Al-Qadisiyah Journal of Pure Science

Volume 25 | Number 1 Article 15

1-7-2020

A MODIFIED ON TWOFISH ALGORITHM BASED ON CYCLIC GROUP AND IRREDUCIBLE POLYNOMIAL IN GF (28)

Suhad Muhajer Kareem
Collage of Computer science andinformation technology, University of Basrah, Basrah, Iraq

Dr. Abdul Monem S. Rahma
Department of Computer science, University of Technology, Baghdad, Iraq

Recommended Citation

Kareem, Suhad Muhajer and Rahma, Dr. Abdul Monem S. (2020) "A MODIFIED ON TWOFISH ALGORITHM BASED ON CYCLIC GROUP AND IRREDUCIBLE POLYNOMIAL IN GF (28)," *Al-Qadisiyah Journal of Pure Science*: Vol. 25: No. 1, Article 15.
DOI: 10.29350/2411-3514.1220
Available at: https://qjps.researchcommons.org/home/vol25/iss1/15

Available online at http://qu.edu.iq/journalsc/index.php/JOPS

Al-Qadisiyah Journal Of Pure Science (QJPS)

Vol. 25, No. 1, pp Comp. 1 –9, Year2020

ISSN 2411-3514 ONLINE

ISSN 1997-2490PRINTED

Received : 23/12/2019 Accepted :12/2/2020

A MODIFIED ON TWOFISH ALGORITHM BASED ON CYCLIC GROUP AND IRREDUCIBLE POLYNOMIAL IN GF (2^8)

Suhad Muhajer Kareem[1] and Dr. Abdul Monem S. Rahma[2]

Collage of Computer science and information technology, University of Basrah, Basrah, Iraq[1]

Department of Computer science, University of Technology, Baghdad, Iraq[2]

ABSTRACT

In this article, a new adjustment is made on Twofish algorithm based on using a new operation called cyclic group extended # (CGE#) operation for increasing the randomness of algorithm. This is a new operation works on 8-bits and using 30 tables constructed with cyclic group and multiplication in Galois Field (GF) (2^8). A new (CGE#) operation is used instead of (XOR) operation in each round of Feistel of Twofish. This is done by using dual keys: one key is used for selecting one table among 30 tables, and the other key is used for: encryption and decryption. The proposed algorithms are evaluated by using many security metrics such as complexity, NIST, histogram and correlation coefficients. The modification has given good results in these metrics, and this leads to make the proposed algorithm much more robust against many the attacks.

KEYWORDS: Cryptography, Symmetric Block Cipher, Twofish, Histogram, NIST, Correlation Coefficients.

1. Introduction

Rapid development in information technology has led to a reliance on the transmission of electronic information via networks. As it is necessary to provide secure information environments, many researchers address this security challenge [1, 2]. One method for protecting information is the use of encryption algorithms between two parties involved in communication by converting the message into a human-unrecognisable form [3]. Algorithmic encryption is classified into symmetric-key and asymmetric-key encryption. Symmetric-key encryption uses the same key to implement encryption and decryption, while asymmetric-key encryption incorporates different public and private keys. Symmetric algorithms include block and stream cyphers [4, 5], and Twofish is an example of a symmetric block encryption.

The strength of the symmetric algorithms truly depends on how the key is securely exchanged between the sender and receiver [6].

Generality modern encryption algorithms rely on functions with two states (0, 1) for encryption and decryption. Twofish, as cryptographic algorithm, use the logical operation XOR that relies on two binary states (0, 1). This approach includes several weaknesses, such as being easy to estimate the key and break the security algorithm. Previous research replaces these two states with four states (0, 1, 2, 3) for increasing the key space, as described in Figure (2) (adopted from [7]) in Section 3. We concentrate on the low points of XOR by exchanging it with a new (CGE#) operation that operates on block with 8-bits sizes with different state tables based on cyclic group and irreducible polynomial in GF (2^8). The total new (CGE#) operation is achieved by using an extra two keys. In this article, modifying Feistel in Twofish by using a new (CGE#) operation in both encryption and decryption process to increase the security level of algorithm. This paper is organized as: section 2 gives a short overview of both Twofish, section 3 introduces some of related works, while section 4 explains the basic mathematical biases used in this work. Construction of proposed tables and proposed method are overviewed in section 5 and 6 respectively. Finally, section 7 and 8 give the evaluation metrics of proposed algorithm and a number of conclusions for the work.

