ISSN 2303-4521
Periodicals of Engineering and Natural Sciences *Original Research*
Vol. 9, No. 3, August 2021, pp.568-578

A new block cipher algorithm that adopts the magic square of the fifth order with messages of different lengths and multi-function in GF(2^8)

Ibrahim Malik ALattar[1] *, Abdul Monem S. Rahma[1]
[1]Computer Science Department, University of Technology-Iraq, Baghdad, Iraq.

ABSTRACT

This paper is considered as a development of encryption algorithms based on Magic Square of Order Five. Both GF(P) and GF(2^8) are used to encode both images and text. Where two different algorithms were used, the first using message length = 10 and the second message length = 14, and an unspecified number of rounds were added and a mask will be used in the even round will use the addition operation and in the odd round will used the multiplication operation so that the text resulting from the first round will be as input text for the next Round, and thus. The speed, complexity, NIST tests and histogram for the first ten rounds were calculated and compared with the results of the previous algorithm before the rounds were made, where the complexity in the first algorithm was = $((256)^{15})^{r+1}\times (256)^{10}$ + or × $(256)^{25}$ and the complexity in the second algorithm = $((256)^{11})^{r+1}\times(256)^{14}$ + or × $(256)^{25}$ where r represents the number of round used.

Keywords: Cryptography, Magic Square, Block Cipher, Gauss Elimination, GF(2^8).

Corresponding Author:

Ibrahim Malik Alattar
Department of Computer Science, University of Technology
Baghdad, Iraq.
ibrahiminter@yahoo.com

1. Introduction

The development in life and the importance of the information transmitted between people on various sites has resulted in not being satisfied with the traditional and well-known methods and the need to develop new proposed algorithms [1]. Magic squares played prominent roles in life in general, as it was found back to the ages B.C. As life developed, magic squares were exploited in many areas of life [2]. Mathematicians were particularly interested in magic squares, as they, together with cryptologists, designed and implemented several games and methods based mainly on magic squares, as in the game of Sudoku [3]. Where the magic square of the third degree was used in encryption by allocate some locations for the key and others for the message, and the work was developed using the magic square of the fourth degree so that the number of message locations was equal to 8 and the number of keys locations = 8 as well, And the work in the two algorithms was mainly based on magic, as it was considered as the encrypted text and it was not required that the result of the encrypted texts be equal in their values [4]. Cryptologists are very interested in magic squares and their properties, as we will see in this paper. Also will include a group of previous works that are related to the proposed work, as shown below In 2015, a group of researchers presented a proposed encryption algorithm based on the magic square, whereby two specific magic squares were created, and during which the even and odd magic square were used[6]. In the same year, a group of researchers proposed a cipher algorithm using asymmetric encryption (public key), which depends on Diffie–Hellman, and during which 6 magic squares of the third degree (magic cube) were used [7].In 2016, Rahma, Abdul Hossen and Dawood proposed a cryptographic algorithm using Diffie-Hellman, through which it shows the dimensions of the magic square, and it relied heavily on the value of the magic constant and the magic sum [8]. In the same year, a group of researchers proposed an encryption

algorithm based on folding 6 magic squares to obtain the magic cube to be used in encryption, regardless of the type of magic square, whether it is odd or even [9].
In 2017, Kaur , Bharadwaj and Mankotia developed an encryption algorithm based on multi-level encryption, where the development was done on the RSA and DES encryption algorithms , and the results were discussed [10]. In 2018, Habboush proposed an encryption algorithm using multi-level encryption, where was combine symmetry strength with the AES algorithm and the Feistel network. Also discussed and compared the results with different algorithms such as RC5, DES and 3DES [11]. In 2019, Al-Hashemi and Mahdi proposed an algorithm for encoding color images where the information was placed in a normal matrix and then multiplied by the magic square, as well as using the XOR process for the two sets of the resulting matrix [12]. In the year 2020, researchers Mohammed and Hasan proposed a method by which to get rid of redundancy characters of cipher text by using the magic square of order 3 [14].

2. Previously technologies and advantages

The golden advantage in magic squares is that the sum of each diagonal, column or row is equal and then it is called the normal magic square, if it is a normal magic square and the numbers in it are all Prime Number then it is called Prime magic square [15]. from that, the properties of magic squares (MS) were used in encryption, as MS5 is filled with numbers from 1 to 25, but here each group of sums does not have to be equal with the other [16]. The specified system is relied upon, as all elements will be dependent on the prime number used (P) [17]. The 8-bit system was used because the current devices used were all based on the eight bits. Then the system of the field was changed from GF(P) to GF(2^8), where the polynomial numbers are used, and the specific field depends on irreducible polynomial number[18]. Let's make this clearer, let's assume that the prime number 151 is chosen for GF(P) and as known that the ASCII code for the existing texts has a value from 0 to 255. Therefore, the Prime number that was chosen does not succeed in retrieving all the numbers in the field because the numbers from 151 - 255 will be neglected, so it is necessary to take a larger primary number, because we find that the largest prime number close to 255 is 251, the same problem will be reached as the numbers From 251 - 255 it will be neglected, and if we raise the prime number from 255 (because 255 not prime number and can't be used) there will be another problem as the numbers from 256 - P will be outside the range, so GF(2^8) was used[19-23]. When using GF(2^8), the decimal numbers will be ignored and replace to the polynomial numbers, so they do not contain numbers except for two numbers zero and one and the rest is an X variable raised to the exponent of a positive integer greater from one [24]. A system of linear equations is a set of linear mathematical equations that may be one or more than that, but they must be within the same set of variables, and Gaussian deletion is a mathematical algorithm used to solve linear equations and consists of several steps and it use during that many operations such as multiplication and addition [25]. Cryptography is a science concerned with encrypting data, preserving its confidentiality, and transmitting it to the other party without change or modification by the third party (external) [11]. Multi-rounds Cryptography it is a system that consists of several rounds that are made in succession, unlike the single round that occurs only once [24].

