DOI: https://doi.org/10.33103/uot.ijccce.21.2.8

A Comparative Study of Researches Based on Magic Square in Encryption with Proposing a New Technology

Ibrahim Malik ALattar[1] , Abdul Monem S. Rahma[2]
[1, 2] *Department of Computer Science, University of Technology, Baghdad, Iraq.*
[1]*ibrahiminter@yahoo.com,* [2]*110003@uotechnology.edu.iq*

Abstract— *This paper aims to develop a new cryptographic algorithm that is based on the magic square method of order five with multi message lengths to be more complex in order to increase the complexity; in addition to comparing the cipher with the use of the magic square of order five, four and three (all single message length. The proposed work has been done by using two extra rounds and depending on round statuse (even or odd) , messages are detected to be used. The key is placed in agreed positions, then the remaining positions are filled with the message, and then certain sums are calculated to represent the encrypted text. Speed, complexity, histogram calculations for images, and NIST calculations for texts were calculated, and the results were compared, where the complexity of the algorithms was as follows* $((P)^{15} \times (256)^{10})^2 \times (P)^{11} \times (256)^{14}$ *and* $((256)^{15} \times (256)^{10})^2 \times (256)^{11} \times (256)^{14}$ *for GF(P) and* $GF(2^8)$ *respectively , From that, it has been discovered that the proposed algorithm (Magic Square of order five with multi message length) is better than the rest of the algorithms as it has excellent complexity and a slight difference in the speed.*

Index Terms— *Cryptography,* $GF(2^8)$*, linear equation system, Magic Square.*

I. INTRODUCTION

The term magic square is very old, as it was over 2000 years ago. Magic squares appeared first in China, then moved to Japan, then to India, and to the Arabs, and then to Europe [1].

In the early uses of the magic squares, they were used in magic and witchcraft; then, they were used in several fields, the most important are astronomy, mathematics, number theory, and cryptography [2].

It was used in some entertaining games like chess, as the movement of the horse in the game of chess is based on the concepts of the magic squares, and most of the entertainment and intelligence games were based on the idea of magic squares such as Sudoku and others[3].

Mathematicians and cryptologists have developed algorithms and methods based on the magic squares of order three (MS3) where it takes numbers between 1 and 9, the magic square of order four (MS4) takes numbers between 1 and 16. The magic square of order five (MS5) takes numbers between 1 and 25 and so on[4].

Received 19/4/2021; Accepted 8/6/2021

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.21.2.8

Invertible matrix has been adopted in advanced encryption, which has been considered as a time-consuming process. The search based on magic squares has been developed to speed up time and get rid of the time consumption, and at the same time, it depends on matrices as well[10].

In this paper, the use of the properties of magic squares and their implementations and results in mathematics and encryption will be observed , also a new presentation of a developed algorithm based on MS5 is proposed.

Some previous works that are related to the proposed study will be presented, and a comparison will be made amongst them.

In 2014, Dharini , Devi and Chandrasekar proposed an encryption algorithm to protect data in Cloud computing using magic square and RSA algorithm [5].

In 2016, Dawood , Rahma and Abdul Hossen developed a new technology to build the magic cube using the magic square and its properties. It takes place regardless of the size or arrangement of the used magic square [6].

In 2020, Mohammed and Hasan developed an encryption algorithm based on its magic square work by removing duplicates, where a main magic square was used with the help of 16 secondary magic squares of order 3 × 3[7].

In 2020, Li , Liu and Chen conducted a study on magic squares and their correlation to mathematics and coding and linked them to the problems of student group learning[8].

II. Previouly Existing Technologies that have been Relied upon

Magic squares have a set of features that distinguish them and give them the magic advantage. For example, when any of its rows columns or diagonals are summed, they are equal and can be called the magic constant or magic sum. Another advantage of the magic squares is when switching a row or column that is far from the center by N with another row or another column that is equally far from the center. It remains a magic square, in addition to preserving its properties [9].

The use of magic squares in encryption mainly depends on the known features of magic squares, but the difference is that the magic sum is not required to be equal for each row sum, column sum, or diameter sum[10].

Moreover, the transition has been made from the unspecified numbers to the specified numbers, as all numbers in the magic square ,that have been used in the encryption, depending on a prime number [11].

Since the prime numbers do not include all natural numbers (positive numbers in addition to zero), which means that the majority of the natural numbers are not prime numbers, leading to a difficulty in retrieving all the original numbers in the case of the decryption (this thing is somewhat clear in the images and when using a smaller prime number From 256) and prompted cryptographers to replace the decimal numbers with the polynomials [12].

