Develop AES Algorithm based on Fuzzy Set Theory

Ali H. kashmar[1], Ammar I. Shihab[2], and Zaineb L. Abood[3]

[1,2,3]University of Baghdad, College of Science, Baghdad, Iraq
Corresponding addresses
Kashmar992000@yahoo.dk, ammarste@gmail.com, zaineblatef@yahoo.com

***Abstract*:** Advance Encryption Standard AES cryptosystem is one of well-known block cipher that widely used to encrypt the sensitive data. However, attackers have pointed some drawbacks in the design of block ciphers, such as: (a) all block ciphers apply a same key for the encipherment of multiple blocks; (b) if adversary can discover the key for one block, he can immediately break the other blocks. Many security attacks have been applied on AES cipher including linear, differential, distinguishing, correlation and statistical attacks. The main objectives of this paper are; to develop a strong and high performance AES algorithm with the utilization of fuzzy function, to suggest three encryption approaches mixing AES with fuzzy function, and to analyze the security and evaluate the efficiency of developed algorithms. The result detects that the ciphertext acquired is the similar as the plaintext and fuzzy set theory was suitable for apply as round function in the design of other block ciphers. Moreover, the security properties, demonstrated that our designs were highly secure and robust against possible cryptographic attacks. Finally, the statistical test for randomness and comparison of the proposed ciphers with identical ciphers revealed that the proposed algorithms were efficient, and faster than the conventional block ciphers.

***Keywords*:** Cryptography, AES, Fuzzy set theory, Security attacks, Statistical tests**.**

1. Introduction

Designers and attackers are always encoded in a constant competition to build new attackable codes; therefore, when broken, the new encryption proposal becomes necessary. For efficient coding of data, symmetric algorithms are used, in particular to block zeros through encryption. The researchers have confirmed the problems of mass zeros. It is said that all longitudinal zeros, for example, suffer from some typical weaknesses: (a) all spectral codes use one key to encode multiple blocks; (b) if the opponent can detect the key for one block, it can easily break the other blocks; Means that the opponent is able to collect many blocks encoded by one key which makes possible more attacks against one block. Many security attacks have been applied on AES such as differential, linear, distinguishing, correlation and statistical attacks.

Block cipher based on fuzzy set theory has become a rich research area in the field of computer security and cryptography. In the following, some of the published works in this area are reviewed.Madanayake, 2012 [1]. Proposed an algorithm provides security levels by using various keys based on fuzzy logic for the encryption / decryption process. Dhenakaran, S.S and.Kavinilavu, N, 2012 [2] Introduced a new method using a mysterious set theory to integrate text encryption and convert unclassified text from numerical to native using fuzzy logic. Hinal, et al.in 2015 [3] presented a cross-sectional approach based on logic technique using the secret sharing program (2, 2). Azam, N. A. 2017 [4] A new image encryption technique is recommended based on several AES Gray S (RTSs) technologies translated to the right. Abdullah, K. 2017 [5] Proposed a new RSA encryption system based on the theory of fuzzy set where the ciphertext and the plaintext are in terms of Triangular Fuzzy Number (TFN). In order to bridge the gaps in AES algorithm, and because of need arises for guarantee the security of the block cipher cryptosystems while the communication must be ensured, it is a good idea to developed AES block cipher algorithm based on fuzzy set theory whereby the plaintext and the ciphertext are in terms of Triangular Fuzzy Number (TFN). The rest of the paper as in the following; in section 2, describe briefly AES algorithm, while some type of fuzzy set functions was discussion in section 3, in section 4, the suggested algorithms with some their properties was illustration, finally, results and discussion, conclusions and further works in sections 5, 6 and 7 respectively.

2. AES Algorithm

The National Institute of Standards and Technology (NIST) began the search for an alternative to the Data Encryption Standard (DES). In 2002 [6] 1997. the Advanced Encryption Standard (AES) is the new standard, as shown in Figure 1, developed by Joan Damen and Vincent Regman. It encrypts/decrypts data in 128-bit clusters using 128-bit (10-rounds), 192-bit (for 12 rounds) and 256-bit (14-round) key sizes; each round includes stages different processing consists of substitution, conversion, mixing of ordinary text of income, and conversion to the final output of encoded text. It is more secure than DES and 3DES, moreover, it is general design, flexible and available worldwide for free [6].

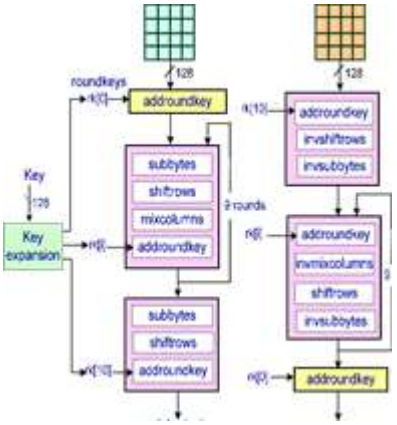

Figure 1. Shows AES algorithm [6].

