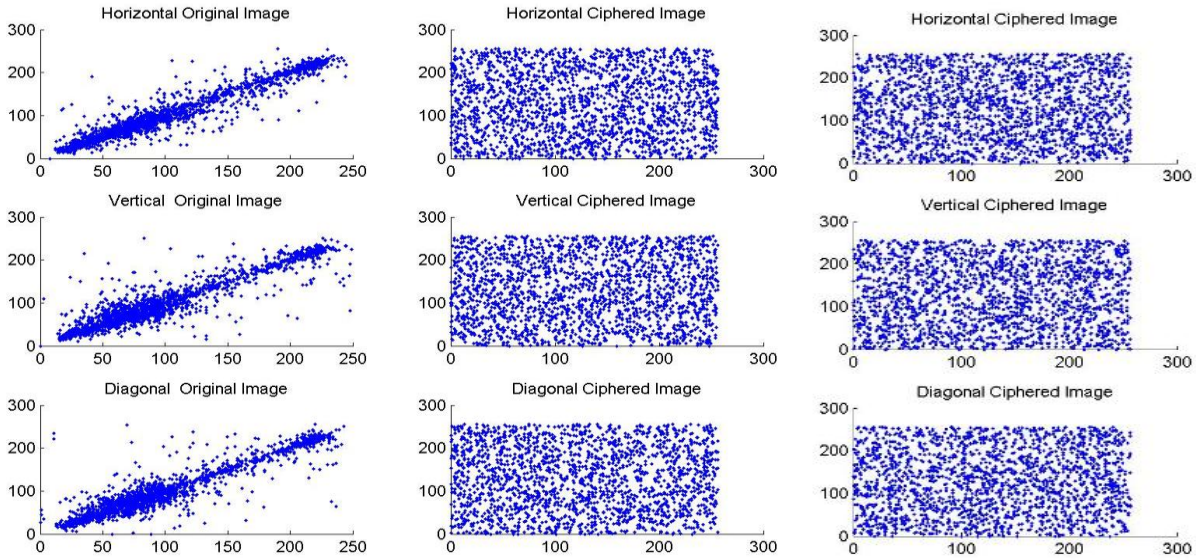
Table (3) Correlation coefficients of encrypted images.

Image	Original AES			Proposed algorithm		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Lena	-0.0013	0.0027	0.0087	3.6402e-05	0.0049	-0.0015
Pens	-0.0066	0.0027	-0.0020	0.0033	-0.0037	-0.0050



(a) (b) (c)

Figure (5): Correlation coefficients of Lena image in horizontal, vertical and diagonal direction: (a) Original image. (b) Cipher image using original AES. (c) Cipher image using proposed algorithm.



(a) (b) (c)

Figure (6): Correlation coefficients of Pens image in horizontal, vertical and diagonal direction: (a) Original image. (b) Cipher image using original AES. (c) Cipher image using proposed algorithm.

5-5 Entropy Analysis

Entropy of a source provides an idea of self-information, i.e., information obtained via a random process about itself, where the information entropy is the most outstanding characteristic of randomness. Let $P(x)$ stands for the information source, the formula for computing information entropy is:

$$Entropy \quad = -\sum_{i=0}^{n-1} p(x_i) \times \log_2 p(x_i) \quad \dots (3)$$

Where $P(\ x_i\ )$ indicates the probability of symbol x_i occurrence and log denotes the base 2 logarithm, thus the entropy is represented in bits. The theoretical entropy of an encrypted image should be 8 contrary to its original form, which means the cryptographic system is secure against entropy attack [14]. The entropy of test images that encrypted by using the original AES and proposed algorithm are shown in Table (4), where the entropy of encrypted images via the proposed algorithm is closer to the ideal value, which is 8, than original AES.

Table (4) Entropy values of encrypted images.

Image	Original AES	Proposed algorithm
Lena	7.9990	7.9991
Pens	7.9990	7.9991

5-6 NPCR and UACI Analysis

Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) are differential attack measurements used for evaluating the sensitivity to slight modification in the original data. Let's suppose the cipher images before and after modifying one pixel in a plain image are *C1* and *C2*. NPCR and UACI formulas are expressed as below:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \quad \dots (4)$$

$$UACI = \frac{1}{M \times N}\left[\frac{\sum_{i,j} C(i,j) - C\prime(i,j)}{255}\right] \times 100\% \quad \dots (5)$$

In which *D* is a two dimensional set and has the equal size of image *C1* or *C2* and *M*, *N* are the width and height of the image, respectively [15]. The

results of NPCR and UACI tests in Table (5) denote that the values of proposed algorithm are closer to the theoretical value than the original AES in most image components.

Table (5) NPCR and UACI results of encrypted images.