3. The proposed cryptography technique

When taking the properties of the normal magic square, 12 equations will be obtained, since five of them are from the sum of the rows, five other equations from the sum of the columns, and two other additional equations for the sum of each diameter from the diagonals of MS5. This suggestion is considered as a development of the suggested algorithms for message length = 10 and 14. Where the suggestion is as follows: The encryption Process is repeated using MS5 several times in order to serve as rounds then In each round, a mask matrix is used which its size is equal to the size of the magic square used and depending on the number of rounds, where if the round number is even, the addition process of the magic square and the mask is used, while in the case of the round number is odd, the multiplication process between the mask and the magic square is used.

3.1. The 1st algorithm suggested: Insert key for message length = 10 using GF(2^8)

After examining the resulting equations, it was found that two of them have dependency and therefore were removed, so the remaining number of equations became 10 equations. Depending on the message length, the length of the key will be 15 (according to MS5), and the selected keys locations have flexibility in the value and location of the keys. As a result, we will have 10 equations, each of which corresponds to each sum of the sums. It is assumed that the next key was chosen by the two parties that will exchange information (see Figure 1).

	k	k	k	k
k		k		k
	k	k		k
k			k	
k		k		k

Figure 1. Assumed keys locations was chosen with message length = 10 for GF(2^8)

Therefore, the message will be filled in at the remaining locations in order, and the result will be MS5 as shown in Figure 2.

M_{00}	M_{01}	M_{02}	M_{03}	M_{04}
M_{10}	M_{11}	M_{12}	M_{13}	M_{14}
M_{20}	M_{21}	M_{22}	M_{23}	M_{24}
M_{30}	M_{31}	M_{32}	M_{33}	M_{34}
M_{40}	M_{41}	M_{42}	M_{43}	M_{44}

Figure 2. The colored cells represent the key and the remaining cells the message in matrix M

Then an addition or multiplication operation is used between the resulting magic square (in Figure 2) and the mask matrix used, depending on the round number used if it is odd or even as shown in figure 3.

N_{00}	N_{01}	N_{02}	N_{03}	N_{04}
N_{10}	N_{11}	N_{12}	N_{13}	N_{14}
N_{20}	N_{21}	N_{22}	N_{23}	N_{24}
N_{30}	N_{31}	N_{32}	N_{33}	N_{34}
N_{40}	N_{41}	N_{42}	N_{43}	N_{44}

=

K_{00}	K_{01}	K_{02}	K_{03}	K_{04}
K_{10}	K_{11}	K_{12}	K_{13}	K_{14}
K_{20}	K_{21}	K_{22}	K_{23}	K_{24}
K_{30}	K_{31}	K_{32}	K_{33}	K_{34}
K_{40}	K_{41}	K_{42}	K_{43}	K_{44}

+ Or ×

M_{00}	M_{01}	M_{02}	M_{03}	M_{04}
M_{10}	M_{11}	M_{12}	M_{13}	M_{14}
M_{20}	M_{21}	M_{22}	M_{23}	M_{24}
M_{30}	M_{31}	M_{32}	M_{33}	M_{34}
M_{40}	M_{41}	M_{42}	M_{43}	M_{44}

Figure 3. Multiplication or addition between MS5 and the used Mask depending on the number of round

Therefore, sums are obtained as shown by the equations below:

$$
\begin{aligned}
&s1: \ Sum1 = N_{00} + N_{01} + N_{02} + N_{03} + N_{04} \\
&s2: \ Sum2 = N_{10} + N_{11} + N_{12} + N_{13} + N_{14} \\
&s3: \ Sum3 = N_{30} + N_{31} + N_{32} + N_{33} + N_{34} \\
&s4: \ Sum4 = N_{40} + N_{41} + N_{42} + N_{43} + N_{44} \\
&s5: \ Sum5 = N_{00} + N_{10} + N_{20} + N_{30} + N_{40} \\
&s6: \ Sum6 = N_{01} + N_{11} + N_{21} + N_{31} + N_{41} \\
&s7: \ Sum7 = N_{03} + N_{13} + N_{23} + N_{33} + N_{43} \\
&s8: \ Sum8 = N_{04} + N_{14} + N_{24} + N_{34} + N_{44} \\
&s9: \ Sum9 = N_{00} + N_{11} + N_{22} + N_{33} + N_{44} \\
&s10: Sum10 = N_{04} + N_{13} + N_{22} + N_{31} + N_{40}
\end{aligned}
\qquad (1)
$$

After that, we will start with new round, where a new key will be chosen in MS5 and the previous Sums will represent the message in the positions of the message, and then used the mask as in figure 3, and new sums will be found, and so forth, according to the number of rounds required. And the value of the final resulting sums represents the encrypted text, which is sent to the recipient.

On the opposite side, the recipient has the keys with length equal to 15 and the encrypted text of message length equal to 10, and in the case of using the even round will subtract the mask and in the case of the even round will multiply with the inverse of the mask. Then will solve the ten equations with ten unknowns as linear equations based on GF(2^8), In our practical and statistical calculations, it was solved by gauss elimination method, It will find the value of unknowns several times depending on the number of rounds used.

The encryption work in this way was also developed using Galois Field based on the prime number GF(P). There is no fixed or specific algorithm for encoding or decoding, but steps have been put in place to explain the proposed algorithm for both encryption and decryption.

Algorithm 1-a: The Suggested algorithm Symmetric cipher based on MS 5 – Encryption.

Input: Key Positions , Key Value , No. of Rounds and The message (Text Or Image)

Output: Cipher text.

Begin:

Step1 : Putting the key value in the agreed locations in MS 5.

Step2 : put the message at the remaining positions in MS 5.

Step3 : used the addition between the mask used and the MS5 formed.

Step4 : Find the sum of each row, column, and diameter in the matrix M (see Figure 2), as in (1).