All operations of AES is applied in GF(2^8) and the sixteen bytes of the 128-bit input block a0,…,a15 being arranged in a (4 × 4) matrix of bytes as shown in Figure 2.

a_0	a_4	a_8	a_{12}
a_1	a_5	a_9	a_{13}
a_2	a_6	a_{10}	a_{14}
a_3	a_7	a_{11}	a_{15}

Figure 2. Shows the (4 × 4) matrix of bytes for AES

Each round uses four actions, as shown in Figure 3, named "ShiftRows","SubBytes","MixColumns"and"AddRoundKey" . The last round has a slightly different shape and deletes the MixColumns process. The encryption begins with the AddRoundKey process, and then, the SubBytes process, at which point each byte is replaced by a byte of a reversible S-box. In the ShiftRows process, the rows (for bytes) are converted to a number of byte locations to the left; the first row is not shifted, the second row is shifted through one position, the third row to two, and the last row three. The last process is MixColumns. At this stage, the four bytes in each column are mixed by the quadrature of the four-byte vector by a constant, reversible, (4×4)-matrix over GF(2^8). The main characteristic is that if two types of input vectors are different in bytes s, the output variables differ in at least5 - s bytes, where 1 ≤ s ≤ 4. Each round closures with AddRoundKey, where 16 round-key bytes are xor'ed to the 16 information bytes. AES has generally straight forward key calendar of length16, 24, and 32 bytes, this key was expanded and returns of 16 × 11, 16 × 13, and 16 × 15 bytes respectively [7].

Decipherment applied the inverse process of encipherment, therefore, when we used the same key at encryption then the plaintext will be receives in decryption.

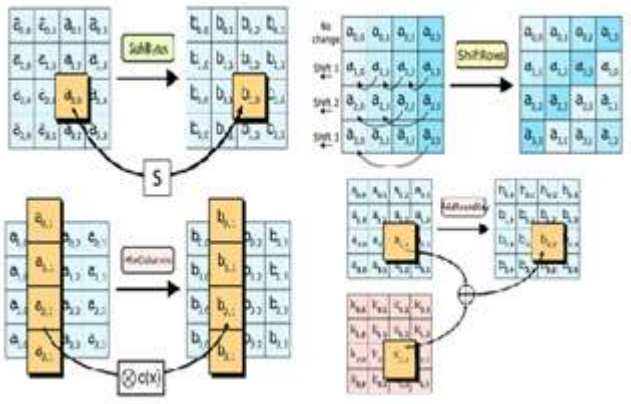

Figure 3. Shows the four transformations of AES algorithm

3. Fuzzy Sets and Fuzzy Membership Functions

Normally, an object has a numeric (degree of membership) between 0 and 1, 0 membership means the object is not in the set,1 membership means the object is fully inside the set and in between means the object is partially in the set. the description of this fact in mathematic can be represented as, If U is a collection of objects denoted generically by x, then a fuzzy set A in U is can be defined as a set of ordered pairs: $A = \{(x, \mu_A(x)) | x \in U\}$, where U : universe of discourse, and $\mu_A: U \rightarrow [0,1]$. Characteristic function μ, indicating the belongingness of x to the set A,

$$\mu_A(x) = \begin{cases} 1 \; if \; x \in A \\ 0 \; if \; x \notin A \end{cases}$$

called membership. The membership functions that characterize the blurry groups and the assemblies used are the basis of fuzzy sets and fuzzy logical systems [8].

Fuzzy logic (FL) is a control system (or logical) of the n-logic system that uses the "or fact" of the inputs and produces outputs based on the input states and the rate of change (instead of the normal "error or error" (1 or 0) , and the logic of low or high (binary) depends on the basis of the modern computer, it provides the basis for the approximate thinking using inaccurate decisions and allows the use of linguistic variables uses FL as a mathematical tool in areas such as job optimization, filtration and installation curves, etc. [9].

The Fuzzy Logic application itself to a special system is in fact not very different from applying logical logic or probability logic. The FL difference comes from its ability to create a more general theory of the decision-making process, called the foggy processor, a special case of approximate inference. The hazy wizard uses a blurry set and FL theory in the logical thinking process and acts as a vague logic algorithm. Ambiguous logic or is made through the mysterious words that we use so much in our daily lives. For example, expressions like a little [10].

Fuzzy membership functions can be seen as a bridge between uncertain data and a blurry world. Organic functions representing mysterious groups have different forms, which are determined by certain types of mathematical formulas. The most common types of functions include trigonometric, trapezoidal, triangular, bell, sinusoid, Gaussian, Cauchy and sigmoid. In order to make operations on cloud groups easier, membership functions are formulated according to their parameters, which include information about the ambiguity and scope of the site in the discourse world. Flexibility in parameter settings makes membership functions also adjustable. Because of the linearity of its structure, it is preferable to use organic functions of the triangular type over others [11].

Some properties of Triangular Membership Functions (TMF) are briefly examining in the following subsection.