2. A short overview of Twofish algorithm

Twofish is one of a symmetric key block cipher with a block size of 128-bits and key sizes up to 256-bits and it is based on Feistel network. Initially, the Twofish separates (128 bit) plain text into four block words of 32 (W_0, W_1, W_2, and W_3), after that each word is jointed using XOR operation with 4-words of 32-bits (K_0, K_1, K_2, and K_3) in the input whitening process. The results of whitening to be passed into the F-function and units. Twofish has a function called the directive function (F), which consists of five components of operations that are composed of 4-dependent keys using: Substitution boxes, maximum distance separable (MDS) matrix, the pseudo Hadamard and addition mod of 2^{32}. After 16- rounds, Twofish also implements output whitening as shown in Figure 1[8, 9].

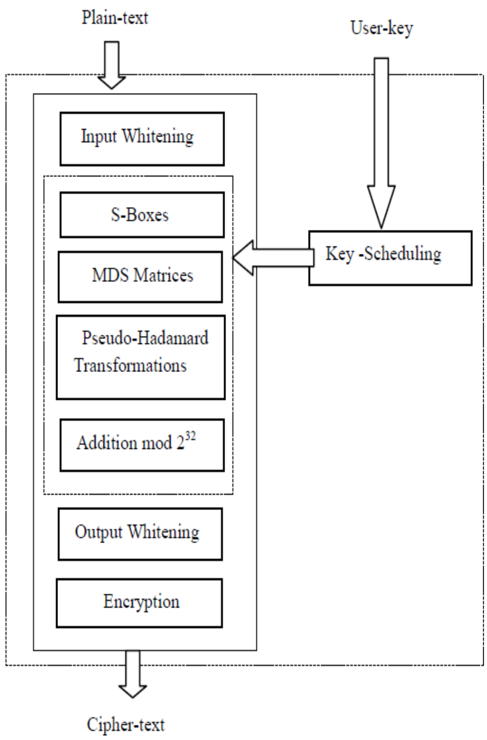


Figure (1) steps for Twofish algorithm [10].

3. Related works

This section overviews the related literature on Feistel of block encryption algorithm and using state tables in key distribution. In 2009 [7], the research has presented the work by combining the curve security methods with quantum encryption notations to raise the security and key space in order to make encryption operation more secure and robust. In this work, the proposed modification focuses on the use of four different states (0, 1, 2 and 3) instead of (0, 1). This is to make changing in the polarized angles which have been used in quantum description encoded in these four tables, in addition to the output descriptions which have used polarized states angles according to the 4-tables. Then doctrinaire ciphers transform plaintext into cipher text by changing the current state pattern of each character by using a logical operator (#) as shown in Figure (2):

#0	0	1	2	3
0	3	2	1	0
1	2	3	0	1
2	1	0	3	2
3	0	1	2	3

#1	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

#2	0	1	2	3
0	2	3	0	1
1	3	2	1	0
2	0	1	2	3
3	1	0	3	2

#3	0	1	2	3
0	1	0	3	2
1	0	1	2	3
2	3	2	1	0
3	2	3	0	1

Figure (2) the 4-states tables for the (#) operation.

The work of (#) operation includes 3-inputs: the first input refers to the state table number which should be used to compute the output among the 4-tables.

The other two inputs determine the row and column number in the given table to give their result as the cross point.

In 2010, [11] the researchers have introduced a proposal for a new method to improve the performance of the DES algorithm. This improvement is demonstrated by replacing the predefined XOR operation applied during the 16 rounds in the standard algorithm Feistel with a new # operation depends on using two keys. Each key consists of a combination of 4-states (0, 1, 2, 3) instead of the ordinary 2-state keys (0, 1) using various state table suggested in [7] Figure (2). In 2019 [12], this work has presented a new method for the modifying DES algorithm called MODDES. This is done by replacing ordinary XOR operation with a new operation based on multiplication in a GF (2^8) based on irreducible polynomials. This is handled using four keys in each round. Two keys are derived from the main key and the other two keys are generated internally. The new algorithm operates on bit instead of byte. Evaluate the proposed algorithm that has shown the increased security level and made it resistant against attacks. In this study, 30 tables are constructed based on cyclic group and irreducible polynomials in GF (2^8), then these tables have been applied on each round of Feistel network of Twofish as shown in the next sections.