The polynomial numbers are specific numbers and mainly depend on an irreducible polynomial. All the numbers in the magic square are smaller than the irreducible polynomial that is used when performing both the multiplication and addition operations of the polynomial numbers [11].

The polynomial numbers are in $GF(2^8)$, where the polynomial numbers are X raised to the power of a natural number, and (2^8) is used because the currently used devices are mainly dependent on the 8 bit systems [13].

Received 19/4/2021; Accepted 8/6/2021
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.21.2.8

The resulting summations have been considered a system of linear equations and are solved using the known mathematical methods. The Gauss elimination was also used to reach the original message when decrypting the ciphertext; however, before solving the resultant equations, they have to be arranged so that the main diagonal is not equal to zero in each location [14].

Cryptography is a science which is used when transferring data between two parties in two different locations to maintain the integrity of the data without modifying or deleting the data in it. It consists of two processes: the encryption used when sending data, and the decryption is retrieving the original data after receiving the encrypted message, so, before decryption, the data is unreadable[15].

In this paper, the proposed system was made to include different types of data, text, and images of various kinds, including the colored images, and also two types of GF that have been used: the GF(P) and GF(2^8).

III. The Block Cryptography Technoque that is Based on MS3 and MS4.

A. Magic Square of Order 3.

In this case, MS3 will contain the numbers from 1 to 9, so the number of digits that the message contains will be 6, which is equal to the number of the equations and the remaining positions of the key will be only 3, as shown in *Fig*.1 below [16].

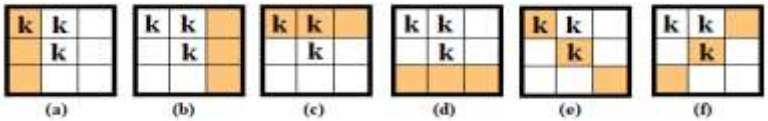

FIG.1.THE EQUATIONS USED IN MS3.

The encryption process will be completed on the message by repeating the process along MS3 (see Appendix for more details). The sums resulting from the equations will be considered the encrypted text, and their number will be equal to the number of the message sites[1].

As for the decoding process, the key locations will be placed in the specified locations, and the message locations will be known, but its values are unknown. However, the known information is the encrypted text, which is represented by the summations that is resulted from the encryption process and its number will be equal to the number of the unknowns[4].

Because the key positions are fixed, the arrangement of the equations will be static (has one case) because the arrangement requires that the main diameter does not contain the value zero[11].

After that, the equations will be solved by the Gaussian elimination[18]. Furthermore, the final result will be the original data[14].

B. Magic Square of Order 4.

In the case of MS4, the numbers can be from 1 to 16, and the sites that will be occupied by the message will be half of them, i.e., 8 locations, and the rest of the 8 positions will be occupied by the keys locations, as shown in *Fig* .2[17].

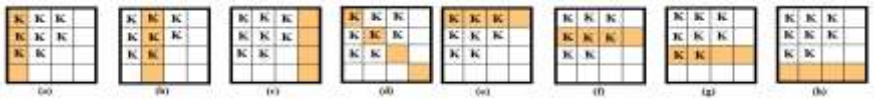

FIG.2. THE EQUATIONS USED IN MS4.

Received 19/4/2021; Accepted 8/6/2021

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.21.2.8

Similarly to the MS3, the process will be repeated using the MS4 along the length of the text that requires to be encrypted, which means that the operation will be repeated several times until all the text is finished[3].

Where 8 sums are obtained each time, and these sums represent the ciphertext[2]. Likewise, as in MS3, the decoding process will be performed by placing the key in the specified positions first, and the remaining sites will be unknown, and their number is equal to the number of the equations (i.e., the encrypted text)[11].It is solved after arranging it by the Gaussian elimination (see the appendix for more details), which results in obtaining the message[14].

The statistical evaluation of NIST test will be according to a book A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications [19].

IV. The Proposed MS of Order 5 with Multi Message Size.

In this case, for using MS5, two types of methods were be used, the first method uses 10 as the length of a message (MS5-L10) and the remaining are 15 key positions, the second uses 14 as the length of a message (MS5-L14), and the remaining are 11 key positions, using MS5 means that it contains the numbers from 1 to 25. *Fig.* 3 illustrates the first revised method, MS5-L10.

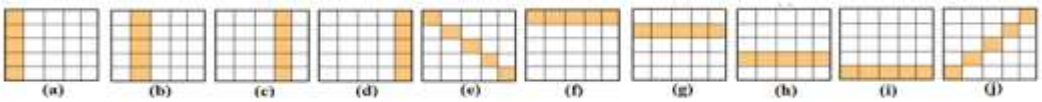

FIG.3. THE EQUATIONS USED IN MS5 WITH MESSAGE LENGTH=10.

