ICIC Express Letters
Part B: Applications
Volume **10**, Number **9**, September **2019**

ICIC International ©2019 ISSN 2185-2766
pp. **823–832**

A NOVEL APPROACH FOR ENHANCING SECURITY OF ADVANCE ENCRYPTION STANDARD USING PRIVATE XOR TABLE AND 3D CHAOTIC REGARDING TO SOFTWARE QUALITY FACTOR

Adnan Ibrahem Salih[1], Ashwak Alabaichi[2] and Ahmed Saleem Abbas[3]

[1]Computer Science Department
College of Science
Kirkuk University
Sayada, Kirkuk 36001, Iraq
adnan.alezzi@uokirkuk.edu.iq

[2]Biomedical Engineering Department
College of Engineering
Kerbala University
P.O.BOX 1125, Fraiha, Kerbala 56001, Iraq
ashwaq.alabaichi@gmail.com

[3]Software Department
College of Information Technology
University of Babylon
P.O.BOX 4, Hilla 51002, Iraq
ahmed_saleam@yahoo.com

Received February 2019; accepted April 2019

Abstract. *The Internet is a medium with low security, so there is a real need for measures to guarantee data integrity and privacy in the networks and associated computer systems. Cryptography plays a valuable role to provide security for data transmission over insecure network. Cryptographic protocols changed data into unreadable text, which may be solely decrypted by those who own the associated key. The Advanced Encryption Standard (AES) is a block cipher algorithm which is symmetric key, that provides a higher level of security and speed as well as throughput; however, still modifications of the algorithm are continuing to boost its performance. This paper introduces a novel approach to increase the security of the AES by replacing the predefined XOR operation which is applied during rounds in AES with a novel private XOR table depending on 3D chaotic map. 3D chaotic map is used as private keys. The private XOR table is based on 4 bits. This replacement adds a new level of security strength. DIEHARD packages and NIST test, entropy, information, and histogram were conducted on a novel Approach. From the results it can be concluding that it is the best in comparison with the original AES. C++ is used in the implementation of the novel approach and original algorithm. MATLAB computing software (R2018a, Mathworks) is used to implement the information entropy and histogram.*

Keywords: AES, NIST, DIEHARD, 3D chaotic map, Private XOR, Software quality factor, Information entropy, Histogram

1. **Introduction.** Recently with the large growth of digital communication over the network, the safety of data content becomes a significant concern. Several security threats are caused by net itself and those threats will destroy the transferred knowledge over a network. Therefore, data security techniques are becoming more essential in today's applications. Security is needed in our daily, particularly the transaction that involves secret data. The information security may be done by cryptographic algorithms as AES, Data Encryption Standard, Twofish, Blowfish, IDEA, SEAL, RC4 & CAST. AES is the

DOI: 10.24507/icicelb.10.09.823

block cipher based symmetric key cryptography to protect the sensitive information. The key sizes of AES are 128, 192, 256 bits. AES is based on substitution-permutation s-trategy. In 2001, NIST accepted Rijndael algorithm as AES after five years of security analysis and evaluation. It is highly secure and efficient compared with DES and other symmetric-key cryptographic algorithms [1-4]. Chaos refers to randomness and makes a definition for it as a study of a nonlinear dynamic system. The properties of these chaos systems are characterized mainly sensitivities to initial conditions and other system parameters. Due to this sensitiveness, the system acts very randomly. Chaotic map has many advantages such as high flexibility within the secret system, accessibility of the huge range of variation in chaotic systems and huge number of secret keys, complex and easy design. This promises to provide strong encryption without compromising the usability system in terms of speed and robustness. 1D chaotic map has a small key space and low security. Consequently, higher-dimensional chaotic systems are currently the focus of recent research. In addition, 3D functions provide good security against cryptanalytic attacks as well as in comparison with one and two dimensional maps, three-dimensional maps offer higher security and randomness algorithm [5-7]. Therefore, 3D chaotic map is used in the current study. In particular, the 3D logistic map is adopted for the proposed algorithm. In this article, a novel approach for enhancing security of AES is suggested. The enhancement is directed by exchange XOR operation in AES by non-public XOR table exploitation 3D logistic map. This table is equivalent to the XOR operation in AES but in this table will be got the different numbers when conducting it. For example, the XOR in AES between two numbers such as two and eleven will be nine but in this table the result will be different. Thus, the security of AES will be increased. The next sections of this paper are arranged as follows. Section 2 illustrates the structure of AES. Section 3 describes a chaotic map and its properties that are associated with cryptography. Section 4 explains the proposed algorithm thoroughly. Section 5 presents the security analysis of the both algorithms proposed and original algorithms. Finally, Section 6 gives conclusion & future works.

