AES WITH CHAOTIC USING CHEBYSHEV POLYNOMIAL

Tanya abdul-sattar jabor [1]
[1]Middle Technical University, Applied Arts Institute

Hiba A. Taresh[2]
[2] Building and Construction Engineering Department, University of Technology, Baghdad, Iraq
heba.art81@gmail.com

Alaa Q. Raheema[3]
[3]Building and Construction Engineering Department, University of Technology, Baghdad, Iraq
alaa.qassim1967@gmail.com

Abstract: All the important information is exchanged between facilities using the internet and networks, all these data should be secret and secured probably, the personal information of person in each of these institutions day by day need to organized secretly and the need of the cryptography systems is raised which can easily encrypt the personal and critical data and it can be shared with other centers via internet without and concerns about privacy. Chaotic performance is added to different phases of AES but very few apply it on key generation and choosing Chebyshev Polynomial will provide a chaotic map which will led to random strong key. our system based on modified advanced encryption standard (AES) , with encryption and decryption in real time taking to consideration the criticality of data images that been encrypted the main encryption algorithm is the same the modification is done by replacing the key generation algorithm by Chebyshev Polynomial to generate key with the required key size.

Keywords: Advanced encryption standard, AES, Chebyshev, modified AES.

I. INTRODUCTION

NIST selected the Rijndael method to be the new advanced encryption standard (AES). Due to the fact that Data Encryption Standard isn't considered to be a Standard anymore, the industries will be rushing from now on into the implementation of the advanced encryption standard for cryptographic application on the products they distribute. Considering that it is the strongest encrypting algorithm that has not been broken yet, it has its own set of drawbacks such as performance. There are different hardware applications for the advanced encryption standard, nevertheless, they each have advantages and disadvantages, and there's lots of effort that is continuously accomplished in this field in order to reach perfection [1].
Some researchers work on breaking the security of AES in 2010 [2] found some issue with the shifting in row which may affect the key.
In 2011 [3] work on modification of the s-box by using 1-D logistic chaos equation and modification to the algorithm is done in [4] by adding chaotic features to s-box using chaotic baker's map equations.

A. Theoretical background:

1) Advanced encryption standard (AES):

In the year of 1997 NIST published a call for proposing a new symmetrical algorithm, known as the Advanced Encryption Standard (AES). In the year of 2000 NIST declared that Rijndael has been selected to be the successor of each of the data encryption standard and AES. The mix of performance, security, sufficiency, flexibility and implementing capability established Rijndael a proper choice for the AES [5].
The nominees for the algorithm of Advanced Encryption Standard were obliged to meet specific designing criteria. Initially, obviously the algorithm had to be a symmetric and it had to be robust in the face of all known attacks. In addition, this algorithm has to be sufficient in implementation and memory for various kinds of platforms. The design had to be simple capable of handling various lengths of keys (128 bits, 192 bits and 256 bits). The block length of the cipher had to be 128 bits [6].

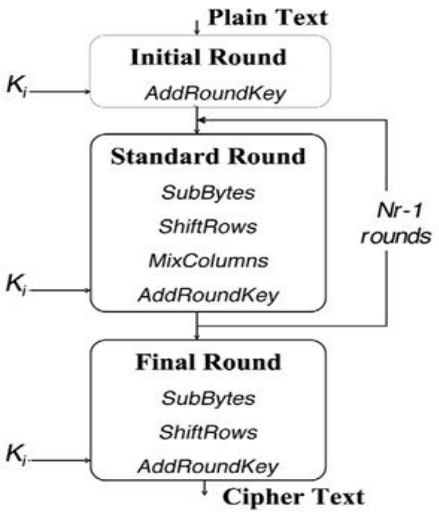

Fig.1. AES general rounds [7]

The AES start with initial round and after that a specific number of standardized rounds, finally it terminates with the last round. Merely 4 distinct processes are necessary for computing those rounds in addition to a key schedule [8].
In Rijndael it is permitted using various key lengths depending on the degree of security needed for the implementation. This method is identified as standard block cipher with deferent key lengths equal to 128 bits, 192 bits or 256 bits. The probable input blocks lengths are 128 bits, 192bits or 256bits for this approach. Advanced Encryption Standard is identical to the Rijndael, with one difference that it only accepts input length of block equal to 128 bits [8].