3.1 Triangular Membership Function (TMF)

Triangular membership functions can made of lines, as

shown in Figure 4, and realized by the combination of line equations given in:

$$M_A(x) = \begin{cases} 0 & if\ x > x_1 \\ \frac{x-x_1}{x_2-x_1} & x_1 \le x \le x_2 \\ \frac{x_3-x}{x_3-x_2} & x_2 \le x \le x_3 \\ 0 & if\ x > x_3 \end{cases} \quad (1)$$

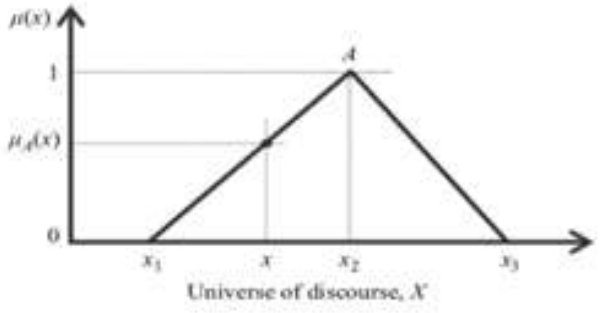

Figure 4. Shows Triangular fuzzy membership function

Where the parameters x1, x2 and x3 give the location of fuzzy membership function A in the X universe as shown in Figure 4. In fact, the parameters x1, x2, and x3 represent the function of membership A and show us its location in the opposite universe. It is sufficient to change parameter values in order to determine a new membership function of a similar format or to change the location of the speech. This is why the parameter formulas are important for representing membership functions. Relation (1) can be used as a parameterized membership function that represents ambiguous subsets of the triangular type. Equation (1) shows that x2 is a convergence point and equation (2):

$$M_A(x) = \left(\frac{x-x_1}{x_2-x_1}\right) < \left(\frac{x_3-x}{x_3-x_2}\right) \quad (2)$$

can be satisfied as long as x1 ≤ x2 and x ≤ x2.

$$M_A(x) = \left(\frac{x3-x}{x3-x2}\right) < \left(\frac{x-x1}{x2-x1}\right) \quad (3)$$

Similarly, equation (3) is satisfied as long as x ≥x2 and x2 ≤ x3. In other words, the output is equal to the smaller part of (2) or (3). However, these equations give a negative output if x < x1 or x > x3. Since the membership scores are set at a time interval [0,1], negative outputs must be changed to 0. Therefore, the maximum value must be set between 0 and output from (2) or (3). Accordingly, (1) can be converted to the figure in (4):

$$M_A(x) = max\left(min\left(\frac{x-x1}{x2-x1}, \frac{x3-x}{x3-x2}\right)\right) \quad (4)$$

Triangular fuzzy subsets are simple to model and very easy to simulate. The sharp peak can them to react to any changes even if they are very small. Thus, sharp peak produces triangle membership functions critical to the changes in the fragile variable x [12].

4. Fuzzy-AES algorithms

This section provided the mathematical basis of proposed algorithms, some of the planners used to structure modern restore block ciphers and modes of procedure. Further, it represents the design of a new efficient and secure block cipher called Fuzzy-AES algorithm. Two major parts are producing by the proposed algorithms: Fuzz set theory and AES algorithm, which is used to implement the encipherment and decipherment processes. From this situation, the name comes Fuzzy-AES. At the beginning of this section, a focus on investigating the structure of Fuzzy-AES algorithms, types of Fuzzy-AES algorithms with encryption/decryption processes. Finally, the significant properties and some advantages to justify the correctness of the proposed algorithms are discussing. The methodology for Fuzzy-AES is demonstrated in Figure 5.

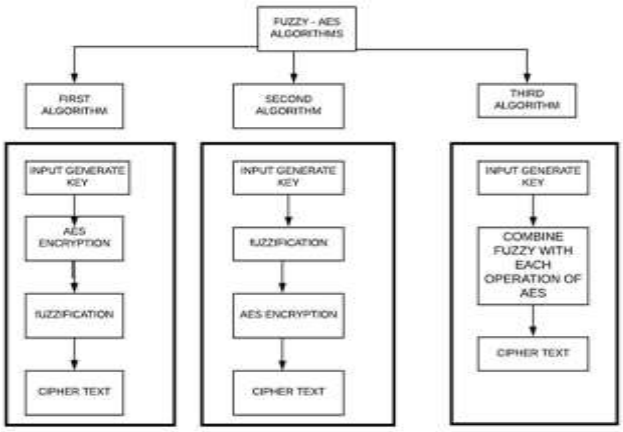

Figure 5. Block diagram of Fuzzy-AES algorithms

As illustration in Figure 5, Fuzzy-AES algorithm consists of the following parts:

a) First Algorithm: start with AES algorithm then used Fuzzy function.
b) Second Algorithm: start with Fuzzy function then used AES algorithm.
c) Third Algorithm: combine between Fuzzy function with each operations of AES algorithm.

The inputs of these algorithms are:

1. The key (K): it is the master keystream of the Fuzzy-AES algorithms, which generated from pseudorandom Number Generator PRNG, applying Cipher Block Chaining CBC mode of operation. It consists of 16-bytes $(k_0, k_1, k_2, \ldots, k_{15})$, that is input into Fuzzy-AES algorithms to generate the new ciphertext for each round.
2. The plaintext $P1, P2, P3, P4, \ldots$: it is the message required to encode. The plaintext P is comprised by

16-bytes $(p_0, p_1, \dots, p_{15})$.

While the output of these algorithms is the Ciphertext (C_i), which was the final output of algorithm, where the ciphertext consists of $C1, C2, C3, C4, \dots$ with each C comprised of 16-bytes $(c_0, c_1, \dots, c_{15})$ for each round, it is returning to PRNG for generated a new keystream.

The following subsections deal with various algorithms with theirs properties.