In the second suggested method, the same equations have been used as in the first method (the ten equations) will be used, and 4 other equations will be added to them so that the total = 14 equations, the added equations are illustrated in *Fig.* 4.

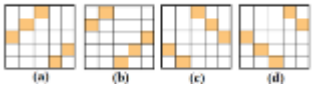

FIG.4. THE EXTRA EQUATIONS ADDED USING MS5 WITH MESSAGE LENGTH=14.

In both cases of the algorithms, the two parties will have the flexibility to choose the key locations. For example, it has been assumed that the key locations were chosen randomly as in the *Fig.* 5.

FIG.5. THE KEYS POSITIONS WERE CHOSEN IN MS5 (A-MESSAGE LENGH=10,B-MESSAGE LENGTH=14).

Likewise, similarly to MS3 and MS4, the process will be repeated several times over the entire length of the text (or image) to be encoded.

Thus, in the first method, there will be 10 sums formed, and in the second method, there will be 14 sums, and the results will represent the encoded text that is sent to the second party (i.e., the recipient).

Received 19/4/2021; Accepted 8/6/2021

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.21.2.8

In turn, the second party will receive the encrypted text while having the (secret) key, which will be placed in the positions that have been agreed upon, which also serve as another key, and the remaining positions will be unknown, and their number is equal to the number of the used equations.

The equations will be arranged in any way (in this paper, they were solved by the suggested method Alattar, which will be mentioned later in this paper), then the equations will be solved to obtain the original text (or picture).

The new development includes the use of a MS5 by adding two additional rounds, if the round number is even then the length of a message = 10 is used, otherwise the length of a message = 14 will be used. It should be noted that the length of the message in this case will be 70 or its multiples . The proposed algorithm can be described as follows:

Algorithm 1-a : Symmetric cipher based on MS5 – Suggested Algorithm for Encryption
Input : Plaintext (Iamge Or Text) , Key value and Positions.
Output : CipherText.
Begin:

For i = 0 to 2
If (i = even)
Messege length = 10;
Else
Message length = 14;
Put the key positions at the agreed position in MS5.
If (i=0)
The remaining Positions will fill with the message.
Else
Put the result (Sums) of Round (i-1) in the remaining positions.
Find the sum for each Row , Column and diagonal in MS.

The final result will represent the Ciphertext.
End.

Algorithm 1-b : Symmetric cipher based on MS5 – Suggested Algorithm for Decryption
Input : CipherText, Key value and Positions.
Output :PlainText(Image or Text).
Begin:

For i = 2 to 0
If (i = even)
Messege length = 10;
Else
Message length = 14;
put the key in the agreed positions.
by having the Keys values and the cipherText (if i=0) OR the final result of (i-1), will have equations equal to the number of Length of message.
Rearrange the equations by the suggested method (Alattar) or any other Methods.
solve the arranged equations by the gauss elimination or any other method.

And the final Result will represent the PlainText (Image Or Text).
End.

Received 19/4/2021; Accepted 8/6/2021

 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.21.2.8

- **The Suggested Method for Arranging the Equation Before Solving it (Alattar Method).**

There is no fixed text for the algorithm to work. Still, as much as possible, some steps have been determined to describe the proposed algorithm, and some steps can be added or minimized according to the required case, and the proposed description can be summarized as follows:

Algorithm 2: Alattar Algorithm for Rearrange the equations

Input: Matrix with order n×n

Output: arranged matrix with diagonal does not contain zero

Step1: $for\ the\ input\ Matrix = \begin{cases} location\ of\ [i,j] & \text{if not equal zero} \\ -1 & otherwise \end{cases}$

Step2:

- Find the sum of Locations for each column which values not equal -1**;**
- Find the smallest sum of them;
- If (sum==1){
  put the value of the position in the new matrix Z as the location found ;
  Exchange the value in the Main Matrix by -1;
  Replace the values for all that row by -1;}

Step3:

while (the Matrix all != -1)**{**

- find the sum of Locations for each row which values not equal -1;
- Find the smallest sum of them with the condition !=0;
- In that row(have smallest sum) find the first value which != -1 ;
- put the value of the position in the Matrix Z as the location found ;
- Exchange the value in the Main Matrix by -1;
- Replace the values for all that column by -1;
- Replace the values for all that row by -1; **}**

Step4: the result of Step3 will be Matrix Z, and according to it will arrange the Main Matrix.

Where the arrangement of equations is the preparation of work for solving equations by Gaussian elimination, as the solution using Gaussian elimination is only possible when the equations are arranged (For more details on the use of the proposed algorithm, see the appendix).