AES is designed in a way that every one of the bits depends on all the bits from the previous two rounds, for example, full Shannon criteria(diffusion and confusion) is given. The rounds numbers which have to be executed depends on the length of the algorithm key.

2) Encryption:

The AES start with initial round and after that a specific number of standardized rounds, finally it terminates with the last round. Merely 4 distinct processes are necessary for computing those rounds in addition to a key schedule [8].
In Rijndael it is permitted using various key lengths depending on the degree of security needed for the implementation. This method is identified as standard block cipher with deferent key lengths equal to 128 bits, 192 bits or 256 bits. The probable input blocks lengths are 128 bits, 192bits or 256bits for this approach. Advanced Encryption Standard is identical to the Rijndael, with one difference that it only accepts input length of block equal to 128 bits [8].
AES is designed in a way that every one of the bits depends on all the bits from the previous two rounds, for example, full Shannon criteria(diffusion and confusion) is given. The rounds numbers which have to be executed depends on the length of the algorithm key

TABLE (1): KEY LENGTHS

	Key length (words)	Number of rounds (Nr)
AES-128	4	10
AES-192	6	12
AES-256	8	14

1. Add Round Key
This step is merely an exclusive-or process between the Key and the State. Round Key step derived from the ciphering key by using key schedule. The Round Key and State have an identical size and for obtaining the next State the E-XOR process is performed an element at a time [5]:

Where:
- S represents the current State.
- S the next one.
- W represents the Round Key.

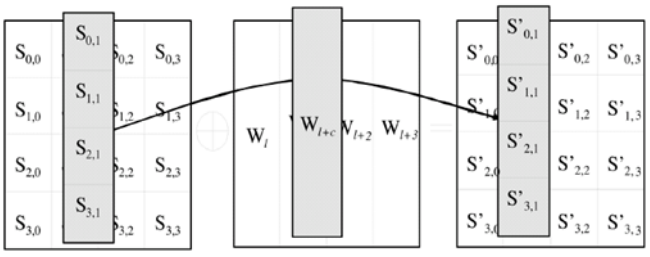

Fig.2. the Operation of the Add Round Key [7]

2. Substitute Bytes
This procedure is identical to the Substitution-box used in the DES. Rijndael has only a single S-box. The criteria followed in design for the S-boxes are in a way that they are robust in the face of the known linear and differential cryptanalysis and attacks by the means of algebraic alterations [8].

		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
x	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Fig.3. an Example of the AES S-Box [4]

3. Shift Rows

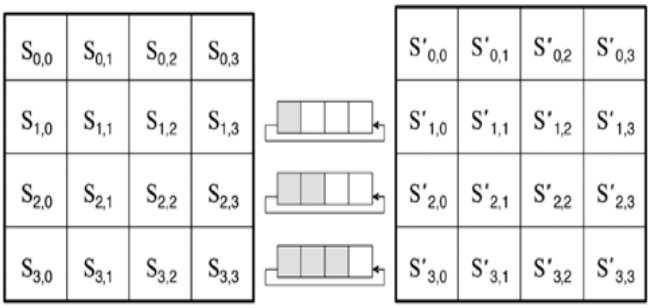

Fig.4. an Illustration of the Shift Rows Operation [4]

In this operation, the rows of State are shifted in a cyclic way with various values. The first row is shifted by c1 bytes, the second row by c2 bytes, and the third row by c3 bytes. c1, c2, and c3 values are dependent on block length, i.e. Nb: [9]