Step5 : repeated the steps bellow many times depending on the number of rounds used

i. Choose another Key value in new Positions.
ii. Put the last sums founds in the remaining positions.
iii. Used the addition or multiplication between the mask and MS5 depending on the number of round used is even or odd.
iv. Find the sums for each new row, column and the two diagnals.

The Result of the final Sums will represent the ciphertext and will be send to the recipient.

End.

Algorithm 1-b: The Suggested algorithm Symmetric cipher based on MS 5 – Decryption.

Input: Key Positions, Key Values , cipher text and No. of Rounds.

Output: plaintext (Image or Text).

Begin:

Step1: repeated the steps bellow depending on the number of rounds used in descending order**.**

i. Put the key value in the agreed position in MS5, thus the length of the keys will be equal to 15.
ii. Put the last cipher text (Sums) gained (which length = 10) in MS5.
iii. Subtrace the key from the mask if the number of round is even, or multiply MS5 by the inverse of the mask in the case of using odd round.
iv. There will be ten equations resulting; these equations will be arranged so that the main diameter does not contain the value zero.
v. Solve the ten equations way as linear equations.

End Loop.

Step2: the final results will be the original message (Image or Text).

End.

3.2. The 2nd Algorithm suggested: Insert key for message length = 14 using GF(2^8) :

The work was to add four new equations to the coding system, so that the total is 14 equations.
In this proposed algorithm,the development will be similar to the first development, which is to add a number of rounds, their number according to the desire of the mutual parties, as there will be a new key and new key locations with each rounds. A mask was also used, and in the event that the number of the round used is even, the addition process is used, and otherwise, the multiplication process between MS5 and the mask is used.
It is assumed that the following locations have been selected for the key (Figure 4)

k		k		k
	k		k	
k		k		
			k	k
	k	k		

Figure 4. Assumed keys locations was chosen with message length = 14 for GF(2^8)

The work will be completely similar to the first algorithm, only the difference the 14 equations will use the first ten exactly as in (1) and the additional four equations (see (2)), where they were selected based on Figure 2.

$$\begin{aligned} s1: \ & Sum11 = N_{02} + N_{11} + N_{20} + N_{34} + N_{43} \\ s2: \ & Sum12 = N_{01} + N_{10} + N_{24} + N_{33} + N_{42} \\ s3: \ & Sum13 = N_{02} + N_{13} + N_{24} + N_{30} + N_{41} \\ s4: \ & Sum14 = N_{03} + N_{14} + N_{20} + N_{31} + N_{42} \end{aligned} \quad (2)$$

The text of the second proposed algorithm will be similar to the first proposed algorithm a and b, and the only difference will be in both the length of the message used as it will be 14 instead of 10 and the key length also 11 instead of 15, and the rest of the steps are the same.
In addition, a work development was made, where both types of GF were used.

4. Evaluation

Cryptography is the science that concerned with the encryption process using certain algorithm and Re-retrieval it by decryption process using inverse steps for the encryption algorithm and the work required private key between the mutual parties , Regardless of the type and name of the encryption algorithm , and the key are kept secret between the two parties to ensure that the message arrives safely without modification or change (data integrity).
Here will discuss speed, complexity, NIST statistics, and histogram statistics for images, and compare the results together and compare them with the results of previous algorithms using the two types of data (images and text), and using both types of GF. Results and statistics were calculated using a laptop in the following specifications: system; Windows 10 Pro , 64-Bit Operating system , ×64-based processor, RAM; 8.00 GB , Processor; Intel(R) Core(TM) i5-4310M CPU @ 2.70GHz 2.70 GHz, Display Name: Intel(R) HD Graphics 4600.

4.1. The complexity for brute force

the complexity of the key will calculated in terms of the number of attempts necessary to try to break it and it is called Brute Force Attack, as it was calculated for each proposed algorithm and for the two types of GF.
In MS5 Using the first algorithm (before adding rounds) the key complexity will be in GF(P) the prime number raised to the exponent of 15 multiplied by or added to the used mask depending on the number of the round. while when using GF(2^8) the complexity of brute force attack will be 256 raised to exponent 15.
In other hand, for the second algorithm the complexity of Brute Force Attack using GF(P) will be the prime number used raised to the exponent 11 since MS5 used 14 length of message. And when using GF(2^8) the complexity of brute force attack will be 256 instead of the prime number. Upon the proposed development, the complexity in brute force Attack will be the same but all equation will be raised to the exponent number round used (r) plus one. The equations (3) - (10) will show the complexity of algorithm 1 using GF(P) , GF(2^8) , Algorithm 2 using GF(P) and GF(2^8) respectively.

If r is even	$K1 = ((P)^{15})^{r+1} + (P2)^{25}$	(3)
If r is odd	$K2 = ((P)^{15})^{r+1} \times (P2)^{25}$	(4)
If r is even	$K3 = ((256)^{15})^{r+1} + (P)^{25}$	(5)
If r is odd	$K4 = ((256)^{15})^{r+1} \times (P)^{25}$	(6)
If r is even	$K5 = ((P)^{11})^{r+1} + (P)^{25}$	(7)
If r is odd	$K6 = ((P)^{11})^{r+1} \times (P)^{25}$	(8)
If r is even	$K7 = ((256)^{11})^{r+1} + (P)^{25}$	(9)
If r is odd	$K8 = ((256)^{11})^{r+1} \times (P)^{25}$	(10)