4. Mathematical bias in cryptography

4.1 Irreducible Polynomial Over Finite Fields

In mathematical terms, a field with finite elements called finite field and also called Galois Field (GF) that operates with polynomials. Then this mathematical term was used in many encryption algorithms such as El Gamal, Diffie, and Hellman in 1976 and AES in 1986 [13]. The arrangement of the finite field must be a power of a prime P^n, where p is a prime number and n is a positive integer, and all the operations such as addition, abstraction and multiplication should be performed and give the result in element into that field [14].There are two types of finite fields: the prime field F (p) and the binary field F (2^n). In binary field, let f(x) a polynomial in GF (2^n) can be represented as following equation (1):

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + a_1 x + a_0 = \sum_{i=0}^{n} a_i x^i \qquad (1)$$

The addition and subtraction which are applied using XOR operation, while the multiplication in GF (2^n) is more difficult than addition and subtraction. The multiplication in GF (2^n) is by multiplying two polynomials for the two elements concerned and reducing the results using irreducible polynomial m(x) of grade n if the multiplication result in a polynomial is a grade greater than n-1, which is, the polynomial is divided by m(x) and the remainder is kept. Every field GF (2^n) needs an irreducible polynomial $P(x)$ of degree n with coefficients from GF (2) [12], for example, GF (2^2), GF (2^3) and GF (2^8) have one, two and thirteen irreducible polynomials respectively. In this paper, the GF (2^8) was addressed in encryption algorithm. Table (1) below shows irreducible Polynomials in GF (2^8).

Table 1: Irreducible Polynomials for GF (2^8).

No.	*Irreducible polynomial*	No.	*Irreducible polynomial*
1.	$x^8 + x^4 + x^3 + x + 1$	16.	$x^8 + x^7 + x^3 + x + 1$
2.	$x^8 + x^4 + x^3 + x^2 + 1$	17.	$x^8 + x^7 + x^3 + x^2 + 1$
3.	$x^8 + x^5 + x^3 + x + 1$	18.	$x^8 + x^7 + x^4 + x^3 + x^2 + x + 1$
4.	$x^8 + x^5 + x^3 + x^2 + 1$	19.	$x^8 + x^7 + x^5 + x + 1$
5.	$x^8 + x^5 + x^4 + x^3 + 1$	20.	$x^8 + x^7 + x^5 + x^3 + 1$
6.	$x^8 + x^5 + x^4 + x^3 +$	21.	$x^8 + x^7 + x^5 + x^4 + 1$

	$x^2 + x + 1$		
7.	$x^8 + x^6 + x^3 + x^2 + 1$	22.	$x^8 + x^7 + x^5 + x^4 + x^3 + x^2 + 1$
8.	$x^8 + x^6 + x^4 + x^3 + x^2 + x + 1$	23.	$x^8 + x^7 + x^6 + x + 1$
9.	$x^8 + x^6 + x^5 + x + 1$	24.	$x^8 + x^7 + x^6 + x^3 + x^2 + x + 1$
10.	$x^8 + x^6 + x^5 + x^2 + 1$	25.	$x^8 + x^7 + x^6 + x^4 + x^2 + x + 1$
11.	$x^8 + x^6 + x^5 + x^3 + 1$	26.	$x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + 1$
12.	$x^8 + x^6 + x^5 + x^4 + 1$	27.	$x^8 + x^7 + x^6 + x^5 + x^2 + x + 1$
13.	$x^8 + x^6 + x^5 + x^4 + x^2 + x + 1$	28.	$x^8 + x^7 + x^6 + x^5 + x^4 + x + 1$
14.	$x^8 + x^6 + x^5 + x^4 + x^3 + x + 1$	29.	$x^8 + x^7 + x^6 + x^5 + x^4 + x^2 + 1$
15.	$x^8 + x^7 + x^2 + x + 1$	30.	$x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + 1$

4.2 Cyclic group

Group G is **cyclic** if each element of G is a power a^k (k is an integer) of a fixed element $a \in G$. The element a is said to **generate** the group G or to be a **generator** of G. A cyclic-group is always abelian and may be finite or infinite [15]. Consequently, group G is called a **cyclic group** if:

$$\mathbf{G} = \langle a \rangle = \{a^n : n n \in \mathbb{Z}\} \text{ for some } a \in \mathbf{G} \quad (2)$$

In cryptography, two parties should communicate securely over unsecure channel for transferring the sensitive information such as credit cards numbers. This needs for shared secret key between two parties for encrypting the message, so Diffe and Hellman in 1976 published a landmark paper, which showed studying of how two parties communicate in secure manner. After applying the term of cyclic group in protocol of Diiffe Hellman, then it is used in El Gamal which is Public-Key Encryption Scheme [16].