Image	Test	Original AES			Proposed algorithm		
		R	G	B	R	G	B
Lena	NPCR	99.6170	99.5575	99.5743	99.6170	99.6170	99.6414
	UACI	33.1902	30.4897	27.6885	33.1129	30.4110	27.7226
Pens	NPCR	99.6246	99.5575	99.6445	99.6460	99.5728	99.6475
	UACI	31.9935	33.1614	33.4866	32.0626	33.2123	33.4459

6-8 Execution Time

The time required by original AES and proposed algorithm to execute both encryption and decryption process for each test image is shown in Table (7). The execution time is calculated in seconds. Obviously, the proposed algorithm is faster than the original AES during the encryption and decryption process.

Table (7) Execution time of encryption and decryption process

Image	Original AES		Proposed algorithm	
	Encryption time	Decryption time	Encryption time	Decryption time
Lena	71.7176	101.9705	4.8735	5.3183
Pens	71.5997	101.7966	4.8697	5.3402

7- Conclusion

In general, speed and secure cryptosystem are very desirable for multimedia applications. In this paper, an efficient method is introduced for image encryption based on a modified AES algorithm by using a new 3D chaotic system. Figure (1) shows the attractor of the new chaotic system and it clearly displays chaotic behavior. The new chaotic system has two positive Lyapunov Exponents, thus it is hyper chaotic, which adds more unpredictability and randomness to corresponding system. According to the experimental results, the proposed algorithm provides high key space, high key sensitivity and less time for encryption and decryption than original AES as well as offering acceptable resistance against differential and statistical attacks.

References

[1] Komal D Patel and Sonal Belani, "**Image Encryption Using Different Techniques: A Review**", *International Journal of Emerging Technology and Advanced Engineering*,Vol. 1, Issue 1, November 2011.

[2] Shraddha Soni, Himani Agrawal and Dr. Monisha Sharma, "**Analysis and Comparison between AES and DES Cryptographic Algorithm**", *International Journal of Engineering and Innovative Technology (IJEIT)*, Vol. 2, Issue 6, December 2012.

[3] Shiguo Lian, "**MultiMedia Content Encryption: Techniques and Applications**", *CRC Press*, 2009.

[4] Sadiq A. Mehdi , Abid Ali H. Alta'ai and Salim Ali ABBAS , "**A novel chaotic System For Color Image Encryption**", *Journal of College of Education, Al-Mustansiryah University*, ISSN:1812-0380, No. 1,2017.

[5] Ali Abdulgader et al., "**Enhancement Of AES Algorithm Based On Chaotic Maps And Shift Operation For Image Encryption**", *Journal of Theoretical and Applied Information Technology*, Vol.71, No.1, January 2015.

[6] Yufen FENG et al., "**An Improved AES Encryption Algorithm Based on the Hénon and Chebyshev Chaotic Map**", *International Journal of Simulation: Systems, Science & Technology (IJSSST)*, Vol. 17, 2016.

[7] William Stalling., "**Cryptography and Network Security: Principles and Practices, Principles and Practices** ", 5th Ed. *Prentice Hall*, 2011.

[8] Saurabh Kumar, "**VLSI Implementation Of AES Algorithm**", M.Sc. Thesis, *Department of Electronics and communication Engineering, National Institute of Technology*, Rourkela, 2011-2013.

[9] GOPI.V, "**Design of Modified High Secure Optimized Mix Column and Virtual S-Box for AES**", *Department Of Electronica And Instrumentation Engineering, St.Peter's Institute Of Higher Education And Research*, St.Peter's University, April 2014.

[10] Jafar Biazar, Tahereh Houlari1 and Roxana Asayesh, "**Implementation of multi-step differential transformation method for**

hyperchaotic Rossler system", *International Journal of Applied Mathematical Research*, 6 (1), 2017.

[11] Gonzalo Alvarez and Shujun Li, "**Some Basic Cryptographic Requirements For Chaos-Based Cryptosystems**", *International Journal of Bifurcation and Chaos*, Vol. 16, No. 8, 2006.

[12] N.F.Elabady et al., "**Image Encryption Based on New One-Dimensional Chaotic Map**", *International Conference on Engineering and Technology (ICET)*, April 2014.

[13] Lingfeng Liu and Suoxia Miao, "**A New Image Encryption Algorithm Based on Logistic Chaotic Map With Varying Parameter**", *SpringerPlus*, 2016.

[14] Mohammed A. Shreef and Haider K. Hoomod, "**Image Encryption Using Lagrange-Least Squares Interpolation**", *International Journal of Advanced Computer Science and Information Technology (IJACSIT)*, Vol. 2, No. 4, 2013.

[15] O. S. Faragallah, "**Efficient confusion–diffusion chaotic image cryptosystem using enhanced standard map**", *Springer*, 2014.