V. Evaluation

Cryptography: It is the process by which information is transferred from one side to the other under three guarantees, which are: availability, integrity, and confidentiality. Furthermore, a key is used during this process, and it is private and only known by two mutual parties. Where in the encryption process, the sum of key values is added to the values of the message, and the resulted (encrypted) text is sent. In return, in the decoding process, the message will be extracted from the encrypted text with the help of the key (known to both parties).

In this part, results will be compared for MS3, MS4, and MS5. It includes calculations of speed and complexity, as well as NIST calculations for the text and histogram of the images, and comparing the final results together.

Results and stats were measured using a Dell laptop, with processor Intel(R) Core(TM) i5-4310M CPU, the OS are Windows 10, and the language used when programming is C#, Visual Studio 2013.

Received 19/4/2021; Accepted 8/6/2021

 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.21.2.8

A. Brute Force Complexity Comparison for the Algorithms and Methods.

First, the key complexity is calculated for each algorithm, which represents the brute force attack strength.

For MS3 using GF(P) the force of the brute force attack will be the value of the prime number that has been raised to the power of the number of key positions represented by 3 Key values . As for the brute force attack, the force of MS3 using GF(2^8) will be 256, raised to the value of the power equal to the number of keys used which is 3 keys .

As for MS4 using GF(P), the force of the brute force attack will be the prime number chosen raised to the power that equals the number of keys, which is represented by 8 , but by using GF(2^8). The force of the brute force attack will be equal to 256 raised to value equal to the number of keys used (8 keys) .

As for MS5 message length = 10 using GF(P), the brute force attack strength will be equal to the prime number raised to 15 , but with GF(2^8) the brute force attack strength will be 256 raised to the number of keys used .

As for the length of the message = 14 using GF(P), the brute force attack strength will be the value of the prime number that has been chosen, raised to the exponent of the value of the number of keys (11 keys) , but by using GF(2^8) the brute force attack, strength = 256 raised to the power of the number of keys .

As for the suggested algorithm (the length of the message = 70) by using GF(P) , the brute force attack strength will be the value of the prime number that has been chosen , raised to the exponent of 15 twice (For rounds 0 and 2) multiplied by the value of the prime number that has been chosen , raised to the exponent of 11 (For round 1) as in (1) , but by using GF(2^8) the brute force attack, strength = 256 raised to the power of 15 twice multiplied by 256 raised to the power of 11 as in (2).

$$C1 = ((P)^{10})^2 \times (P)^{14} \quad (1)$$

$$C2 = ((256)^{10})^2 \times (256)^{14} \quad (2)$$

B. The General Complexity Comparison for Algorithms and Methods

The overall complexity in each algorithm will be the complexity of the key (brute force attack force) multiplied by the complexity of the text as follows.

For MS3, the complexity of the text will be the ASCII code that has been used in the text, represented by 256 raised to the number of message locations that are represented by 6 locations.

The overall complexity will be the text complexity, multiplied by the key complexity of each type GF .

Regarding MS4, the complexity of the text will be 256 raised to the exponent of the number of message sites, which is represented by 8 sites, while the total complexity will be the brute force attack force multiplied by the complexity of the text in each case GF.

As for MS5, the length of the message = 10, the complexity of the text will be 256 raised to exponent the number of message sites, and the total complexity will be the complexity of the text, multiplied by the complexity of the brute force of each type of GF as in (3) and (4). The same applied to the length of the message = 14, as in the length of the message = 10, and the difference is only in the number of locations of the message, see (5) and (6).

$$C1 = (P)^{10} \times (256)^{15} \quad (3)$$

$$C2 = (256)^{10} \times (256)^{15} \quad (4)$$

Received 19/4/2021; Accepted 8/6/2021

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.21.2.8

$$C3 = (P)^{14} \times (256)^{11} \quad (5)$$

$$C4 = (256)^{14} \times (256)^{11} \quad (6)$$

As for MS5 (the suggested algorithm) , the length of the message = 70 , the complexity will be 256 raised to exponent of 10 twice multiplied by 256 raised to exponent of 14, and the total complexity will be the complexity of the text, multiplied by the complexity of the brute force of each type of GF as in (7) and (8).

$$C5=((P)^{15}\times(256)^{10})^{2}\times(P)^{11}\times(256)^{14} \quad (7)$$

$$C6=((256)^{15}\times(256)^{10})^{2}\times(256)^{11}\times(256)^{14} \quad (8)$$

All the methods will be compared in terms of strength as in the following Figures:

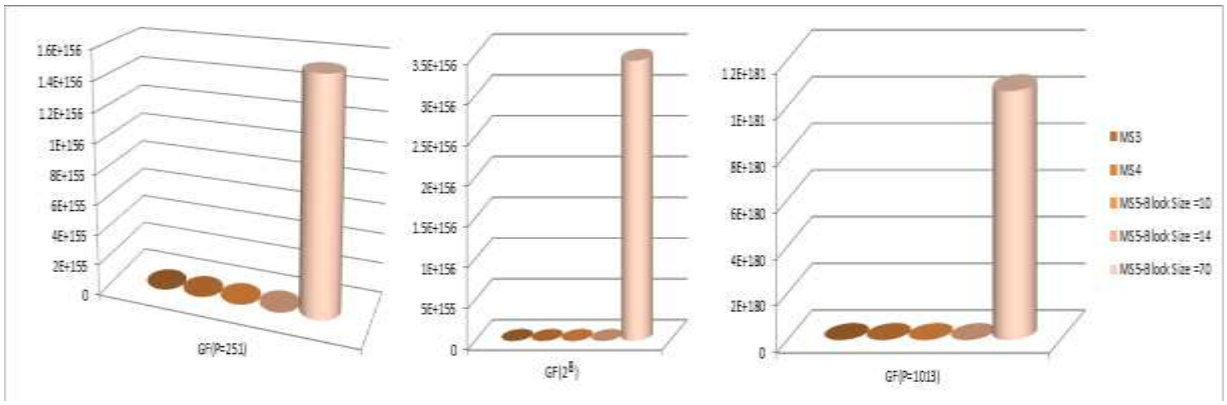

FIG.6. COMPARING THE COMPLEXITY IN ALGORITHMS USING DIFFERENT GF TYPES.

It was noticed from the previous Figures that the complexity of the proposed algorithm greatly outweighs the complexity of the rest of the algorithms.

C. The Required Time for Encryption / Decryption

Another important statistic should be calculated to show which algorithm is better in terms of implementation speed. In this part, the time of implementation will be discussed in each of the algorithms in details (Where only the time that has been spent in encryption/decryption was counted and not including printing and other processes).

Received 19/4/2021; Accepted 8/6/2021

 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.21.2.8

TABLE1. THE TIME FOR MS5 FOR DIFFERENT SIZES OF TEXTS.

MS order	Message length	GF	No. of Character	Encryption Time (in m.s)	Decryption Time (in m.s)
5	10	GF(P)	1680	0.0028418	0.0796452
5	10	GF(P)	2800	0.0032565	0.1303993
5	10	GF(P)	3360	0.0034710	0.1561516
5	10	GF(2^8)	1680	0.2543642	0.1374090
5	10	GF(2^8)	2800	0.4421827	0.2128382
5	10	GF(2^8)	3360	0.5010086	0.2625744
5	14	GF(P)	1680	0.0031227	0.0928777
5	14	GF(P)	2800	0.0030387	0.1428336
5	14	GF(P)	3360	0.0031375	0.1857235
5	14	GF(2^8)	1680	0.1792357	0.3095154
5	14	GF(2^8)	2800	0.2972834	0.5285472
5	14	GF(2^8)	3360	0.3582305	0.5891164
5	10,14	GF(P)	1680	0.0040651	0.2394973
5	10,14	GF(P)	2800	0.0054108	0.4123487
5	10,14	GF(P)	3360	0.0059882	0.4774341
5	10,14	GF(2^8)	1680	0.6693480	0.6477219
5	10,14	GF(2^8)	2800	1.1390941	1.1066943
5	10,14	GF(2^8)	3360	1.3868518	1.4092479

TABLE2. THE TIME FOR MS5 FOR DIFFERENT SIZES OF IMAGES.

MS order	Message length	GF	No. of PXLs	Encryption Time (in m.s)	Decryption Time (in m.s)
5	10	GF(P)	150 × 100	0.0218485	24.6415527
5	10	GF(P)	120 × 120	0.0342916	24.5136421
5	10	GF(2^8)	150 × 100	6.7227181	08.0427420
5	10	GF(2^8)	120 × 120	7.0442016	08.7498214
5	14	GF(P)	150 × 100	0.0171467	19.2715916
5	14	GF(P)	120 × 120	0.0164762	19.1560889
5	14	GF(2^8)	150 × 100	4.6880022	09.2143606
5	14	GF(2^8)	120 × 120	5.0188778	10.8444842
5	10,14	GF(P)	150 × 100	0.0512054	07.6893856
5	10,14	GF(P)	120 × 120	0.0520919	1:07.8888713
5	10,14	GF(2^8)	150 × 100	18.6617257	18.5280523
5	10,14	GF(2^8)	120 × 120	17.4524002	18.3929142

D. NIST Tests Analysis

NIST (which is an abbreviation to the National Institute of Standards and Technology) is another statistic test that has been calculated within the evaluation; it includes a group of statistics test that were examined for the two types of GF, as in the table 3.