5. Construction of proposed tables in GF (2^8)

The basic idea constructed from our state tables based on using two mathematical concepts used in cryptography: cyclic group and irreducible polynomials in GF (2^8). Since each number within the finite field has cyclic group that is different from other numbers, so we relied on this concept to generate new tables that the elements depend on cyclic group by selecting randomly only one number from this cyclic group to generate the new number. This is done by using the key generated randomly in decimal form for selecting a number within the cyclic group to generate a new number for tables to increase the randomness in these tables. While 30 irreducible polynomial in GF (2^8), then, 30 proposed tables are created, and samples of these tables are shown in Table (2) through Table (7).

Algorithm (1) illustrates the basic steps that are used for constructing the proposed tables.

Algorthim1: Constructing the proposed tables.

Step1: Generate 30 multiplication tables, each table is created based on irreducible polynomial in GF (2^8) as shown in table 1.

Step2: For each multiplication table that is generated in step1, generate a cyclic group for each item in tables saving the length of this cyclic group length.

Step3: Construct the proposed tables for each multiplication tables based on cyclic group as:

Step3.1: For each row and column in proposed table:

Step3.2: Bring the cyclic group of any item and the length of it labelled (L).

Step3.3: Generate random key in decimal form for selecting the number within the range of the length (L) of the cyclic group of this item, named lcg.

Step4: Compute result= (item^{lcg} mod irreducible polynomial) for this table

Step5: Save the result in the proposed table.

Table (2) State (ECG#0) Addition in GF (2^8)

ECG# 0	0	1	2	…	125	126	…	253	255	255
0	0	1	2	…	125	126	…	253	254	255
1	1	0	3	…	124	127	…	252	255	254
2	203	202	201	…	182	181	…	54	53	52
3	75	74	73	…	54	53	…	182	181	180
. . .	. . .	. . .	. . .	. . .	. . .	. . .	…	. . .	. . .	. . .
50	67	66	65	…	62	61	…	190	189	188
51	27	26	25	…	102	101	…	230	229	228
52	156	157	158	…	248	249	…	97	98	99
. .	. .	. .	. .	. .	. .	. .	. .	. .	. .	. .

.	.	.	.	.	.	.	.	.	.	.
252	56	57	58	…	69	70	…	187	198	199
253	199	198	197	…	186	185	…	58	57	56
254	103	102	101	…	26	25	…	154	153	152
255	34	35	32	…	95	92	…	223	220	221

Table (3) State (ECG#1) Addition in GF (2^8)

ECG# 1	0	1	2	…	125	126	…	253	255	255
0	0	1	2	…	125	126	…	253	254	255
1	1	0	3	…	124	127	…	252	255	254
2	99	98	97	…	30	29	…	158	157	156
3	103	102	101	…	26	25	…	154	153	152
. . .	. . .	. . .	. . .	. . .	. . .	. . .	…	. . .	. . .	. . .
50	98	99	96	…	31	28	…	159	156	157
51	190	191	188	…	195	192	…	67	64	65
52	183	182	181	…	201	202	…	74	73	72
. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .
252	231	230	229	…	154	153	…	26	25	24
253	94	95	92	…	34	35	…	163	160	161
254	99	98	97	…	30	29	…	158	157	156
255	124	125	126	…	1	2	…	129	130	131

Table (4) State (ECG#8) Addition in GF (2^8)

ECG# 8	0	1	2	…	125	126	…	253	255	255
0	0	1	2	…	125	126	…	253	254	255
1	1	0	3	…	124	127	…	252	255	254
2	14	15	12	…	115	112	…	243	240	241
3	84	85	86	…	41	42	…	169	170	171
. . .	. . .	. . .	. . .	. . .	. . .	. . .	…	. . .	. . .	. . .
50	247	246	245	…	138	137	…	10	9	8
51	208	209	210	…	173	174	…	45	46	47
52	167	168	165	…	218	217	…	90	89	88
. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .
252	21	20	23	…	104	107	…	232	235	234
253	221	220	223	…	160	163	…	32	35	34
254	66	67	64	…	63	60	…	191	188	189
255	238	239	236	…	147	144	…	19	16	17

Table (5) State (ECG#15) Addition in GF (2^8)

ECG# 15	0	1	2	…	125	126	…	253	255	255
0	0	1	2	…	125	126	…	253	254	255
1	1	0	3	…	124	127	…	252	255	254
2	89	88	91	…	36	39	…	164	166	167
3	119	118	117	…	10	9	…	138	137	136
. . .	. . .	. . .	. . .	. . .	. . .	. . .	…	. . .	. . .	. . .
50	36	37	38	…	89	90	…	217	218	219
51	251	250	249	…	134	133	…	6	5	4
52	4	5	6	…	121	122	…	249	250	251

. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .
252	200	201	202	…	181	182	…	53	54	55
253	117	116	119	…	8	11	…	136	139	138
254	239	238	237	…	146	145	…	18	17	16
255	206	207	204	…	179	176	…	51	48	49

Table (6) State (ECG#20) Addition in GF (2^8)

ECG# 20	0	1	2	…	125	126	…	253	255	255
0	0	1	2	…	125	126	…	253	254	255
1	1	0	3	…	124	127	…	252	255	254
2	247	246	245	…	138	137	…	10	9	8
3	41	40	43	…	84	87	…	212	215	214
. . .	. . .	. . .	. . .	. . .	. . .	. . .	…	. . .	. . .	. . .
50	33	32	35	…	92	95	…	220	223	222
51	163	162	161	…	222	221	…	94	93	92
52	154	155	152	…	231	228	…	103	100	101
. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .
252	196	197	198	…	185	186	…	57	58	59
253	103	102	101	…	26	25	…	154	153	152
254	119	118	117	…	10	9	…	138	137	136
255	249	248	251	…	132	135	…	4	7	6

Table (7) State (ECG#29) Addition in GF (2^8)

ECG# 29	0	1	2	…	125	126	…	253	255	255
0	0	1	2	…	125	126	…	253	254	255
1	1	0	3	…	124	127	…	252	255	254
2	16	17	18	…	190	191	…	237	238	239
3	7	6	5	…	122	121	…	250	249	248
. . .	. . .	. . .	. . .	. . .	. . .	. . .	…	. . .	. . .	. . .
50	225	227	226	…	156	159	…	28	31	30
51	219	218	217	…	166	165	…	38	37	36
52	90	91	88	…	39	36	…	167	164	165
. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .
252	32	34	35	…	93	94	…	221	222	223
253	68	69	70	…	57	58	…	185	186	187
254	52	53	54	…	73	74	…	201	202	203
255	56	57	58	…	69	70	…	197	198	199

6. Proposed improved methods

It is important to secure the encryption algorithm against all types of attacks by increasing the randomness of the algorithms. Thus, this section proposes a new method for increasing the security of the Twofish algorithm without increasing the complexity of its calculation. The basic idea of the proposal in question depends on extension previous # operation proposed cited in [7] but by constructing the new thirty tables that have been created based on cyclic group and irreducible polynomial called cyclic group extended # (CGE#). This is done by using additional key in encryption and decryption also to key that is used for creating the tables. Additional key is generated independently, the first key is called ($key_{\text{no of table}}$) which is used to determine the number of tables used to apply the (CGE#) operation. The second key is used to encrypt and decrypt. This (CGE#) operation requires three inputs: the first one specifies the index of the state table number, while the other two inputs match the row and column numbers in the specified state table; the cross point of these two numbers gives the result. The next section explains how to apply the proposed operation in Twofish algorithms.

6.1 Proposed Twofish Algorithm

There are many points of weaknesses in Twofish leading for breaking it such as: it depends only on single bit (0 or 1), using XOR operation and operates on bit. Therefore, to overcome these problems, a new method is introduced in this section, this is done by suggested Twofish algorithm used a new (CGE#) operation instead of the ordinary XOR operation used in the Feistel network. Since the XOR operation occurs twice in each round of the Feistel algorithm, the (CGE#) operation is also applied twice in each round after implementing the F-unction between the plain text and key scheduling. The total process of the (CGE#) operation, which needs three inputs to complete the work, is shown in Figure 3 and algorithms 2, where the modified steps are stated in red colour.

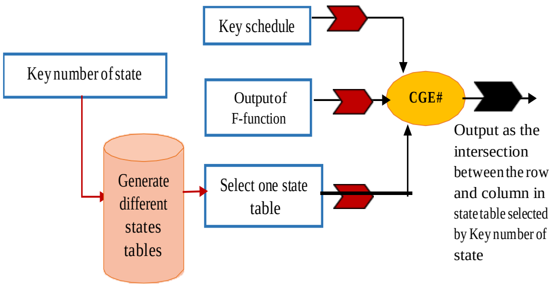


Figure (3) modified one round in Twofish algorithm.

Algorithm 3.10: Proposed Twofish Algorithm using (CGE#) operation.