Nb	c1	c2	c3
4	1	2	3
6	1	2	3
8	1	3	4

doi: 10.25195/2017/4426

4. Mix Columns

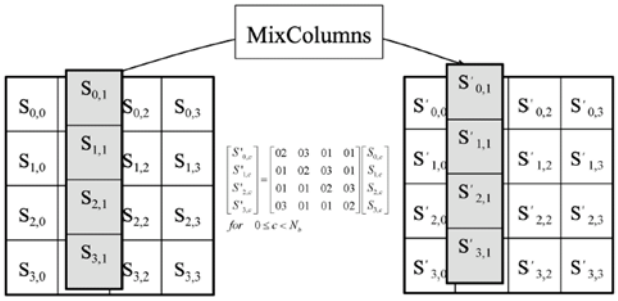

Fig.5. Mix Columns

The Mix Column is a process on various columns. For the calculation of this operation the current state columns are represented as pre-defined polynomials in the field of GF (28) [10

3) Key schedules.

Round Keys which obtained from the Cipher-Key with using a key schedule step. The number of round related to Keys that are needed for encrypting a single block of data is dependent on the lengths of the block and the key due to the fact that this will provide the number of rounds. And length of a block with the equal to 128 bits, with eleven Round Keys (one for the first round, nine for the standard rounds and one for the last round) are required [9]

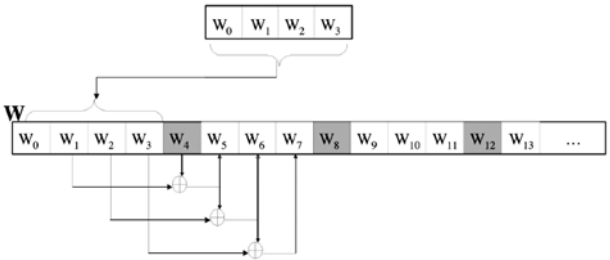

Fig.6. Key Schedule

4) Chebyshev polynomials:

Are sequences of orthogonal polynomials that are in a correlation with the formula of de Moivre's and that might be identified in a recursive way. It is typically distinguished between Chebyshev polynomials of the 1st type that are represented by Tn and Chebyshev polynomials of the 2nd type represented by Un.

Those polynomials Tn or Un are of degree n and the series of Chebyshev polynomials of any of the kinds generates the sequence of the polynomial [6].

The Chebyshev polynomial Tn is a polynomial with the biggest probable leading coefficient, nevertheless subjected to the case where their absolute value on the interval [−1,1] is bounded by

1. In addition, it is the extremely polynomial for several of other features. [6]

This type of polynomials is valuable in the theory of approximation due to the fact that the roots of those polynomials are of the 1st type, which are known as the Chebyshev nodes as well, are utilized as nodes in polynomial interpolations. The resultant polynomial of interpolation plays a role in the minimization of the issue of Runge's phenomenon and also gives an approximation near to the polynomial of the optimal approximation to a continuous function within the maximal norm. This approximation directly results in the approach of Clenshaw–Curtis quadrature [6].

$$(1-x^2)\,y'' - xy' + n^2 y = 0$$

And

$$(1-x^2)\,y'' - 3xy' + n(n+2)y = 0$$

2. Proposed system:

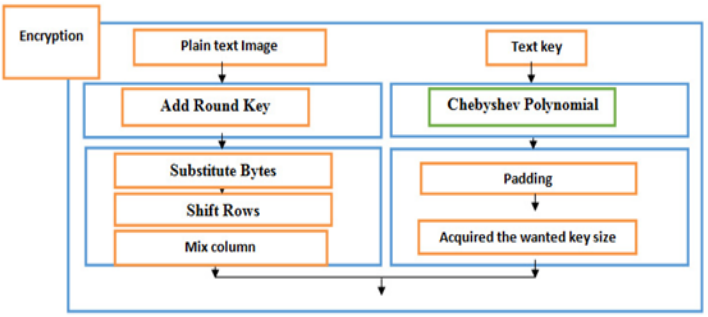

Fig.7 one round of the proposed system

The proposed modification to the AES by merges the chaotic behavior of Chebyshev polynomial to produce the key that is used for encryption and decryption operation the state in the original AES state is replaced by the output of the Chebyshev polynomial which will provide more randomness to the key of the system which provide higher level to the security with the unpredictable behavior of the Chebyshev polynomial to calculate the key.