4.1 First algorithm

In this algorithm, first applied the same procedure operations of AES algorithm to the input data, then make fuzzicaition for the output data by employing a Triangular Fuzzy Membership (TFM) map to produce the ciphertext of this algorithm, as shown in Figure 6.

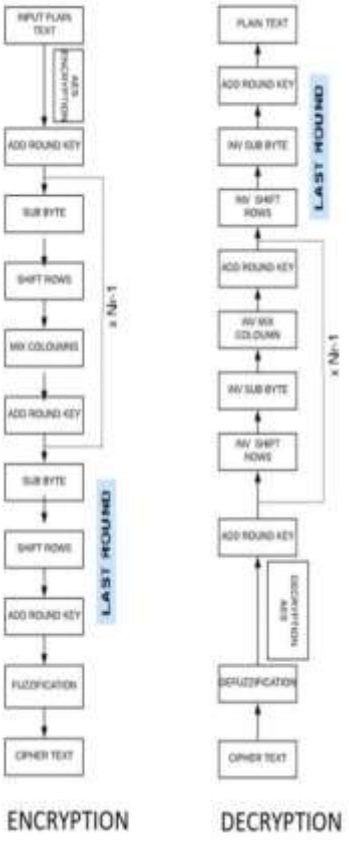

Figure 6. Encryption/Decryption process of 1st algorithm

4.2 Second algorithm

The second algorithm begin with fuzzication the input by applying a triangular fuzzy membership map, then applied the same procedure operation of AES algorithm for the output to produce the ciphertext of this algorithm as shown in the Figure 7.

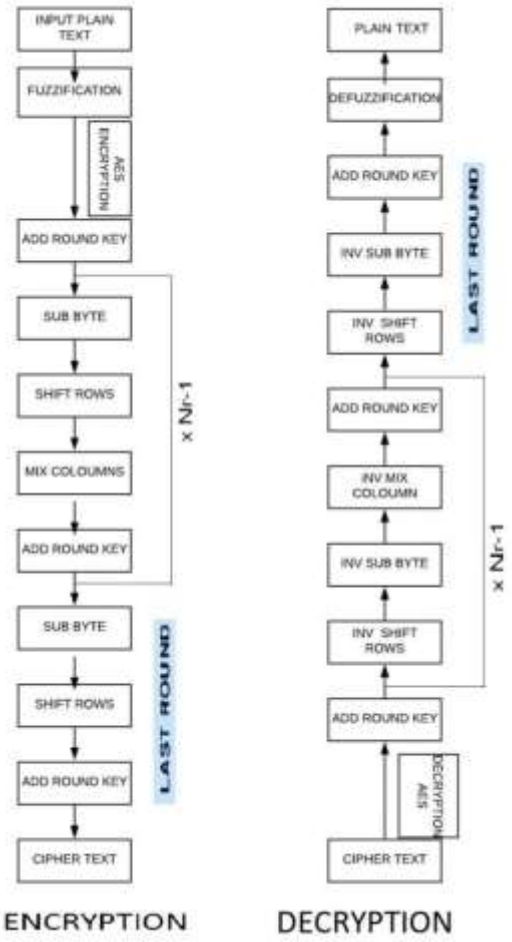

Figure7. Encryption/Decryption process of 2nd algorithm

4.3 Third algorithm

In the third algorithm, start with AES algorithm that has four stages, namely AddRound key, SubByte, ShiftRow and MixColumn, and for each round, applied these operations as the following steps:

a) Applied AddRound key stage, which represented the first operation of AES to the input, then make fuzzicition to the output of this stage by using a triangular fuzzy membership map, as describe in subsection 3.1.
b) Next, the result input to SubByet stage, which represented the second operation of AES, then make fuzzicition to the output of this stage by using TFM.
c) After that, the result input to the ShifRow stage, which represented the third stage of AES, then make fuzzicition to the output of this stage by using TFM.
d) Finally, the result input to MixColumn stage, which represented the final stage of AES, then make fuzzicition to the output of this stage by using TFM.
e) The final output represented the ciphertext of this algorithm as shown in Figure 8.