Received 19/4/2021; Accepted 8/6/2021

 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.21.2.8

TABLE 3. NIST TEST RESULTS FOR A SET OF RANDOM TEXT LENGTH = 200 CHARACTER.

MS order	Length of Message	GF type	Frequency calculate	Cumulative sums calculate	Runs calculate	The longest runs of ones calculate	Approximate entropy calculate	Serial calculate
MS5	10	GF(P)	0.900524	0.629223	0.382076	0.067104	0.602167	0.595074
MS5	10	GF(2^8)	0.790254	0.525486	0.385264	0.026584	0.652162	0.586227
MS5	14	GF(P)	0.802587	0.338189	0.455501	0.018572	0.733585	0.568339
MS5	14	GF(2^8)	0.882545	0.425862	0.412556	0.032153	0.710254	0.492584
MS5	10,14	GF(P)	0.621554	0.315684	0.315745	0.065887	0.515846	0.601547
MS5	10,14	GF(2^8)	0.715496	0.591452	0.395841	0.041589	0.431215	0.541566
	Results		Success	Success	Success	Success	Success	Success

E. Histogram estimations and their details

Histogram calculations were performed for a different set of color images before and after encryption and as shown in *Figs.* 14 -16.

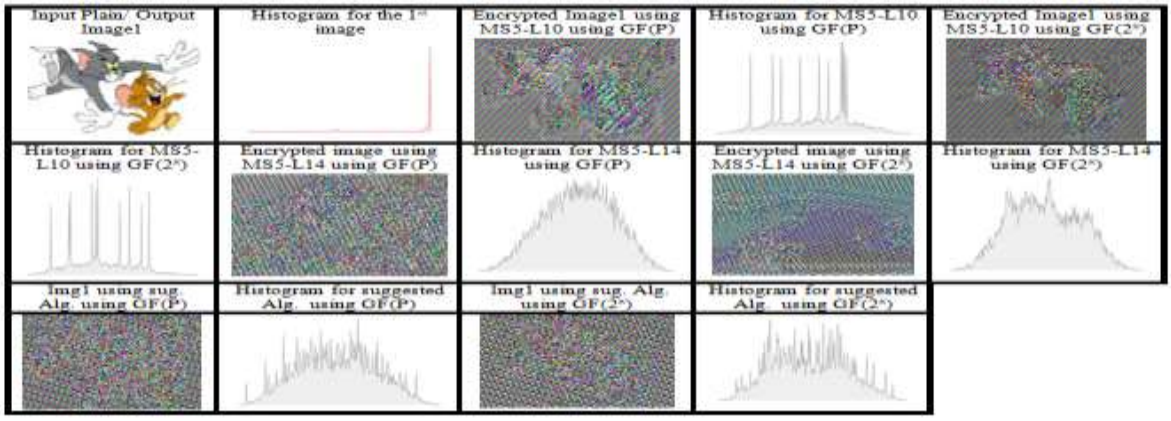

FIG.7. HISTOGRAM USING MS5 FOR IMAGE1 (TOM & JERRY).