The original key generation algorithm in the AES is a strong tool to find the key but since many attacks were made to this algorithm and its key generation a chaotic characteristics could be added to the system of AES to provide more randomness levels.

The analysis of the result obtained is measured via applications and two image samples is used and tested, the time comparison is done via calculation the time takes for using the system to encrypt the two sample images and the randomness of the system is tested as shown in table (2).

The proposed system pass all the statistical tests applied to the system done with the p-value table (3) and chai square table (2)

TABLE (2): TEST RESULTS OBTAINED BY USING CHAI VALUE STATISTICAL TESTS

tests	Standard key	Chebyshev key
frequency	0.93	0.4723
serial	1.923	0.05284
poker	6.41	1.7842
run	5.53	3.3402
Auto correlation	1.78	1.3333

TABLE (3): TEST RESULTS OBTAINED BY USING NIST STATISTICAL TESTS PACKAGE

Tests	Standard key	Chebyshev key
Frequency	Pass	Pass
Frequency Test within a Block	Pass	Pass
Runs	Pass	Pass
Longest Run of 1s in a Block	Pass	Pass
Binary Matrix Rank	Pass	Pass
Discrete Fourier	Pass	Pass
Transform	Pass	Pass
Non-overlapping Template Matching	Pass	Pass
Overlapping Template Matching	Pass	Pass
Maurer's	Pass	Pass
Linear Complexity	Pass	Pass
Serial	Pass	Pass
Approximate Entropy	Pass	Pass
Cumulative Sums	Pass	Pass
Random Excursions	Pass	Pass
Random Excursions Variant	Pass	Pass

Fig.7. image sample 1

Fig.8. image sample 2

Samples images is encrypted via the proposed modified AES and decrypted and the resulted data is obtained as Figure (9, 10), since the main input of this system is tested by using images the details of the image used and its histogram should hide the details of the pictures which mean the encryption process done correctly.

Fig.9 sample 1 encrypted image

Fig.10. sample 2 encrypted image

The histogram which represents the distribution of pixels in the image which will provide better understanding to the changing to the pixels encrypted by the proposed modified AES will be calculated and the entropy which represent is average amount of information produced by a probabilistic stochastic source of image data will be calculated for both the encrypted and original samples images

The calculated entropy of the images show increasing in its value (maximizing the entropy) which means improving the security by changing the texture of the image and all the original information will be secure ,Entropy details in table 4 and figure (11, 12, 13, and 14).

TABLE (4) ENTROPY

Image name	Entropy
Original sample 1	3.45114385987626
Encrypted sample 1	9.02627923737164
Original sample 2	8.39809460272765
Encrypted sample2	9.03615015385716