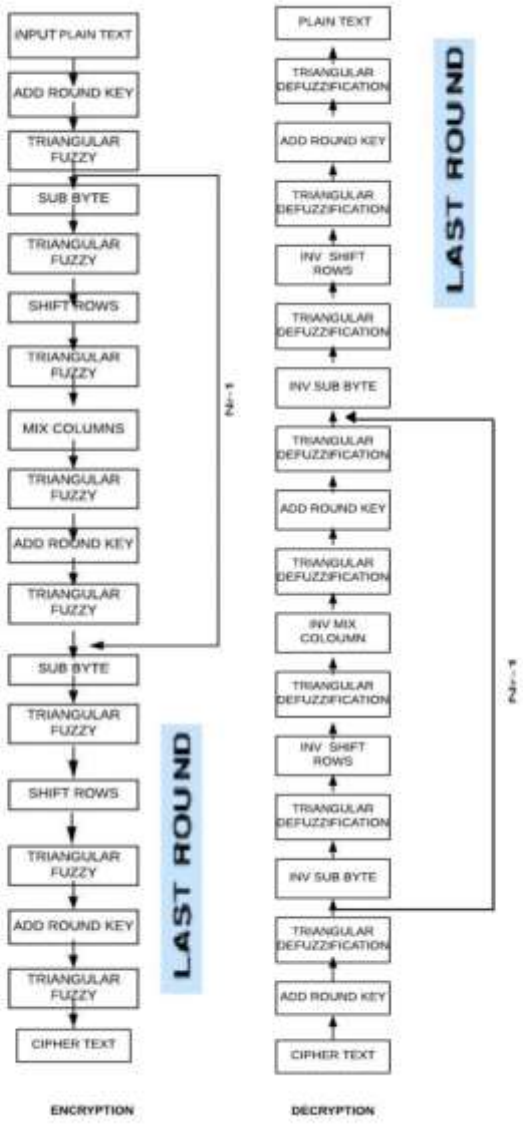

Figure7. Encryption/Decryption process of 3rd algorithm

4.4 Properties of Fuzzy-AES algorithms

1. Fuzzy-AES algorithm was characterized by its ability to produce greater security with proper implementation and by generating new functions between the cluster cryptography round and the fuzzy set theory.
2. In these new designs, a fuzzy set theory was proposed to produce an effective and long cyst. Some randomized sequences, which cannot be distinguished from truly random sequences, can be used for cryptographic system applications. These semi-random sequences use a larger number of alphabets for these purposes to increase the number of possibilities.
3. The main purpose of designing Fuzzy-AES algorithms is to use appropriate and effective PRNG along with the appropriate uniform.
4. Thus, we can realize that Fuzzy-AES algorithms, as more efficient and powerful algorithms, have an additional positive effect on plaintext and keystream. They have the ability to generate a kind of balance in their structure.
5. Moreover, they can produce a real encoder resulting from the plain text mixture and the keystream. As a result, fuzzy set theory PRNG is deploying by the Fuzzy-AES to generate the keystream, which is feature by high-level security and performance.
6. Occasionally, a triangular fuzzy membership map as a function with special properties, working on the two inputs (i.e., plaintext and keystream), has the ability to return a copy of the encrypted text to PRNG, which generates the next keystream.
7. As a result, the PRNG-encoded comment process results in a greater advantage for Fuzzy-AES than the three-pointed post function.
8. There is a similarity in design between the proposed algorithms and other ciphers. Fuzzy-AES is a self-synchronous block encoding where encrypted text has an effect on the image key. It has a high level of safety.
9. Intentional fuzzy-AES algorithms are intending for use with 16-byte keystream. This Keystream is using in PRNG to produce a new cyst of up to 64 bytes. In each round of AES-Fuzzy algorithms, PRNG generates a 16-byte keystream by combining, using Nonlinear Invertible Round Function (NLIRF), with 16-byte plaintext to generate 16-byte encrypted text.

5. Results and discussions

This section addresses the major issues regarding Fuzzy-AES algorithms; it examines the performance of these algorithms along with possible security attacks and administers the binary digits randomness tests of the ciphertext bits for these algorithms. A brief survey of the security analysis for Fuzzy-AES algorithms is providing in the following subsections.

5.1 Possible Attacks against Fuzzy-AES algorithms

a) Brute-force Attack: In this type of attack, the adversary try all possibilities**.**Since Fuzzy-AES algorithms applied 128-bit as a keystream, therefore the attacker needs 2^{128} possible keys, which approximately equal 3.4×10^{38} keys, this mean that the time required at one encryption per μs was approximately equal to $2^{127} = 1.7 \times 10^{38}$ years in order to apply a brute force attack against Fuzzy-AES algorithms [13]. Hence, an exhaustive key search attack took a long time and it appears infeasible.

b) Ciphertext Only Attack: The adversary has only a number of ciphertext messages and tries to discovery any relationships between the ciphertext and the data that expose the cipher system till the ciphertext message is solved. In Fuzzy-AES algorithms, the plaintext data that input to fuzzy set theory is randomized and Perform with a keystream sequence through an exclusive or operation. Then, the result data can be changed through many conversion stages of the round function that include the byte and transformation rows Mixcolumn and AddRound Key. As a result, the statistical properties of the plain text message will be removed and the resulting encrypted text message will result in near-

randomization. Thus, the attack appears to be encrypted text is not possible.

c) Known Plaintext Attack: The adversary in this type of attack need the plaintext corresponding the ciphertext.The plaintext bytes in Fuzzy-AES algorithms are XOR'ed with the keystream bytes, the resulting bytes are substitute by employing AES transformation and fuzzy function. The secret key that used to update AES transformation and fuzzy function make the opponent unable to determine the plaintext byte. Therefore, it was difficult to applied known plaintext attack.

d) Statistical Attack: tests of statistical are been performed on Fuzzy-AES algorithms, e.g. Frequency test, Serial test, Poker test, Runs test and Auto-correlation test [14]. In the current AES-Fuzzy algorithms, keystream and ciphertext have been adopted on the mysterious group theory functions and the AES algorithm to produce effective cryptographic text. As a result, to ensure that the new encrypted text remains strong, the bits of encoded text in the proposed algorithms have been tested extensively with the application of statistical tests of different lengths. The resulting encoded output passed all statistical tests, including randomized, binary numbers (see Tables 1, 2, 3, and 4) that justified the generation of encrypted text.

e) Differential Analysis Attack: Differential Analysis Attack is a generic term for all kind of cryptanalysis which investigates how differences in the information input can result in differences in the output**.** This attack seems undetectable to apply on Fuzzy-AES algorithms since the S-box is update by secret key for each round. Accordingly, the opponent does not have any information about the arrangement of S-box.

f) **Distinguishing and Correlation Attacks:** Two sets of attacks (i.e. differential and correlational) which closely resemble each other are discussing in this part. Any type of cryptanalysis which is applied in order to distinguish the encoded data from random data is called by the generic term distinguishing analysis or attack. Correlation analysis refers to a class of known plaintext attacks, employing Boolean function. A weakness in the choice of Fuzzy-AES algorithm Make encryption functionality susceptible to link analysis. It is recommended to choose a logical function that cannot be exploited by correlation analysis. In general, designers should exercise caution when applying zeros using the logical function.