4.2. The complexity for suggested algorithms

In the beginning we will discuss the complexity of the algorithm before development, where the complexity will be equal to the product of data complexity multiplied by the complexity of the key, the complexity of the key has been previously calculated (see sec. 5.1), while the complexity of the data will be the same for all algorithms which is equal to the value 256 (which represent the value of the ASCII code)raised to the message length according to the proposed algorithm.
In the first algorithm using GF(P), the total complexity will be the complex of the key multiplied by 256 raised to the power of 10 (message length), while when using GF(2^8) key complexity will be multiplied by 256 raised to Power 14. While in the second algorithm the total complexity with using GF(P) and GF(2^8) will be the key

complexity of each one of them multiplied by the complexity of data which equal to 256 raised to the exponent of 14 which represent the length of the message used. and the general complexity for the development of adding Rounds will be the key complexity multiplied by the data complexity, the equations (11) – (18) will Illustrates the complexity of the first algorithm using GF(P), using GF(2^8), the second algorithm using GF(P) and using GF(2^8) Respectively.

$$\textit{If r is even} \quad C1 = ((P)^{15})^{r+1} \times (256)^{10} + (P)^{25} \tag{11}$$

$$\textit{If r is odd} \quad C1 = ((P)^{15})^{r+1} \times (256)^{10} \times (P)^{25} \tag{12}$$

$$\textit{If r is even} \quad C2 = ((256)^{15})^{r+1} \times (256)^{10} + (P)^{25} \tag{13}$$

$$\textit{If r is odd} \quad C2 = ((256)^{15})^{r+1} \times (256)^{10} \times (P)^{25} \tag{14}$$

$$\textit{If r is even} \quad C2 = ((P)^{11})^{r+1} \times (256)^{14} + (P)^{25} \tag{15}$$

$$\textit{If r is odd} \quad C2 = ((P)^{11})^{r+1} \times (256)^{14} \times (P)^{25} \tag{16}$$

$$\textit{If r is even} \quad C2 = ((256)^{11})^{r+1} \times (256)^{14} + (P)^{25} \tag{17}$$

$$\textit{If r is odd} \quad C2 = ((256)^{11})^{r+1} \times (256)^{14} \times (P)^{25} \tag{18}$$

The figure 5 bellow will explain comparing the complexity for Algorithms 1 and 2 .

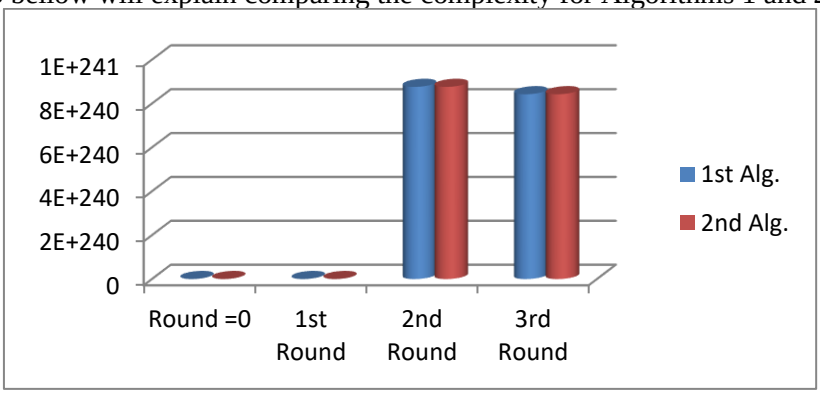

Figure 5. The complexity for the first and the second suggested algorithms

4.3. The time to implementation

The execution time was calculated for the proposed algorithms where the execution time was calculated for the encryption and decryption processes for each type of GF and for the first 10 rounds randomly.

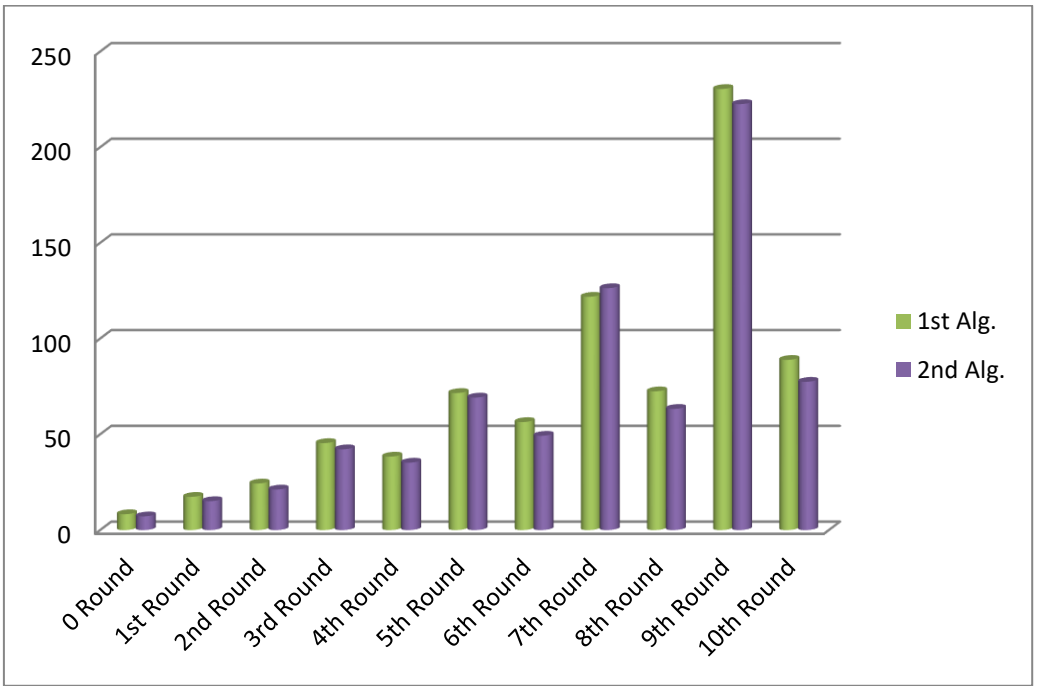

Figure 6. Comparison of the execution time of the proposed algorithms using GF(P)