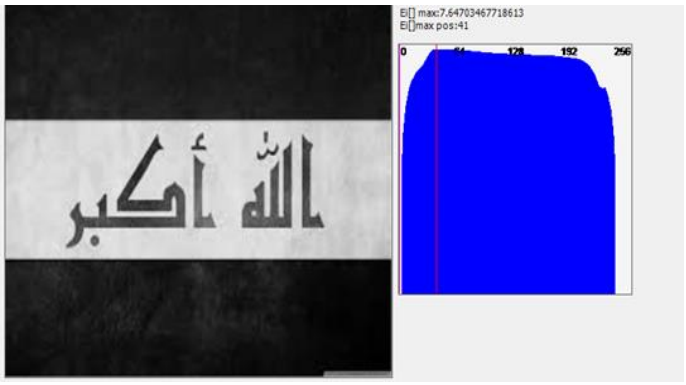

Fig.11. original sample 1 entropy

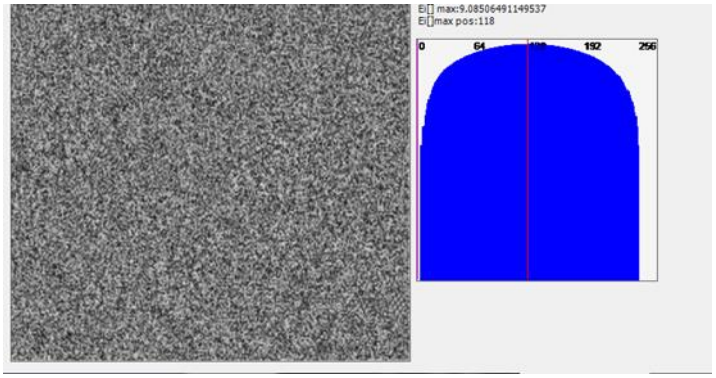

Fig.12. encrypted sample 1 entropy

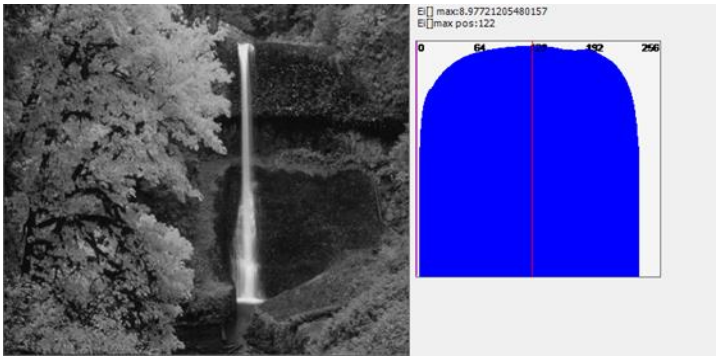

Fig.13. original sample 2 entropy

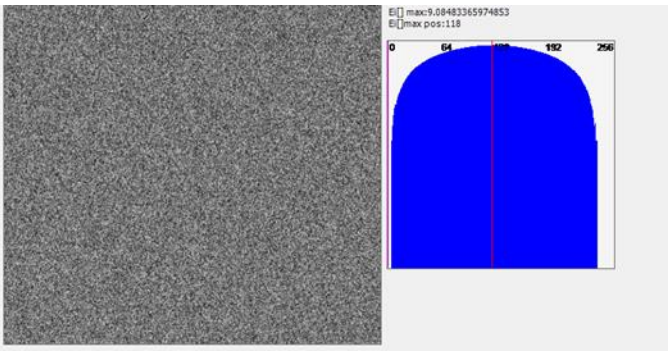

Fig.14. encrypted sample 2 entropy

The histogram details for all images is calculated, figure (15, 16, 17 and 18)