5.2 Basic Five Binary Digits Statistical Tests

Random property and ciphertext bits are analyzed by applying the five statistical tests named Frequency test, Serial test, Poker test, Runs test and Auto-correlation test [15]. The frequency test is for uniformity and the other tests are for independence. These tests are a fundamental package that is usually applying for block cipher, stream cipher and keystream generation [16]. The resulting values of each test were comparing with the corresponding value of Chi square distribution. The keystream and ciphertext generated in the proposed Fuzzy-AES algorithms for different key length sizes are successfully passed all these tests for every run. A summary of the results are giving in Tables 1, 2, 3 and 4.

Table 1. Statistical tests for the master keystream of the Fuzzy-AES algorithms

Tests	*1st alg =128bit*	*2nd alg =128bit*	*3rd alg =128bit*	*Pass value*	*Result*
Frequency	0.654	2.793	0.0312	≤ 3.841	Pass
Serial test	-26.088	-31.599	0.0118	≤ 5.991	Pass
Poker test	-32.000	-8.000	6.761	≤ 14.067	Pass
Run test	3.559	3.873	1.882	≤ 22.362	Pass
Auto correlation					
Shift 1	-28.751	-3.882	0.266	≤ 1.960	Pass
Shift 2	-12.644	-14.462	0.178		Pass
Shift 3	-18.814	-9.458	-1.162		Pass
Shift 4	-19.894	-1.232	1.616		Pass
Shift 5	-18.064	-3.639	-0.631		Pass
Shift 6	-14.910	-12.631	-0.543		Pass
Shift 7	-17.667	-1.044	0.272		Pass
Shift 8	0.602	-5.595	-1.278		Pass
Shift 9	-8.294	-6.411	-1.191		Pass
Shift 10	-21.865	-1.5807	1.104		pass

Table 2. Statistical tests for ciphertext of **1st** algorithm with different key lengths

Tests	*Key length =128bit*	*Key length =512bit*	*Key length =1024 bit*	*Pass value*	*Result*
Frequency	1.3333	0.363	0.568	≤ 3.841	Pass
Serial test	4.1273	2.531	4.272	≤ 5.991	Pass
Poker test	-16.000	-4.000	-64.000	≤ 14.067	Pass
Run test	1.1990	1.022	1.402	≤ 22.362	Pass
Auto correlation				≤ 1.960	
Shift 1	-0.619	-2.110	-16.879		Pass
Shift 2	-7.818	-20.009	-9.961		Pass
Shift 3	-6.469	-0.311	-11.094		Pass
Shift 4	-7.964	-18.819	-3.934		Pass
Shift 5	0.583	-0.230	-9.016		Pass
Shift 6	-1.368	-16.111	-17.368		Pass
Shift 7	-0.739	-3.818	-11.918		Pass
Shift 8	-4.231	-14.677	-0.454		Pass
Shift 9	-8.485	-12.274	-14.454		Pass
Shift 10	-9.200	-11.018	-3.689		Pass

Table 3. Statistical tests for ciphertext of **2nd** algorithm with different key lengths

Tests	*Key length =128bit*	*Key Length =512 bit*	*Key length =1024 bit*	*Pass value*	*Result*
Frequency	0.278	0.187	0.000	≤ 3.841	Pass
Serial test	3.424	2.969	1.900	≤ 5.991	Pass
Poker test	-2.000	-4.000	-16.000	≤ 14.067	Pass
Run test	1.287	1.235	1.020	≤ 22.362	Pass
Auto correlation					
Shift 1	-13.947	-6.585	-6.092	≤ 1.960	Pass
Shift 2	-3.863	-5.810	-1.772		Pass
Shift 3	1.734	-0.309	-7.363		Pass
Shift 4	-3.863	-4.193	-0.889		Pass
Shift 5	-15.758	-8.547	0.000		Pass
Shift 6	-7.191	-9.293	-1.285		Pass
Shift 7	-4.483	-8.040	0.315		Pass
Shift 8	-4.134	-4.209	-4.055		Pass
Shift 9	-2.629	-1.728	-4.647		Pass
Shift 10	-5.973	-2.611	-2.607		Pass

Table 4. Statistical tests for ciphertext of 3rd algorithm with different key lengths