Table 1. The time spent in encryption/decryption

No. of Algorithm suggested	GF type	Data type	No. of Round/s	Encryption Time	Decryption Time
1st alg.	GF(P)	image	Round =0	00:00:00.0213934	00:00:08.2601670
1st alg.	GF(P)	image	1st Round	00:00:00.1117305	00:00:17.2345303
.	.	.	.	.	.
.	.	.	.	.	.
1st alg.	GF(P)	image	10th Round	00:00:00.2052750	00:01:28.6570786
1st alg.	GF(2^8)	image	Round =0	00:00:02.7163126	00:00:03.1716145
1st alg.	GF(2^8)	image	1st Round	00:21:06.9138232	00:31:04.6424432
.	.	.	.	.	.
.	.	.	.	.	.
1st alg.	GF(2^8)	image	10th Round	00:00:21.1235424	00:00:30.7547822
2nd alg.	GF(P)	image	Round =0	00:00:00.0174759	00:00:07.1284692
2nd alg.	GF(P)	image	1st Round	00:00:00.0912548	00:00:15.0158423
.	.	.	.	.	.
2nd alg.	GF(P)	image	10th Round	00:00:00.1755863	00:01:17.2489296
2nd alg.	GF(2^8)	image	Round =0	00:00:02.2434374	00:00:05.7370713
2nd alg.	GF(2^8)	image	1st Round	00:19:05.1548418	00:40:10.1989336
.	.	.	.	.	.
2nd alg.	GF(2^8)	image	10th Round	00:00:20.7904024	00:00:55.0053715
1st alg.	GF(P)	text	Round =0	00:00:00.0030773	00:00:00.0985611
1st alg.	GF(P)	text	1st Round	00:00:00.0078285	00:00:00.2188839
.	.	.	.	.	.
1st alg.	GF(P)	text	10th Round	00:00:00.0314256	00:00:01.0057278
1st alg.	GF(2^8)	text	Round =0	00:00:00.1319539	00:00:00.4325824
1st alg.	GF(2^8)	text	1st Round	00:01:03.5621219	00:01:14.3239081
.	.	.	.	.	.
1st alg.	GF(2^8)	text	10th Round	00:00:02.0048684	00:00:01.8778170
2nd alg.	GF(P)	text	Round =0	00:00:00.0027125	00:00:00.0901478
2nd alg.	GF(P)	text	1st Round	00:00:00.0702485	00:00:00.1812849
.	.	.	.	.	.
2nd alg.	GF(P)	text	10th Round	00:00:00.6982681	00:00:01.0892157
2nd alg.	GF(2^8)	text	Round =0	00:00:00.1134821	00:00:00.7970462
2nd alg.	GF(2^8)	text	1st Round	00:01:03.4026476	00:01:40.7605775
.	.	.	.	.	.
2nd alg.	GF(2^8)	text	10th Round	00:00:01.49454704	00:00:04.5761732

And the following figures 6 and 7 shows a comparison between the first and second algorithms, using both types of GF.

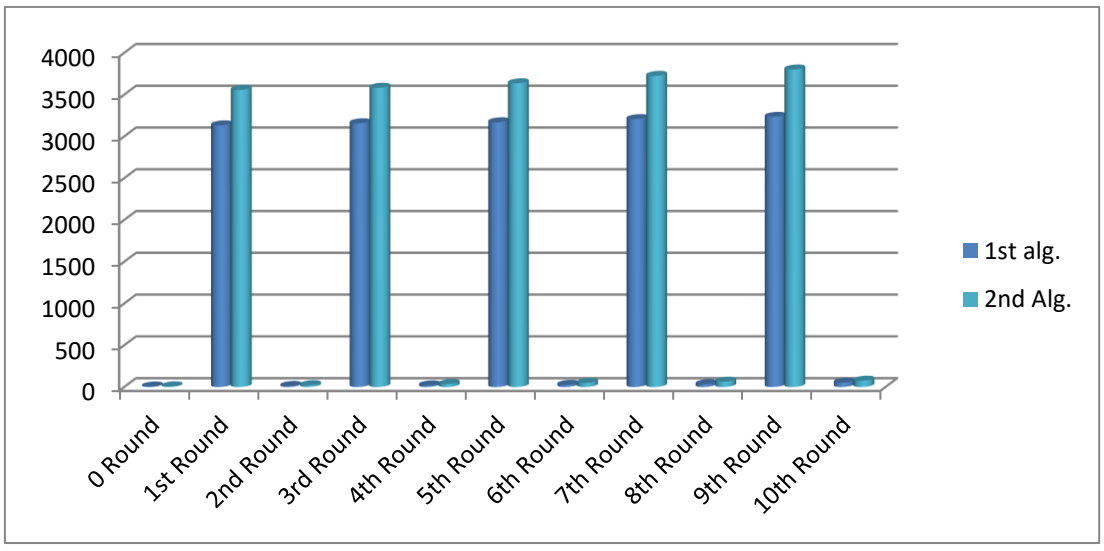

Figure 7. Comparison of the execution time of the proposed algorithms using GF(2^8)

4.4. NIST tests

NIST (shortcut for National Institute of Standards and Technology) statistics are used as another evaluation. Several calculations are calculated, including the measurement of randomness and other statistics. Experiments were conducted on all the proposed methods and algorithms as shown in the following tables.