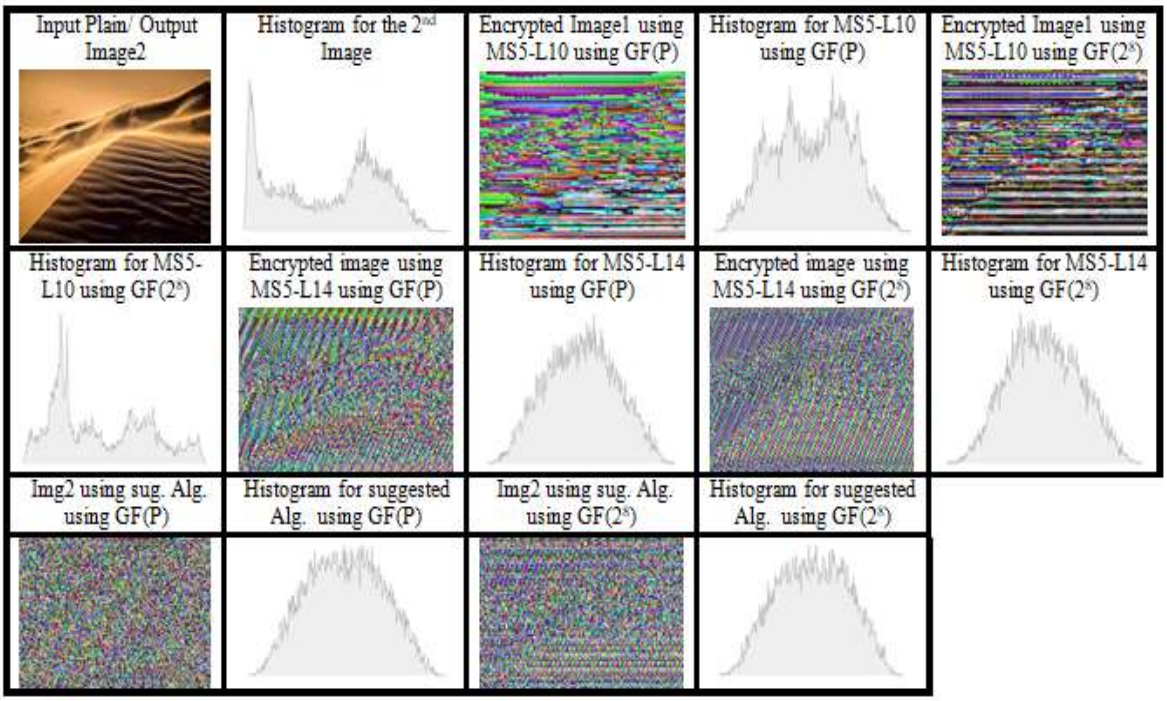

FIG.8. HISTOGRAM USING MS5 FOR IMAGE2 (DESERT).

Received 19/4/2021; Accepted 8/6/2021

 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.21.2.8

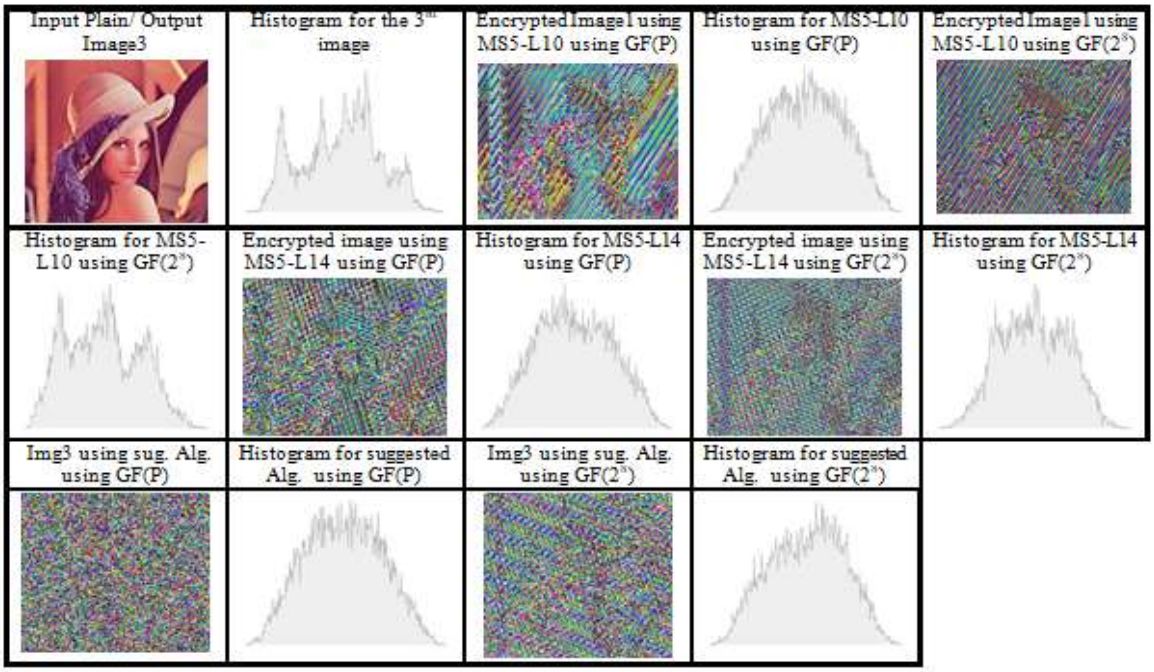

FIG.9. HISTOGRAM USING MS5 FOR IMAGE3 (LENA).

F. Comparisom between Algorithms and the Discussed Results

The comparison between the five algorithms will be summarized in Table 4, where it includes terms of complexity, speed, number of keys positions, number of message positions, and the possibility of the lengths of the message. It can be seen that the MS5 has three possibilities in the size of the message, which are 10 , 14 and multi –size while MS4 and MS3 have only one possibility that is 6 and 8 for each one of them respectively and the two types of GF for all orders of the magic squares.

TABLE4. COMPARING RESULTS FOR ALGORITHMS.