Input: Plaintext P (128-bits) and Key K (128-bits)

Output: Cipher text (128-bits)

Begin

Step1: Separate the plain text (P) block into four sub-blocks: P_0, P_1, P_2, and P_3.

Step 2: Initialise the key (K).

Step 3: Input whitening ($P_0' = P_0 \oplus K_0$, $P_1' = P_1 \oplus K_1$, $P_2' = P_2 \oplus K_2$, and $P_3' = P_3 \oplus K_3$).

For each round from 1 to 16:

Step 4: P_3' is rotated one bit left.

Step 5: P_0' and P_1' are rotated left 8 bits and are each submitted to Four key-dependent S-boxes with 8-bit inputs and outputs.

Step6: Apply MDS matrix.

Step 7: Apply a PHD transform to output P_0'' and P_1''.

Step 8: The first subkey for the round is added to the output of Step6 to produce P_0''' and P_1'''.

Step 9: Compute $P_2'''' = (P_0'''$ CGE# $P_2')$ and $P_3'''' = (P_1'''$ CGE# $P_3')$.

Step10: P_2'''' is rotated (1-bit) right.

Step11: Two halves of the block are swapped: P'_0 is swapped with P''''_2, and P'_1 is swapped with P''''_3.

End For

Step12: Output whitening.

//Compute P_2'''' by applying the operation on P_0''' CG# P_2' according to 3-inputs (index = number of state tables, row = P_0''', and column = P_2').The output is computed as the cross point between the row and column in the specified state table gives the result. As the same manner, the P_1''' CGE# P_3' is computed.

End.

7. Evaluation

7.1 Computational Complexity

Complexity of encryption algorithm is calculated against the assailants to guess the key. The complexity is computed from the possible number of keys a conqueror requires in order to decrypt the cipher text (128-bits). **First**, the complexity of the original Two fish algorithm is compute using a predefined binary XOR operation (0, 1), that way giving the number of possible keys "applied in the encryption and decryption as: $2 \times (2)^8 \times 32 \times 4 = 2^{16}$. **Then** computing the complexity of the proposed algorithm using (CGE#) operation: the probability of plaintext × (The probability of key)$^{\text{no.of round}}$ × The probability of states tables.

The complexity of the proposed Twofish using CGE# is:

$(2^8)^{16} \times ((2^8)^{16})^8 \times 30 \times 32 \times 4 = 2^{1159} \times 30$ … (3)

Table 8 presents the results based on calculating the complexity of the modified Twofish algorithm compared with the well-known Twofish algorithm.

Table (8) total complexity comparison of the well-known and proposed Twofish algorithms for sixteen rounds.

Algorithm	The complexity key size (128-bit)
well-known Twofish algorithm	2^{16}
Proposed Twofish algorithm	$2^{1159} \times 30$

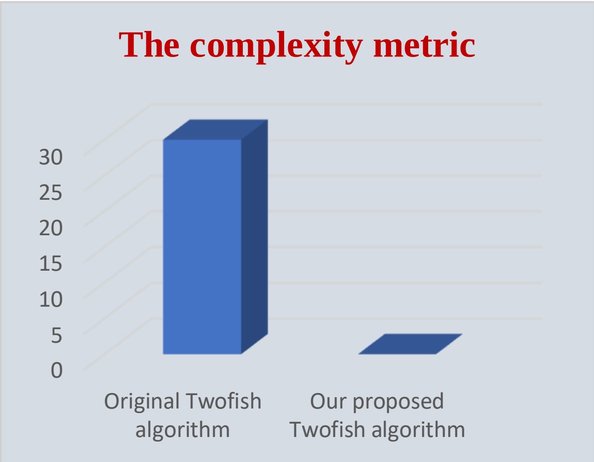


Figure (4) the complexity of original Twofish compared with proposed Twofish proposed.

Figure (4) illustrates how the proposed Twofish algorithm features higher complexity compared to the well-known in sixteen rounds.

7.2 National Institute of Standards and Technology (NIST)

For testing the randomness of the encryption algorithms, NIST test is used this purpose. NIST has a number of tests [17]. This study uses fifteen statistical tests from NIST statistical for testing the randomness of Twofish algorithms. The average tests are computed and tabulated in Table (9).

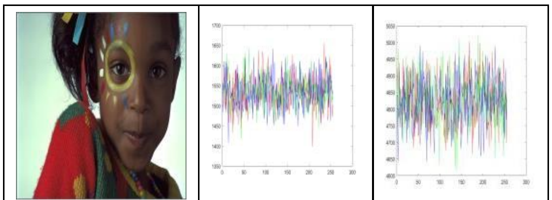
Table (9) Result of Running NIST on the Generated Key by Twofish and the Proposed Twofish.