Table 2. The final results for NIST tests using the suggested algorithms

No. of Alg.	Round No.	GF Type	The Frequency	Cumulative Sums	The Runs	The Longest Runs of ones	Approximate entropy	The Serial test
1st Alg.	1	GF(2^8)	0.203092	0.014419	0.110617	0.950667	0.124295	0.663650
1st Alg.	2	GF(2^8)	0.777297	0.405915	0.204926	0.659313	0.355435	0.648221
.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.
1st Alg.	10	GF(2^8)	0.651553	0.328426	0.195425	0.599652	0.3065845	0.598548
1st Alg.	1	GF(P)	0.007210	0.014419	0.498806	0.072069	0.0229920	0.522046
1st Alg.	2	GF(P)	0.364545	0.154765	0.365544	0.095458	0.3025548	0.485144
.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.
1st Alg.	10	GF(P)	0.396144	0.770513	0.423422	0.091831	0.5062610	0.033373
2nd Alg	1	GF(2^8)	0.887537	0.131984	0.322842	0.516449	0.522462	0.481909
2nd Alg	2	GF(2^8)	0.852515	0.205248	0.358844	0.458965	0.369744	0.254799
.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.
2nd Alg	10	GF(2^8)	0.336844	0.082254	0.293681	0.099145	0.192455	0.394154
2nd Alg	1	GF(P)	0.571608	0.314554	0.124670	0.682873	0.208172	0.353455
2nd Alg	2	GF(P)	0.471589	0.298414	0.201478	0.145252	0.214551	0.321558
.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.
2nd Alg	10	GF(P)	0.301756	0.197544	0.258465	0.258472	0.214855	0.384155
	Final results		All success	All success	All success	All success	All success	All success

4.5. Histogram accounts

Histogram calculations were made for a variety of images using both the first and second proposed algorithms, for each of GF(P) and GF(2^8), and for a different number of rounds for each proposed algorithm, and the results were compared and compared with the original image as shown below:

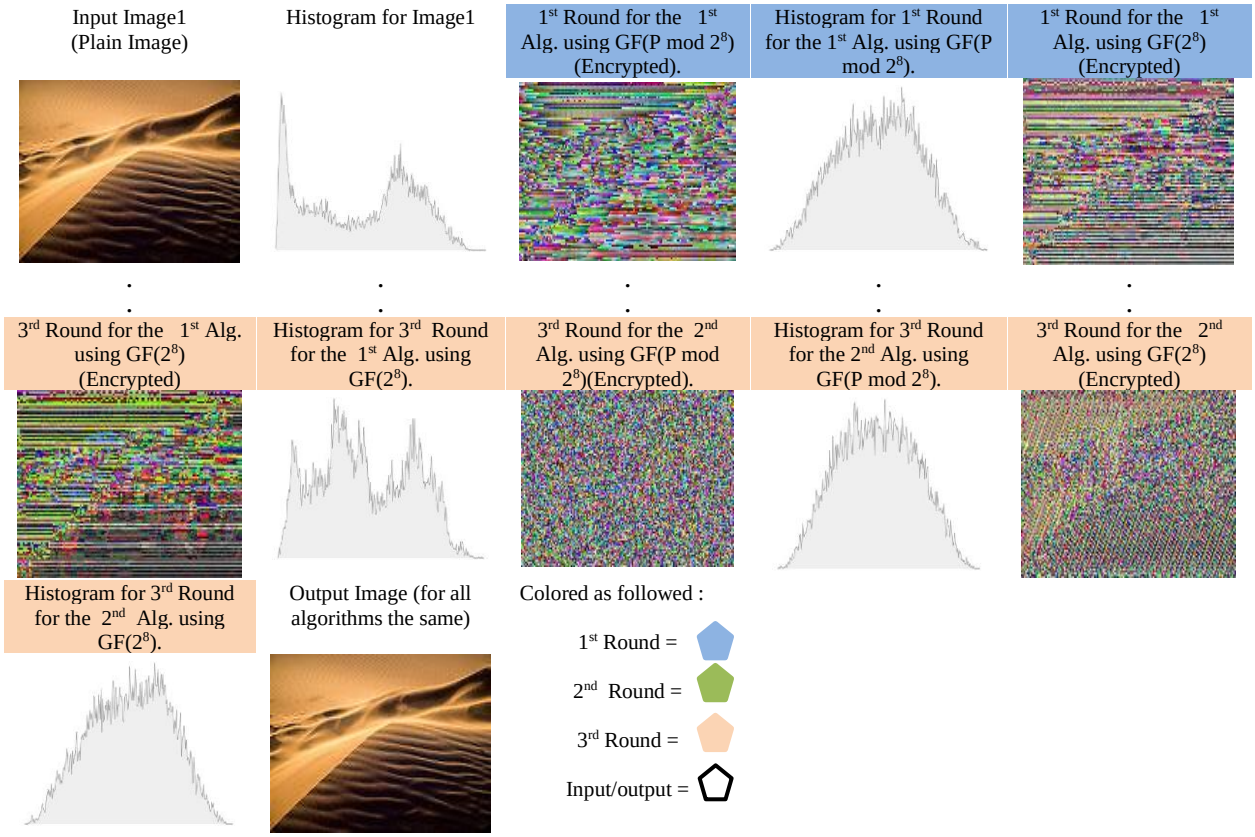

Figure 8. A set of histogram calculations and cipher images for the image 1

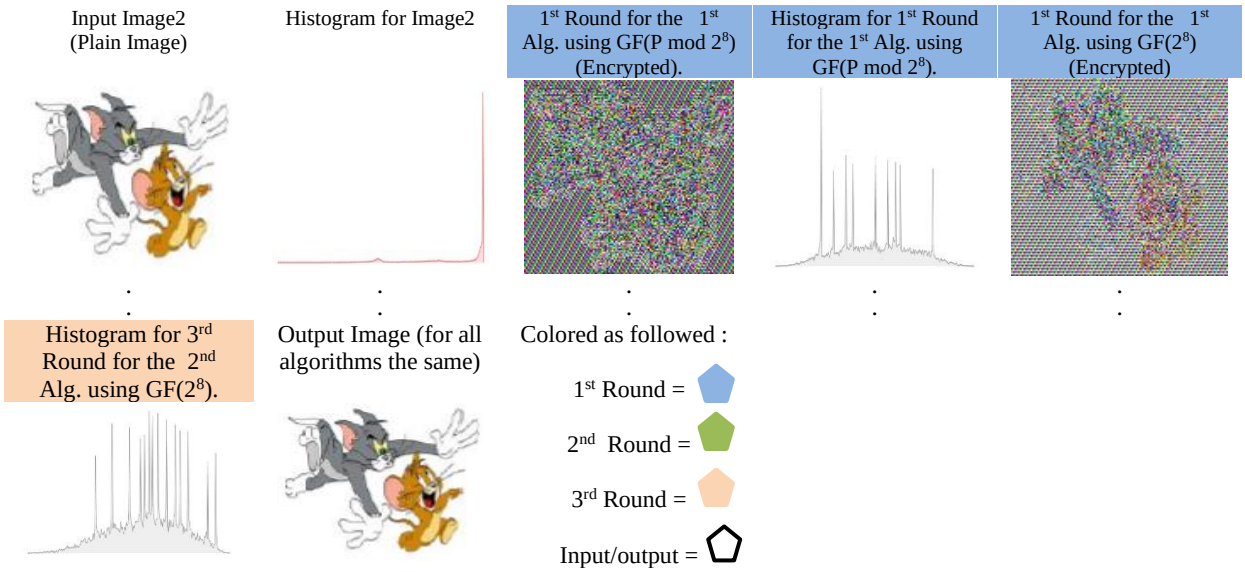

Figure 9. A set of histogram calculations and cipher images for the image 2

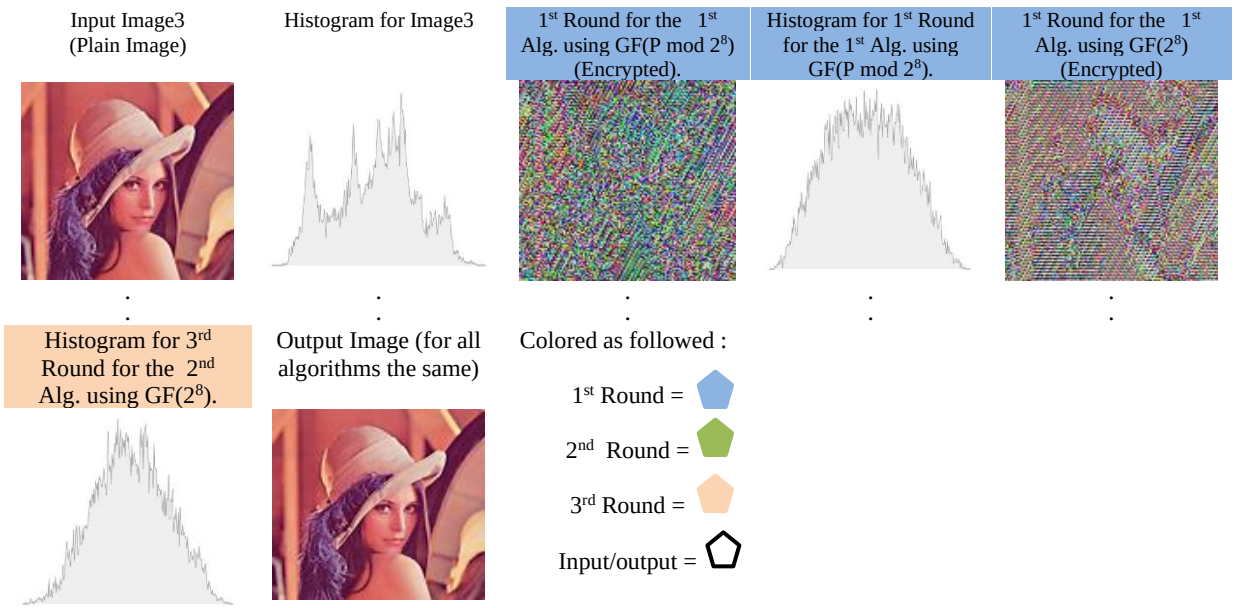

Figure 10. A set of histogram calculations and cipher images for the image 3

4.6. Comparing and discussing all results

By comparing all the previous results with each other, was noted that the new development is much better than its predecessor in terms of complexity, as by comparing the percentage of time increase with complexity, it was noted that the increase in complexity ratio is much more compared to the increase in time between each round. The MS5 is distinguished from the MS3 by increasing the complexity ratio with a small difference in speed, which gives preference to the MS5 with distinction.

The second proposed algorithm is faster than the first algorithm, and this is evident in the big data, while the first algorithm is more complex.

Using GF(2^8) gives a relatively good advantage as it gives faster execution, while using GF(P) is give more complexity.

When using a mask will give extra strength. When using addition in the even rounds it will give speed compared to multiplying in odd rounds. When multiplication is used in odd rounds, it will give a higher complexity compared to using addition in even rounds.
When using an extra mask and using the addition and multiplication operations, some time will be lost, although the increase in complexity is much greater than the time loss.

This proposed cryptography can be utilized as future work to develop intelligent wireless communication along with microstrip filters, antenna and Arduino with effective performance [26-28].

5. Conclusion

The increase in rounds gave an excellent idea. The development of MS5 for MS3 is characterized by increased complexity with little increase in time. Using GF(2^8) gives speed while using GF(P) gives more complexity. The larger the prime number, the more complex. The greater the number of equations used, the higher the velocity is obtained on the opposite side, the complexity will be reduced. Using an extra mask gives an extra complex. Addition is faster than multiplication, but it gives less complexity.