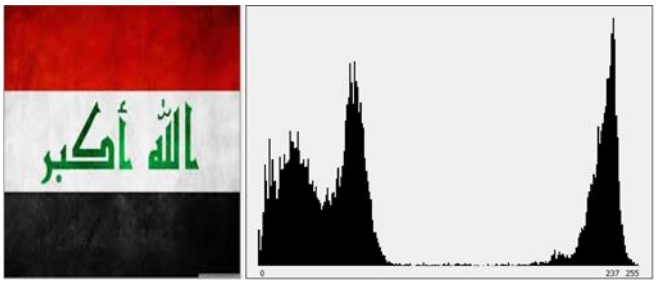

Fig.15. original sample1 histogram

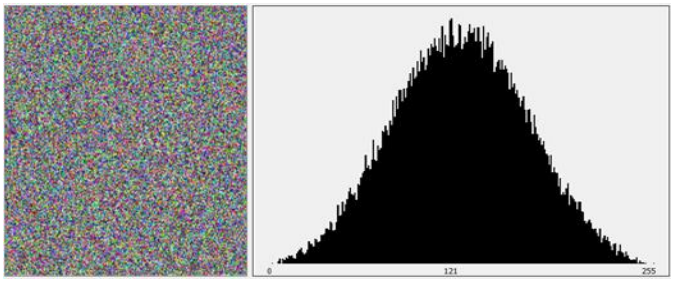

Fig.16. encrypted sample1 histogram

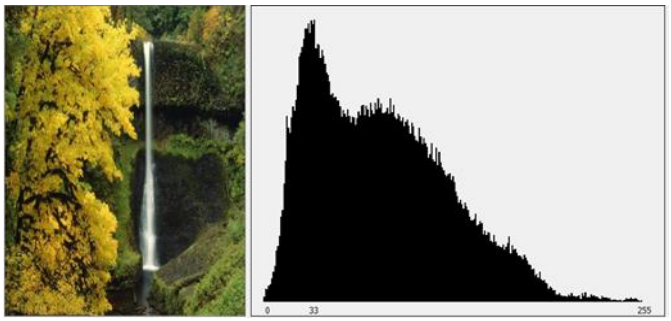

Fig.17. original sample2 histogram

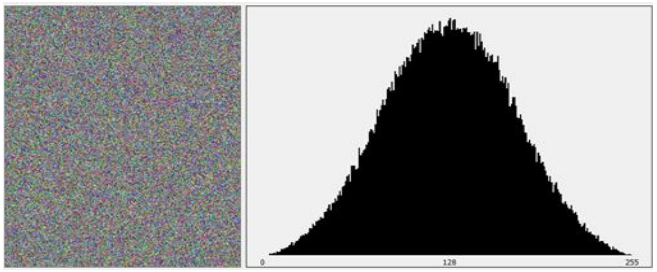

Fig.18 encrypted sample2 histogram

Conclusions:

Using chaotic algorithms merging with exist will help to provide a randomness level to the key that most of the block cipher algorithms looking for.

The proposed system pass all the randomness tests provided by NIST.

REFERENCES

[1] Stallings, William, and Lawrie Brown. "Computer security." Principles and Practice (2008).

[2] El-Sayed Abdoul-Moaty ElBadawy, Amro Mokhtar, Waleed A. El-Masry, Alaa El-Din Sayed Hafez (2010), "A New Chaos Advanced Encryption Standard (AES)Algorithm for Data Security", International Conference on Signals and Electronic Systems, Poland, pp 405- 408.

[3] Zhang Zhao, Sun Shiliang (2011), "Image encryption algorithm Based on Logistic chaotic system and s- box scrambling", 4th International Congress on Image and Signal Processing , IEEE, pp: 177-181.

[4] Amutha, V., and CT Vijay Nagaraj. "A Secured Joint Encrypted Watermarking In Medical Image Using Block Cipher Algorithm." International Journal Of Innovative Research In Science, Engineering And Technology 3.

[5] Tanya abdul sattar and hala bahjat "improve NTRU algorithm based on chebyshev polynomial"WCTTCA , IEEE (2015).

[7] Biryukov, Alex. "Block Ciphers and Stream Ciphers: The State of the Art." IACR Cryptology ePrint Archive 2004 (2004): 94.

[8] Federal Information Processing Standards Publications (FIPS 197), "Advanced Encryption Standard (AES) ", 26 Nov. 2001.

[9] K. Gaj, P.Chodowiec, "Fast implementation and fair comparison of the final candidates for advanced encryption standard using field programmable gate arrays", in : CT-RSA 2001, pp.84-99.

[10]J.J. Amador, R. W.Green "Symmetric-Key Block Cipher for Image and Text Cryptography": International Journal of Imaging Systems and Technology, No. 3, 2005, pp. 178-188.