2. **Advanced Encryption Standard.** Joan Daemen and Vincent Rijmen [2,3] developed Rijndael which is a block cipher. This algorithm will support any combination of data and key size may be (128, 192, or 256) bits. However, AES merely permits a 128 bit block length that may be divided into four basic operation blocks. These blocks work on a matrix of bytes and are organized as a 4×4 matrix that is referred to as "state". For complete encryption process, the data is passed inside Nr rounds which are 10, 12, and 14. The subsequent steps represented the encryption method:

- Initial Round: AddRoundKey
- Rounds: SubBytes, ShiftRows, MixColumns, and AddRoundKey
- Last Round: SubBytes, ShiftRows, and AddRoundKey
- SubBytes – A non-linear substitution step where every byte is changed by replacing with another by depending on the S-box.
- ShiftRows – A transposition step where every row of the state is shifted periodically (a certain number of times).
- MixColumns – A mixing operation, which works on the columns of the state, combining the 4 bytes in every column.
- AddRoundKey – States's each byte is combined with the block of the round key XORed with I/Pblock operation.

Rijndael's round function is explained above and it is four-layered. The decryption method is completed in reverse order of encryption method [9-11].

3. **Chaotic Map.** Chaos is a present ubiquitous phenomenon existing in deterministic nonlinear systems that exhibit sensitivity to initial condition and generate the longest non

repetitive random like sequence. The features of chaos are sensible to initial condition; this sensitivity property is employed for the keys of cryptosystems that makes it thus tough to decipher topological transitivity connected to the diffusion characteristic of cryptosystem, and density of periodic purpose. These features usually accustomed build symmetric cryptography key in chaotic cryptography. The encrypting becomes so sophisticated as a result of the property of sensitivity to initial conditions. The sequence is additionally sensible to control parameter [5,6,12,13].

- **3D Logistic Map**

The most simple chaos formula is logistic map such as below:

$$x_{n+1} = \lambda x_n(1 - x_n) \tag{1}$$

For $0 < x_n < 1$ and $\lambda = 4$ the formula depicts the behavior of chaotic. In [8] the authors suggest the 2D logistic map shown by the equations below:

$$x_{i+1} = \mu_1 x_i(1 - x_i) + \gamma_i y_i^2 \tag{2}$$

$$y_{i+1} = \mu_2 y_i(1 - y_i) + \gamma_2 \left(x_i^2 + x_i y_i\right) \tag{3}$$

The above equations maximize the quadratic coupling of the items y_i^2, x_i^2, $x_i y_i$ and produce more security to the system.

When $2.75 < \mu_1 < 3.4$, $2.7 < \mu_2 < 3.45$, $0.15 < \gamma_1 < 0.21$, and $0.13 < \gamma_2 < 0.15$, the system comes into chaotic state and can produce a chaotic sequence within the region $(0, 1)$.

3D logistic map is extending to 2D logistic map by using the following equations:

$$x_{i+1} = \lambda x_i(1 - x_i) + \beta y_i^2 x_i + \propto z_i^3 \tag{4}$$

$$y_{i+1} = \lambda y_i(1 - y_i) + \beta z_i^2 y_i + \propto x_i^3 \tag{5}$$

$$z_{i+1} = \lambda z_i(1 - z_i) + \beta x_i^2 z_i + \propto y_i^3 \tag{6}$$

Equations (4) to (6) represented the chaotic behavior for $3.53 < \lambda < 3.81$, $0 < \beta < 0.022$, $0 < \alpha < 0.015$ and can take the values in $[0, 1]$ [6,14,15].