Tests	*Key length =128bit*	*Key Length =512 bit*	*Key length =1024 bit*	*Pass value*	*Result*
Frequency	1.531	2.000	3.781	≤ 3.841	Pass
Serial test	1.767	2.244	4.809	≤ 5.991	Pass
Poker test	-2.000	-4.000	-15.500	≤ 14.067	Pass
Run test	0.602	-0.253	0.887	≤ 22.362	Pass
Auto correlation				≤ 1.960	
Shift 1	-1.400	-3.400	-1.069		Pass
Shift 2	-2.155	-1.708	-6.075		Pass
Shift 3	-1.448	-0.545	-7.379		Pass
Shift 4	-1.454	-2.412	-5.488		Pass
Shift 5	-4.989	-2.233	-6.974		Pass
Shift 6	-3.713	-4.314	-2.435		Pass
Shift 7	-2.008	-6.708	-0.736		Pass
Shift 8	-5.031	-0.360	-4.800		Pass
Shift 9	-6.037	-4.663	-2.967		Pass
Shift 10	0.381	-7.293	-4.800		Pass

Moreover, the statistical tests compression for 1st , 2nd and 3rd algorithms for different key length sizes are successfully passed all five statistical tests for every run. A summary of the results is presenting in Tables 5, 6 and 7.

Table 5. Statistical tests compression of 1st , 2nd and 3rd algorithms for key length 128-bit

Tests	*1st alg =128bit*	*2nd alg =128bit*	*3rd alg =128bit*	*Pass value*	*Result*
Frequency	1.333	2.793	2.531	≤ 3.841	Pass
Serial test	4.127	-31.599	3.224	≤ 5.991	Pass
Poker test	-16.000	-8.000	-42.000	≤ 14.067	Pass
Run test	1.199	3.873	0.033	≤ 22.362	Pass
Auto correlation				≤ 1.960	
Shift 1	-0.619	-3.882	-1.546		Pass
Shift 2	-7.818	-14.462	-5.031		Pass
Shift 3	-6.469	-9.458	-4.451		Pass
Shift 4	-7.964	-1.232	-3.863		Pass
Shift 5	0.583	-3.639	0.000		Pass
Shift 6	-1.368	-12.631	-.122		Pass
Shift 7	-0.739	-1.044	-7.672		Pass
Shift 8	-4.231	-5.595	-6.841		Pass
Shift 9	-8.485	-6.411	-1.100		Pass
Shift 10	-9.200	-1.5807	-2.525		pass

Table 6. Statistical tests compression of 1st , 2nd and 3rd algorithms for key length 512-bits

Tests	*1st alg =512bit*	*2nd alg =512bit*	*3rd alg =512bit*	*Pass value*	*Result*
Frequency	0.363	2.793	0.187	≤ 3.841	Pass
Serial test	2.531	-31.599	2.969	≤ 5.991	Pass
Poker test	-4.000	-8.000	-4.000	≤ 14.067	Pass
Run test	1.022	3.873	1.235	≤ 22.362	Pass
Auto correlation				≤ 1.960	
Shift 1	-2.110	-3.882	-6.585		Pass
Shift 2	-20.009	-14.462	-5.810		Pass
Shift 3	-0.311	-9.458	-0.309		Pass
Shift 4	-18.819	-1.232	-4.193		Pass
Shift 5	-0.230	-3.639	-8.547		Pass
Shift 6	-16.111	-12.631	-9.293		Pass
Shift 7	-3.818	-1.044	-8.040		Pass
Shift 8	-14.677	-5.595	-4.209		Pass
Shift 9	-12.274	-6.411	-1.728		Pass
Shift 10	-11.018	-1.5807	-2.611		pass

Table 7. Statistical tests compression of **1st , 2nd** and **3rd** algorithms for key length 1024-bits

Tests	*1st alg =1024bit*	*2nd alg =1024*	*3rd alg =1024*	*Pass value*	*Result*
Frequency	0.568	0.000	3.781	≤ 3.841	Pass
Serial test	4.272	1.900	4.809	≤ 5.991	Pass
Poker test	-64.000	-16.000	-15.500	≤ 14.067	Pass
Run test	1.402	1.020	0.887	≤ 22.362	Pass
Auto correlation				≤ 1.960	
Shift 1	-16.879	-6.092	-1.069		Pass
Shift 2	-9.961	-1.772	-6.075		Pass
Shift 3	-11.094	-7.363	-7.379		Pass
Shift 4	-3.934	-0.889	-5.489		Pass
Shift 5	-9.016	0.000	-6.974		Pass
Shift 6	-17.368	-1.285	-2.435		Pass
Shift 7	-11.918	0.315	-0.736		Pass
Shift 8	-0.454	-4.055	-4.800		Pass
Shift 9	-14.454	-4.647	-2.967		Pass
Shift 10	-3.689	-2.607	-4.880		pass

Finally, the comparison for 1st, 2nd and,3rd algorithms with identical cipher algorithms such as AES, DES and 3DES has been done . A summary of the results is available in Table 8.