References

[1] R. S. Mohammed, K. K. Jabbar and H. A. Hilal , " Image encryption under spatial domain based on modify 2D LSCM chaotic map via dynamic substitution-permutation network" , International Journal of Electrical and Computer Engineering (IJECE) , 2021.
[2] M. S. Rao , T. Murari , N. D. Priya and K. R. Raghunandand , " Preservation of data using magic squares in Asymmetric key cryptography" ,in materials today proceedings ,2021.
[3] M. Benssalah , Y. Rhaskali and K. Drouiche , "An efficient image encryption scheme for TMIS based on elliptic curve integrated encryption and linear cryptography " , Multimedia Tools and Applications, volume 80, pages2081–2107, 2021.
[4] D. A. Jabbar and A. S. Rahma ,"Proposed Cryptography Protocol based on Magic Square, Linear Algebra System and Finite Field ", Jour of Adv Research in Dynamical & Control Systems, Vol. 10, No. 10, 2018.
[5] S. M. M. Najeeb, S. M. Ali, H. Salim "Finding the discriminative frequencies of motor electroencephalography signal using genetic algorithm," *TELKOMNIKA*, vol. 19, no. 1, pp. 285-291, 2021.
[6] Z. Duan, J. Liu, J. Li and C. Tian ," Improved even order magic square construction algorithms and their applications in multi-user shared electronic accounts" , Theoretical Computer Science 607, 391–410 ,2015.
[7] S. Kaur, P. Bharadwaj and S. Mankotia , "Study of Multi-Level Cryptography Algorithm: Multi-Prime RSA and DES" , I. J. Computer Network and Information Security, 2017.
[8] A. Habboush , "Multi-Level Encryption Framework" , International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 9, No. 4, 2018.
[9] R. H. AL-Hashemy and S. A. Mehdi ,"A New Algorithm Based on Magic Square and a Novel Chaotic System for Image Encryption", J. Intell. Syst ; 29(1): 1202–1215, 2019.
[10] Z. K. Obaidand and N. F. Al Saffar , "Image encryption based on elliptic curve cryptosystem" , International Journal of Electrical and Computer Engineering (IJECE) ,Vol. 11, No. 2, pp. 1293~1302, 2021.
[11] S. D. Mohammed and T. M. Hasan , " Cryptosystems using an improving hiding technique based on latin square and magic square ", Indonesian Journal of Electrical Engineering and Computer Science, Vol. 20, No. 1, pp. 510~520,2020.
[12] S. Cichacz and T. Hincbc , "A magic rectangle set on Abelian groups and its application" , Discrete Applied Mathematics , Volume 288, Pages 201-210 , 2021.
[13] N. A. Hussein. H. A. Naman, M. Al-dabag, H. Salim, "Encryption System for Hiding Information Based on Internet of Things," International Journal of Interactive Mobile Technologies (iJIM), vol. 15, no. 2, 2021.
[14] S. M. Kareema and A. S. Rahma, "A new multi-level key block cypher based on the Blowfish algorithm" , Telkomnika Telecommunication, Computing, Electronics and Control , Vol. 18, No. 2, pp. 685~694 , 2020.
[15] I. M. Alattar and A. S. Rahma, " New Cryptography Algorithm Based On Magic Square Order Five for GF(P) and GF(28) Data ",in Conference: Journal of Physics: Conference Series, Publisher: IOP Publishing, Musol, Iraq, (under publication).

[16] D. Y. Khudhur, S. S. Hameed and S. M. Al-Barzinji , "Enhancing e-banking security: using whirlpool hash function for card number encryption " , International Journal of Engineering & Technology , 7 (2.13) , 281-286 , 2018.
[17] V. Nandalal and V. Anand Kumar, " Design and Analysis of (5, 10) Regular LDPC Encoder Using MRP Technique", Wireless Personal Communications ,volume 118, pages1295-1311, 2021.
[18] H. T. Salim, N. A. Jasim, "Design and Implementation of Smart City Applications Based on the Internet of Things," International Journal of Interactive Mobile Technologies (iJIM), vol. 15, no. 13, pp. 4-15, 2021.
[19] W. Stallings, "Cryptography and network security: principles and practice 6 Edition," Person Education Inc, 2014.
[20] H. Alrikabi, and H. T. Hazim,"Enhanced Data Security of Communication System using Combined Encryption and Steganography," International Journal of Interactive Mobile Technologies, vo.15, no. 16, 2021.
[21] M. S. Rani , G. G. Mary and K. R. Euphrasia , "Multilevel Multimedia Security by Integrating Visual Cryptography and Steganography Techniques" in Conference: Computational Intelligence, Cyber Security and Computational Models pp 403-412 , the Advances in Intelligent Systems and Computing book series (AISC, volume 412), 2015.
[22] Roa'a, I. A. Aljazaery, S. K. Al_Dulaimi, H. T. S. Alrikabi, and Informatics, "Generation of High Dynamic Range for Enhancing the Panorama Environment," *Bulletin of Electrical Engineering*, vol. 10, no. 1, 2021.
[23] A. S. Hussein, R. S. Khairy, S. M. M. Najeeb, and H. ALRikabi, "Credit Card Fraud Detection Using Fuzzy Rough Nearest Neighbor and Sequential Minimal Optimization with Logistic Regression
[24] O. A. Dawood , A. S. Rahma and A. J. Abdul Hossen ," New Variant of Public Key Based on DiffieHellman with Magic Cube of Six-Dimensions" , IJCSIS, Vol. 13, No. 10, 2015.
[25] I. Loth, B. Kargoll and W. Schuh , "Non-Recursive Representation of an Autoregressive Process Within the Magic Square" , pp 183-189 , the International Association of Geodesy Symposia book series ,(IAG SYMPOSIA, volume 151), 2019.
[26] S. Shandal, Y. S. Mezaal, M. Kadim, and M. Mosleh, "New compact wideband microstrip antenna for wireless applications," Adv. electromagn., vol. 7, no. 4, pp. 85–92, 2018.
[27] Y. S. Mezaal, and H. T. Eyyuboglu. "Investigation of new microstrip bandpass filter based on patch resonator with geometrical fractal slot, " *PloS one,* vol.11, no. 4, e0152615, 2016.
[28] Z.K. Hussein, H.J. Hadi, M.R. Abdul-Mutaleb, Y.S. Mezaal, "Low cost smart weather station using Arduino and ZigBee." Telkomnika , vol.18, no. 1, pp.282-288, 2020.