4. **Proposed Algorithm.** In this section, the proposed algorithms can be abstracted in the following points.

- Initialize the three secret parameters of the 3D logistic map to produce secret keys.
- Generate secret keys from the 3D logistic map.
- Convert them to decimal numbers between 0 and 15 using the following equations.

$$x_{i,j} = \left(x_{i,j} \times 10^{10} \bmod 16\right) \tag{7}$$

$$y_{i,j} = \left(y_{i,j} \times 10^{10} \bmod 16\right) \tag{8}$$

$$z_{i,j} = \left(z_{i,j} \times 10^{10} \bmod 16\right) \tag{9}$$

- XOR between x, y, and z.
- The XOR in AES with four bits can be shown in Figure 1.

From the XOR table, it can be seen the following features.

- Sum every row or column equal to 120.
- Every column or row includes the numbers (0 to 15) without repeating.
- The table is a symmetric.

Private XOR table has the same properties of the XOR in AES except the numbers are generated from 3D chaotic map. Figure 2 illustrates private XOR table.

It will be seen XOR in AES crossing between row eleven and column three is eight whereas in private XOR table is five. Algorithm (1) is used to generate private XOR table. Every byte in AES will be divided into two 4 bits. The first byte represents rows while the second byte represents columns and the intersection between them is the results. For example, the first byte is 11101011 and the second byte is 11100110. The first byte

xor	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	0	3	2	5	4	7	6	9	8	11	10	13	12	15	14
2	2	3	0	1	6	7	4	5	10	11	8	9	14	15	12	13
3	3	2	1	0	7	6	5	4	11	10	9	8	15	14	13	12
4	4	5	6	7	0	1	2	3	12	13	14	15	8	9	10	11
5	5	4	7	6	1	0	3	2	13	12	15	14	9	8	11	10
6	6	7	4	5	2	3	0	1	14	15	12	13	10	11	8	9
7	7	6	5	4	3	2	1	0	15	14	13	12	11	10	9	8
8	8	9	10	11	12	13	14	15	0	1	2	3	4	5	6	7
9	9	8	11	10	13	12	15	14	1	0	3	2	5	4	7	6
10	10	11	8	9	14	15	12	13	2	3	0	1	6	7	4	5
11	11	10	9	8	15	14	13	12	3	2	1	0	7	6	5	4
12	12	13	14	15	8	9	10	11	4	5	6	7	0	1	2	3
13	13	12	15	14	9	8	11	10	5	4	7	6	1	0	3	2
14	14	15	12	13	10	11	8	9	6	7	4	5	2	3	0	1
15	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0

FIGURE 1. XOR in AES

xor	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	7	8	3	2	14	12	6	0	1	9	15	11	5	13	4	10
1	8	9	2	14	6	15	4	7	0	1	10	13	12	11	3	5
2	3	2	1	0	13	9	14	15	12	5	11	10	8	4	6	7
3	2	14	0	9	10	11	13	12	15	3	4	5	7	6	1	8
4	14	6	13	10	7	8	1	4	5	15	3	12	11	2	0	9
5	12	15	9	11	8	5	10	13	4	2	6	3	0	7	14	1
6	6	4	14	13	1	10	0	11	8	12	5	7	9	3	2	15
7	0	7	15	12	4	13	11	1	14	10	9	6	3	5	8	2
8	1	0	12	15	5	4	8	14	6	11	13	9	2	10	7	3
9	9	1	5	3	15	2	12	10	11	0	7	8	6	14	13	4
10	15	10	11	4	3	6	5	9	13	7	1	2	14	8	12	0
11	11	13	10	5	12	3	7	6	9	8	2	0	4	1	15	14
12	5	12	8	7	11	0	9	3	2	6	14	4	1	15	10	13
13	13	11	4	6	2	7	3	5	10	14	8	1	15	0	9	12
14	4	3	6	1	0	14	2	8	7	13	12	15	10	9	5	11
15	10	5	7	8	9	1	15	2	3	4	0	14	13	12	11	6