Table 8. Compression between **1st , 2nd** and **3rd** algorithms and Identical Algorithms [17]

Algorithms	*Key Length*	*No.of Round*	*Block Size*	*Cryptanalysis Resistance*	*Security Level*	*Possible Keys*	*Time Required*
DES	**65 bits**	**16**	**64 bits**	**Vulnerable to Differential & linear attacks**	**Proven inadequate**	2^{35}	**For 56 bits key =400 days**
3DES	**K1 , k2, k3=168 bits**	**48**	**64 bits**	**Vulnerable to Brute Force, plain text & differential attacks**	**One only weak which is exit in DES**	2^{112} 2^{168}	**For 112 bits =800 days**
AES	**128 192 256**	**10 12 14**	**128 192 256**	**Absolut Strong against Differential, Linear , interpolation & square attack**	**Considered secure**	2^{128} 2^{192} 2^{256}	**For 128 bit key =5*10^21 years**
1st alg.	**128**	**10**	**128**	**Strong against Differential , linear , statistical attack**	**Considered secure**	2^{128}	**For 128 bit key =5*10^21 years**
2st alg.	**128**	**10**	**128**	**Strong against Differential , linear , statistical attack**	**Considered secure**	2^{128}	**For 128 bit key =5*10^21 years**
3st alg.	**128**	**10**	**128**	**Strong against Differential , linear , statistical attack**	**Considered secure**	2^{128}	**For 128 bit key =5*10^21 years**

6. Conclusions

The current paper attempt to discuss the possibilities of developing a new block cipher algorithms of more efficiency (pass the statistical tests for randomness) and security (resists against security attacks) than other block ciphers. In this paper, the mechanism used to develop the weak classical concept of the AES algorithm worked to form a stronger and more suitable coding. A little later, this paper attempted to introduce new block encryption algorithms called Fuzzy-AES. Thorough tests have been done by describing these algorithms, evaluating their performance and security properties, and examining their implementation aspects. The analysis of the devised algorithms demonstrated that the proposed algorithms are characterized by flexibility; speed; sufficient; and highly secured than similar block ciphers such as DES, 3DES and AES. In the future, NIST tests can be used to show a promising building block for cryptographic systems with certain advantages over ambiguous set theorems and fuzzy logic. With a new blur mechanism by applying an additional type of organic functions such as Gaussian, Cauchy and Bell

References

[1] R. Madanayake, N. Peiris, G. Ranaweera, and U. Jayathilake, Advanced Encryption Algorithm Using Fuzzy Logic, *International Conference on Information and Computer Networks* (ICICN 2012) IPCSIT. vol. 27 ,2012

[2] . S.S. Dhenakaran, and. N. Kavinilavu,. "A New Method For Encryption Using Fuzzy Set Theory," *International Journal of Engineering Trends and Technology*, vol. 3, no.3- pp,320-326. 2012

[3] M. Hinal,.Mudia and V. Pallavi,.Chavan.. Fuzzy logic based image encryption for confidential data transfer using (2, 2) secret sharing scheme-review, *1st International Conference on Information Security & Privacy (ICISP)*, 11-12 December 2015, Nagpur, India, Procedia Computer Science 78, pp:,632 – 639.

[4] N. A. Azam,. ."A Novel Fuzzy Encryption Technique Based on Multiple Right Translated AES Gray S-Boxes and Phase Embedding," *Security and Communication Networks* vol. 2017, Article ID 5790189. 2017.

[5] . K. Abdullah, S.Abu Bakar,N.H, Kamis, and H. Aliamis,. RSA Cryptosystem with Fuzzy Set Theory for Encryption and Decryption, *AIP Conference Proceedings 1905, (2017) Proc. 13th Imt-Gt International Conf. on Mathematics, Statistics and Their Applications (ICMSA)*.2017,pp. 4–7 December 2017, Kedah, Malaysia.

[6] J. Daemen, and V. Rijmen. "The Design of Rijndael: AES the Advanced Encryption Standard,." *Berlin: Springer*, .2002.

[7] H. Dobbertin., V. Rijmen, and A. Sowa. "AES". *4th International Conference, AES 2004*, Bonn, Germany, May 10-12, 2004.

[8] Ying Bai, Hanqi Zhuang and Zvi. S Roth, "Fuzzy Logic Control to Suppress Noises and Coupling Effects in a Laser Tracking System," *IEEE Trans on*

Control Systems Technology, Vol.13, No.1, January 2005, pp.113-121

[9] H.-J. Zimmermann. "Fuzzy Set Theory-and Its Applications," *Fourth Edition, Springer Science and Business Media, LLC*, Library of Congress Cataloging-in-Publication Data.2001.

[10] J. M. Mendel and R. I. John. "Type-2 Fuzzy Sets Made Simple," *IEEE Transactions on Fuzzy Systems*, vol. 10, no. 2, April 2002, pp. 117- 127.

[11] H. İsmail . Altas . "Fuzzy Logic Control in Energy Systems: with Design Applications in Matlab/Simulink, *handbook, IET Digital Library*.2017.

[12] K. M. Passino, S. Yurkovich, Fuzzy Control, *Addison Wesley*, 1998.

[13] W. Stallings, Cryptography and Network Security: Principal and Practice. *New Jersey: Prentice-Hall*.2003.

[14] A. J. Menezes,,P. van Oorschot , and S. Vanstone. *Handbook of Applied Cryptography. Florida*: CRC Press. 2006.

[15] H. Beker, and F. Piper. Cipher System: The Protection of Communication. London: *Northwood*.1982.

[16] CRYPT-X'98.. A graphical Package for the Statistical Testing of Stream Cipher, block Cipher and key generators. *Queensland University of Technology (QUT)*, Australia. 1999

[17] Noura Aleisa. A Comparison of the 3DES and AES Encryption Standards. *International Journal of Security and Its Applications*, Vol.9, No.7, pp.241-246. 2015.