Test no.	Statistical Test Name	original Twofish		Proposed Twofish using CGE# operation	
		P-Value	Status	P-Value	Status
1	Approximate Entropy	0.187	pass	0.486	Pass
2	Block Frequency	0.187	pass	0.643	Pass
3	Cumulative Sums	0.837	pass	0.119	Pass
4	FFT	0.601	pass	0.750	Pass
5	Frequency	0.090	pass	0.019	Pass
6	Linear complexity	0.844	pass	0.711	Pass
7	Longest Run	0.141	pass	0.357	Pass
8	Non Overlapping Template	0.373	pass	0.485	Pass
9	Overlapping Template	0.369	pass	0.781	Pass
10	Random Excursions	0.401	pass	0.240	Pass
11	Random Excursions Variant	0.580	pass	0.411	Pass
12	Rank	0.251	pass	0.259	Pass
13	Runs	0.133	pass	0.338	Pass
14	Serial	0.339	pass	0.634	Pass
15	Universal	0.233	pass	0.140	Pass

The probability value (p-value) is set to a value of (0.01) to emphasize whether the output is random or not. If the test results provide a p-value “asymptotically approaching 1, then the output should appear to have complete randomness. A p-value equal to zero signifies that the output is non-random. The pass status represents that the p-value of these tests is greater than 0.001 and denotes the output is acceptable (e.g., offers good randomness). The p-values of most of the tests from the proposed Twofish algorithms are greater than the p-values of the original algorithm, as shown in Table (9). Consequently, the proposed algorithms are better than the original in most tests.

7.3 Histogram

A histogram is used to measure the security of the original and encrypted images by showing the distribution between the pixels. A histogram analysis was conducted for both the original and proposed DES and AES. Figures (5 and 6) show the experimental results for two standard colour images with JPEG formats.



a. image1 | a1. Histogram of well-known Twofish | a2. Histogram of Twofish using CGE#

Figure (5) results histogram of original and proposed Twofish for image2.

Figure (6) results histogram of original and proposed Twofish for image1.

7.4 Correlation Coefficients

It is a statistical measure used to evaluate the level of similarity between two adjacent pixels in the image or between two pixels in the same location of the original and encrypted image [18]. Karl Pearson in 1895 defined the equation for calculating the correlation coefficient called *r* which it is most used in statistical security analysis. The Pearson's correlation coefficient can be calculated by using the following equation which defined as [19]:

$$r = \frac{\sum(X_i - \bar{X})(Y_i - \bar{Y})}{\left[\sum(X_i - \bar{X})^2 \ (Y_i - \bar{Y})^2 \ \right]^{1/2}} \qquad (5)$$

Where X and Y are the pixels and neighbouring pixels of the original and encrypted image. The standard values of r in the range ($-1 \leq r \leq 1$), if the value of r is close to zero, the association between the original and encrypted image is perfect uncorrelated. If the value of r is give negative value that mean the encrypted image is negative of original image [20]. Table (10) shows the values of correlation coefficients in horizontal pixels for peppers image that encrypted by original and proposed Twofish.

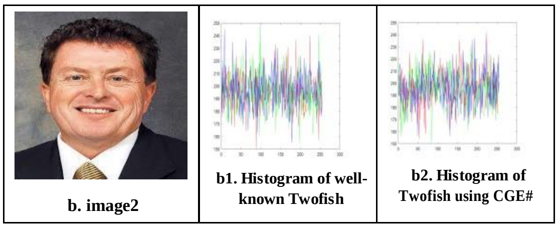
Table (10) results for the correlation coefficients.

Algorithm	Correlation coefficients
Well-known Twofish algorithm	**-0.00099219**
Proposed Twofish algorithm	**-0.00023793**

As show in the above table, our proposed Twofish give value of correlation lower than the original Twofish.

8. Conclusion

In this article, a new method modification on Feistel Twofish algorithm. This is done using additional key for handling the 30 tables are created using multiplication operation with cyclic group and irreducible polynomial in GF (2^8).The experimental results are obtained from the proposed algorithm compared with the original based four security metrics using (C#) programming language in Visual Studio 2017. Our modified algorithm gives good results in



acceptable results against differential attacks using correlation coefficients analysis**.** Consequently, our modification on the proposed Twofish gives best results compared with original once.