FIGURE 2. Private XOR table

is divided into 1011 which is equal to 11 and to 1110 is equal to 14 which represent rows while the second byte 11110110 is divided into 0110 which is equal to 6 and to 1111 is equal to 15 which represent columns. The intersection between the 11 and 6 is equal to 7 that is 0111 while the intersection between 14 and 15 is equal to 11 that is 1011. The

result byte will be concatenated between them as 10110111. The following algorithm is used to generate the private XOR table.

Algorithm (1): Private XOR table generation
Input: seed, is initial of 3D logistic map
Output: p_xor is an array of 16 rows and 16 columns representing private XOR table.
Generate secret keys from 3D logistic map x, y, z.
XOR between x, y, z and set them in $x1$
Begin:
For $i = 0$ to 15 do
    For $j = i$ to 15 do
Label1:
Set $x1$ is a random number ranged from 0 to 15
        IF $x1$ value not found in column p_xor[j] and row p_xor[i] Then
            p_xor[i,j] = $x1$
            p_xor[j,i] = $x1$
        Else
            Go to Label1
        End if
    End for
End for

5. **Security Analysis.** In this section, we present number of analyses as NIST test, histograms, DIEHARD packages, and information entropy to ensure the enhanced security of the proposed algorithm. The security analysis is conducted by using MATLAB (R2018a) software platform in a laptop with Intel® Core™ i7-7500U.

5.1. **National Institute of Standard and Technology (NIST) test.** The most significant aspects of the security of any cryptography algorithms are the randomness of its output. One element used to assess the AES candidate algorithms was their established suitability as random number generators. Randomness test is one of the security analyses to measure confusion and diffusion properties of the new encryption algorithm [21-23]. The NIST test is known as statistical package, and it comprises 15 tests. These tests were established to test the arbitrariness of random long binary sequences. These sequences are produced by either hardware or software [16-18,24,26]. The proposed algorithm has generated 128 different sequences, each of 1,000,000 bits. The P value is calculated according to each corresponding sequence across all 15 tests of NIST and the results are presented in Table 1. The results in Table 1 have shown that the sequences have all successfully passed the arbitrariness tests. Therefore, it can be deduced that the proposed algorithm has generated sequences that possess good arbitrary properties satisfying the conditions for all 15 tests in the NIST. The symbol $\surd$ in table means pass.

5.2. **DIEHARD tests.** The DIEHARD test battery consists of twelve tests of which few repeated with various parameters. These tests are choosing arbitrary points on a large interval. The spacings between the points ought to be asymptotically Poisson distributed. The name is based on the birthday contradictory. DIEHARD statistical package is made up of a number of standard tests that operate by P-value method [17]. The result of DIEHARD test is shown in Table 2.

5.3. **Histogram analysis.** In statistics, a histogram is a graphic show of tabulated frequencies depicted as bars. It illustrates what proportion of cases represents into several classes. It is a kind of data binning. The classes are typically specified as intervals of some

TABLE 1. Results of the NIST tests of the proposed algorithm

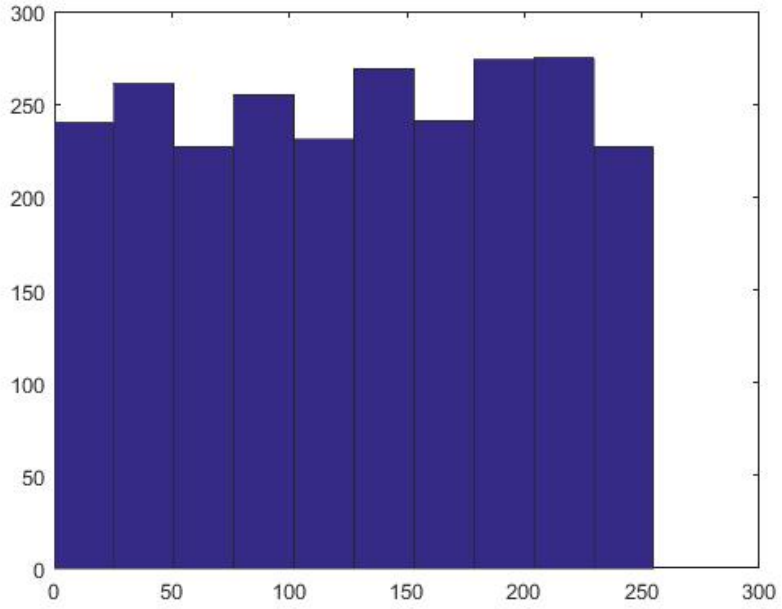
No	Test	Success sequence P-value	Proportion successful	Assessment
1	Frequency	0.819544	1.0000	√
2	Block frequency	0.043745	0.976563	√
3	Accumulative sums (forward)	0.437274	0.992188	√
	Accumulative sums (reverse)	0.500934	1.0000	√
4	Run	0.116519	0.992188	√
5	FFT	0.162606	0.992188	√
6	Non Overlapping Template	0.42599	0.988123	√
7	Overlapping Template	0.671779	0.992188	√
8	Universal	0.931952	0.992188	√
9	Approximate Entropy	0.037157	0.992188	√
10	Long run	0.337162	0.984375	√
11	Rank	0.534146	1.0000	√
12	Random Excursions	0.458257	0.996115	√
13	Random Excursions Variants	0.445946	1.0000	√
14	Serial 1	0.422034	1.0000	√
	Serial 2	0.602458	1.0000	√
15	Linear Complexity	0.468595	0.984375	√

TABLE 2. Results of DIEHARD tests

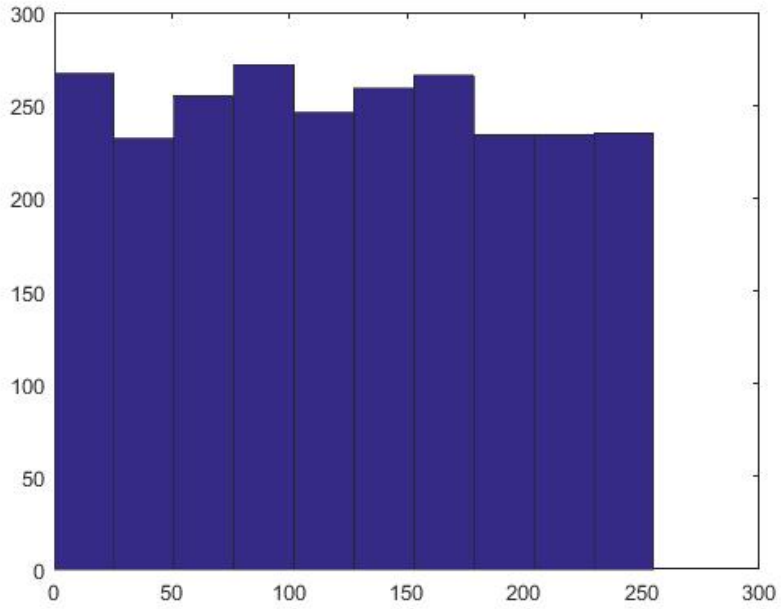
Test	P-value	Assessment
Birthdays	0.495535	√
Operm5	0.465079	√
32×32 Rank	0.498203	√
6×8 Rank	0.571041	√
Bit stream	0.607126	√
OPSO	0.508648	√
OQSO	0.5112	√
DNA	0.437519	√
Count-1s-star	0.533108	√
Count-1s-byte	0.635047	√
Parking-lot	0.518915	√
Minimum Distance	0.915335	√
3dspheres	0.929953	√
Squeeze	0.44562	√
Overlapping Sums	0.531665	√
Run	0.456044	√
Craps	0.568977	√

variable while not overlapping. The classes "bars" should be adjacent. Generally, the intervals are at an equivalent size, and are most simply inferred [19,20]. In Figure 3, the histograms of the proposed algorithm and the original algorithm (AES) with 2500 8-bit numbers are tested. Based on graphics, the proposed algorithm can generate a uniform output.