References

[1] Swathi S, IILahari P. Encryption algorithms: a survey. International Journal of Advanced Research in Computer Science & Technology 2016; 4(2): 81-88.

[2] Septafiansyah D.P, Mario Y., Sarwono S., Yusuf K., Adang S. A. Power analysis attack against encryption devices: a comprehensive analysis of AES, DES, and BC3, TELKOMNIKA, Vol.17, No.3, June 2019, 1282~1289.

[3] Sonia R, Harpreet K. Technical survey on cryptography algorithms for network security. International Journal of Advanced Research in Computer Science and Software Engineering 2016; 4(9): 204-209.

[4] Christina L, Joe Irudayaraj V S. Optimized Blowfish encryption technique. International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certi_ed Organization) 2014; 2(7): 5009-5015.

[5] M. A. Hameed, Ahmed I.Jaber, Jamhoor M. Alobaidy, Alaa A. Hajer, "Design and Simulation DES Algorithm of Encryption for Information Security," *American Journal of Engineering Research (AJER)*, vol. 7, no. 4, pp.13-22, 2018.

[6] Sreeja Rajesh, Varghese Paul, Varun Menon , Mohammad Khosravi, *"*A Secure and Efficient Lightweight Symmetric Encryption Scheme for Transfer of Text Files between Embedded IoT Devices", *Symmetry MDPI*, Vol. 11, NO. 2, February 2019.

[7] Hala B. Abdul Wahab and Abdul Monem S. Rahma, "Proposed New Quantum Cryptography System Using Quantum Description techniques for Generated Curves", *The 2009 International conference*

on security and management, SAM2009, July 13-16 2009, Las Vegas, USA, SAM 2009.
[8] Deepali R. Superiority of Twofish over Blowfish. International Journal of scientific research and management 2016; p. 4744-474, 64(11).
[9] Apoorva, Yogesh, K. Comparative Study of Different Symmetric Key Cryptography Algorithms. International Journal of Application or Innovation in Engineering & Management (IJAIEM) 2013; p. 204-206, 2(7).
[10] Purnima Gehlot S. R Biradar and B. P. Singh , "Implementation of Modified Twofish Algorithm using 128 and 192-bit keys on VHDL", *International Journal of Computer Applications (0975 – 8887) Volume 70– No.13, May 2013.*
[11] Rehab F. Hassan, "New Approach for Modifying DES Algorithm Using 4-States Multi keys", *Eng. & Tech. Journal*, Volume 28, No.20, 2010.
[12] Sahab Dheyaa Mohammed and Abdul Monem S. Rahma, "Modifying DES Algorithm by Using Diagonal Matrix Based on Irreducible Polynomial", *Journal of Theoretical and Applied Information Technology*, pp.1476-1487, Vol.97. No 5, March 2019.
[13]Lidl, Rudolf, and Harald Niederreiter, "Introduction to finite fields and their applications". Cambridge university press, 1994.
[14] Madhuri, O. B. B., E. Rambabu, and Malijeddi Murali. "Design and Implementation of Arithmetic Unit for GF (2m)." *International Journal of Advanced Research in Computer Engineering &Technology (IJARCET)* pp-185, 2012.
[15] Stallings W. "*Cryptography and network security principles and practice*. USA: Prentice Hall; 2006.
[16] Marlow Anderson**,** "A First Course in Abstract Algebra: Rings, Groups, and Fields", Third Edition.
[17] Alaa M. Riad and etc., Evaluation of the RC4 Algorithm as a solution for Converged Networks, Journal Of electrical engineering, Vol. 60, No. 3, pp.155–160, 2009.
[18] Priya Ramasamy, Vidhyapriya Ranganathan, Seifedine Kadry, Robertas Damaševiˇcius and Tomas Blažauskas , "An Image Encryption Scheme Based on Block Scrambling, Modified Zigzag Transformation and Key Generation Using Enhanced Logistic—Tent Map", Mdpi/journal/entropy, Vol.21, No.7, pp.1-17, 2019.
[19] J.L.Rodgers, W.A. Nicewander, "Thirteen Ways to Look at the Correlation Coefficient", The American Statistician, Vol. 42, No. 1, pp.59-66, February 1988.
[20] Avneet Kaur, Lakhwinder Kaur and Savita Gupta, "Image Recognition using Coefficient of Correlation and Structural SIMilarity Index in Uncontrolled Environment", International Journal of Computer Applications (0975 – 8887) Vol. 59, No.5, pp.32-39, December 2012.