5.4. **Information entropy.** Information theory is the mathematical theory of information storage and communication. Recent information theory cares with data compression,



(a) Histogram of the proposed algorithm



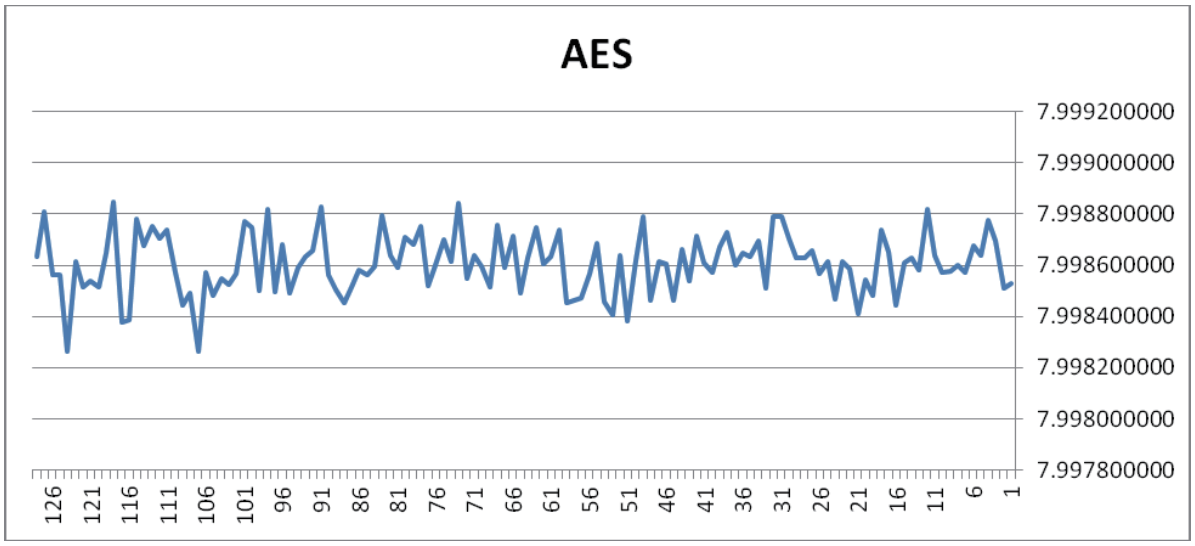
(b) Histogram of AES

FIGURE 3. (a) Histogram of the proposed algorithm and (b) histogram of AES

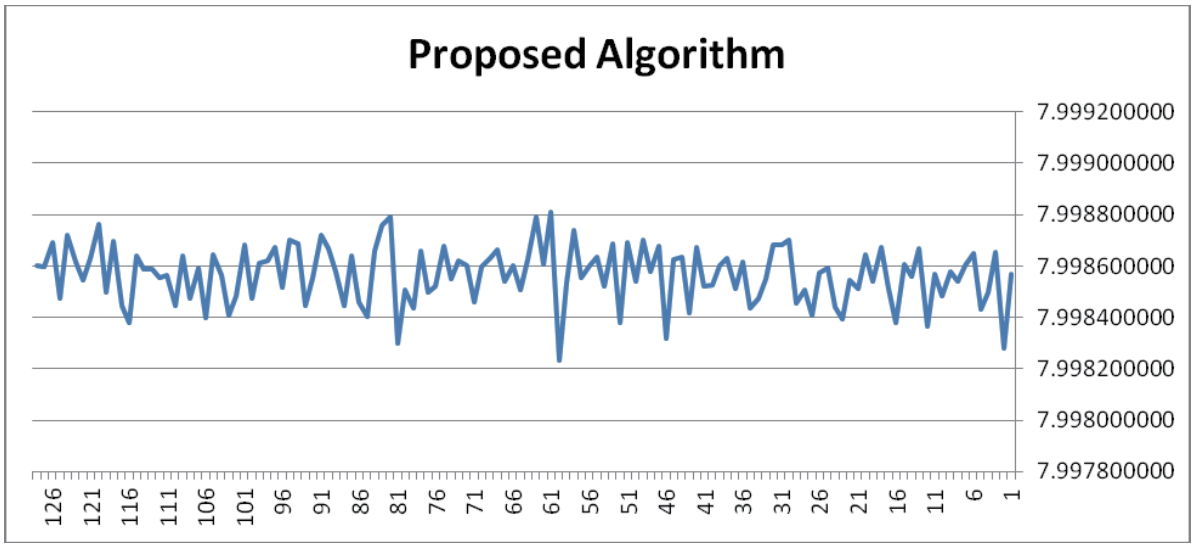
error-correction, communications systems, cryptography, and associated topics. To figure the entropy $H(m)$ of a supply m, we have:

$$H(m) = \sum_{i=0}^{2^{n-1}} p(m_i) \log_2 \frac{1}{p(m_i)} \text{ bits}, \tag{10}$$

And $p(m)$ is the likelihood of symbol m and therefore the entropy is represented in the bit. Assume that the supply emits 2ˆ8 symbols with equal likelihood. Using Equation (10), the entropy will be eight according to a very random source. Rarely produce random



(a) Entropy of AES



(b) Entropy of the proposed algorithm

FIGURE 4. (a) Histogram of AES and (b) histogram of the proposed algorithm

messages; generally its entropy worth is smaller than the perfect one. However, once the messages are encrypted, their entropy ought to ideally be eight. If the entropy of cipher displays result less than eight, there exist percentage of obviousness and the security will be violation [25]. The result of entropy is calculated on 128 sequences of 1000000 bits of the proposed and the AES algorithms using 128 different randomly keys. Figure 4 shows the results of entropy for both proposed and the AES algorithms. The average entropy of the proposed algorithm is 7.998602793256858. While of the AES are 7.998602816030 the entropy in the proposed algorithm and AES are nearly 8.

6. **Conclusion and Future Works.** This study proposes to use private XOR table in AES based on 3D chaotic map instead of XOR operation to increase security and make XOR operation secure instead of public. From the experimental results it can be witnessed that the proposed algorithm can provide high levels of security and that lead to high level of software quality. In future work, XOR will be dynamic.

REFERENCES

[1] A. Moh'd, Y. Jararweh and L. Tawalbeh, AES-512: 512-bit advanced encryption standard algorithm design and evaluation, *Proc. of the 7th International Conference on Information Assurance and Security (IAS)*, pp.292-297, 2011.

[2] A. Alabaichi and A. Salih, Enhancing security of advance encryption standard algorithm based on key dependent S-box, *Proc. of the 5th International Conference on Digital Information Processing and Communications*, Switzerland, pp.44-53, 2015.

[3] S. K. Rao, D. Mahto and D. A Khan, A survey on advanced encryption standard, *International Journal of Science and Research (IJSR)*, vol.6, no.1, pp.711-724, 2017.

[4] P. K. Choudhury and S. Kakoty, Comparative analysis of different modified advanced encryption standard algorithms over conventional advanced encryption standard algorithm, *International Journal of Current Research and Review*, vol.9, no.22, pp.31-34, 2017.

[5] A. Alabaichi, Color image encryption using 3D chaotic map with AES key dependent S-Box, *International Journal of Computer Science and Network Security (IJCSNS)*, vol.16, no.10, pp.105-115, 2016.

[6] A. Alabaichi, True color image encryption based on DNA sequence, 3D chaotic map, and key-dependent DNA S-Box of AES, *Journal of Theoretical and Applied Information Technology (JATIT)*, vol.96, no.2, pp.304-321, 2018.

[7] M. Ahmad and S. Alam, A new algorithm of encryption and decryption of images using chaotic mapping, *International Journal on Computer Science and Engineering*, vol.2, no.1, pp.46-50, 2009.

[8] H. Liu, Z. Zhu, H. Jiang and B. Wang, A novel image encryption algorithm based on improved 3D chaotic cat map, *The 9th International Conference for Young Computer Scientists*, Hunan, China, pp.3016-3021, 2008.

[9] M. Zeghid, M. Machhout, L. Khriji, A. Baganne and R. Tourki, A modified AES based algorithm for image encryption, *International Journal of Computer, Electrical, Automation, Control and Information Engineering*, vol.1, no.3, pp.745-750, 2007.

[10] A. AL-Abiachi, F. Ahmad and K. Ruhana, A competitive study of cryptography techniques over block cipher, *Proc. of the 13th International Conference on Modelling and Simulation (UKSim)*, Cambridge, UK, pp.415-419, 2011.

[11] A. Sachdev and M. Bhansali, Enhancing cloud computing security using AES algorithm, *International Journal of Computer Applications*, vol.6, no.9, pp.19-23, 2013.

[12] R. K. Yadava, B. K. Singh, S. K. Sinha and K. K. Pandey, A new approach of colour image encryption based on Henon like chaotic map, *International Conference on Recent Trends in Applied Sciences with Engineering Applications*, vol.3, no.6, 2013.

[13] S. Shrivastava, A novel 2D cat map based fast data encryption scheme, *International Journal of Electronics and Communication Engineering*, vol.4, no.2, pp.217-223, 2011.

[14] P. N. Khade and M. Narnaware, 3D chaotic functions for image encryption, *International Journal of Computer Science Issues (IJCSI)*, vol.9, no.3, pp.323-328, 2012.

[15] R. Enayatifar, A. H. Abdullah, I. F. Isnin, A. Altameem and M. Lee, Image encryption using a synchronous permutation-diffusion technique, *Optics and Lasers in Engineering*, pp.146-154, 2017.

[16] S. Kim and K. Umeno, Randomness evaluation and hardware implementation of nonadditive CA-based stream cipher, *National Institute of Information and Communications Technology*, Japan, 2004.

[17] M. M. Alani, Testing randomness in cipher text of block-ciphers using DIEHARD tests, *International Journal of Computer Science and Network Security (IJCSNS)*, vol.10, no.4, pp.53-57, 2010.

[18] A. Alabaichi, R. Mahmood, F. Ahmad and M. S. Mechee, Randomness analysis on blowfish block cipher using ECB and CBC modes, *Journal of Applied Sciences*, pp.768-789, 2013.

[19] B. F. Vajargah and R. Asghari, A novel pseudo-random number generator for cryptographic applications, *Indian Journal of Science and Technology*, vol.9, no.6, pp.1-5, 2016.

[20] A. E. D. Riad, H. K. Elminir, A. R. Shehata and T. R. Ibrahim, Security evaluation and encryption efficiency analysis of RC4 stream cipher for converged network applications, *Journal of Electrical Engineering*, vol.64, no.3, pp.196-200, 2013.

[21] J. Soto and L. Bassham, Randomness testing of the advanced encryption standard finalist candidates, *DTIC Document*, 2000.

[22] V. Katos, A randomness test for block ciphers, *Applied Mathematics and Computation*, vol.162, no.1, pp.29-35, 2005.

[23] F. Sulak, A. Doganakso, B. Ege and O. Koak, Evaluation of randomness test results for short sequences, *Proceedings in the Sequences and Their Applications*, Paris, France, pp.309-319, 2010.

[24] H. Isa and M. R. Z'aba, Randomness analysis on LED block ciphers, *Proc. of the 5th International Conference on Security of Information and Networks*, Jaipur, India, pp.60-66, 2012.

[25] A. H. M. Ragab, O. S. F. Allah, K. W. Magld and A. Y. Noaman, Security evaluation of robust chaotic block cipher, *International Journal of Soft Computing and Engineering (IJSCE)*, vol.3, no.6, pp.9-16, 2014.

[26] A. Alabaichi, R. Mahmood and F. Ahmad, Randomness analysis of 128 bits blowfish block cipher on ECB and CBC modes, *International Journal of Digital Content Technology and Its Applications*, vol.7, no.15, pp.77-89, 2013.