MS Order	GF type	Probability of message lengths	No. Of Message positions	No. Of keys positions	The complexity	The average time for encryption & decryption in M.S
MS3	GF(P)	1	6	3	$(256)^6 \times (P)^3$	27.45215
MS3	GF(2^8)	1	6	3	$(256)^6 \times (256)^3$	07.89478
MS4	GF(P)	1	8	8	$(256)^8 \times (P)^8$	25.76544
MS4	GF(2^8)	1	8	8	$(256)^8 \times (256)^8$	09.14577
MS5	GF(P)	3	10	15	$(256)^{10} \times (P)^{15}$	24.54793
MS5	GF(2^8)	3	10	15	$(256)^{10} \times (256)^{15}$	11.79402
MS5	GF(P)	3	14	11	$(256)^{14} \times (P)^{11}$	19.17257
MS5	GF(2^8)	3	14	11	$(256)^{14} \times (256)^{11}$	15.86336
MS5	GF(P)	3	10,14	15,11	$((256)^{10} \times (P)^{15})^2 \times (256)^{14} \times (P)^{11}$	1:07.94096
MS5	GF(2^8)	3	10,14	15,11	$((256)^{10} \times (256)^{15})^2 \times (256)^{14} \times (256)^{11}$	35.84531

By comparing all the previous and current statistical results, it becomes clear that the complexity in MS5 is greater than MS4 and MS3, as it contains more equations and the size of the magic square is greater. Furthermore, it has been noticed that the increasment of the number of equations will decrease the implementation time. On the other hand, when you increase the size of the magic square, the number of cycles will be decreased, and the

Received 19/4/2021; Accepted 8/6/2021

 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.21.2.8

reason is due to the amount of data that have been truncated in each cycle, and in the case of decreasing the number of the turns, the speed will increase.

Thus, the MS5 is better than the MS4 and the MS3 as it has more complexity, and the difference in the speed is small compared to the increasment in complexity.

CONCLUSION :

By comparing the works together, it appears that the complexity increases in the case of increasing the magic square. In the MS5 method, increasing the number of equations leads to have an increasment in the speed of execution. When using rounds in MS5, the complexity will be double and the increasment in time is relatively small. The use of two different sizes of message in one algorithm gives excellent interference which can cause a high complexity. In term of using GF(2^8) , the MS3 is faster than both the MS4 and the MS5, but in return, it is less complex, and MS4 is faster than MS5 and less complex. In term of using GF(P) , whenever increase the size of the magic square will increase the complexity and decrease the time required to implementation. In other words, MS5 is faster than MS4 and in turn faster than MS3. In any case, for all MS variations in this paper, the percentage of the increasment in the complexity is greater than the increasment in time. As a result, the MS5 is better than the MS4 and the MS3 in cryptography.

REFERENCES

[1] M. S. Rao , T. Murari , N. S. Priya and K.R. Raghunandand , " Preservation of data using magic squares in Asymmetric key cryptography" , materials today proceedings , 2021.

[2] S. Cichacz and T. Hincbc , "A magic rectangle set on Abelian groups and its application" , Discrete Applied Mathematics , Volume 288, Pages 201-210 , 2021.

[3] I. Loth, B. Kargoll and W. Schuh , "Non-Recursive Representation of an Autoregressive Process Within the Magic Square" , IAG SYMPOSIA, volume 151 , 2019.

[4] A. K. Pan , "Semi-device-independent randomness certification using Mermin's proof of Kochen–Specker contextuality" , The European Physical Journal D 75, Article number: 98 , 2021.

[5] A. Dharini, R. S. Devi, and I. Chandrasekar, "Data Security for Cloud Computing using RSA with Magic Square Algorithm", International Journal of Innovation and Scientific Research , Vol. 11 No. 2, pp. 439-444 , 2014.

[6] O. A. Dawood , A. S. Rahma and A. J. Abdul Hossen," Generalized Method for Constructing Magic Cube by Folded Magic Squares ", IJ Intelligent Systems and Applications, 2016.

[7] 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.

[8] H. Li, C. Liu, and S. C. Chen, "A Study of Authenticated Communication Based on Magic Square and Goldbach's Conjecture", INTERNATIONAL JOURNAL OF CIRCUITS, SYSTEMS AND SIGNAL PROCESSING, 2020.

[9] N. Rani and V. Mishra , "Behavior of powers of odd ordered special circulant magic squares" , International Journal of Mathematical Education in Science and Technology , 2021.

[10] A. N. Mazher and J. Waleed ," Implementation of Modified GSO Based Magic Cube Keys Generation in Cryptography" , Eastern-European Journal of Enterprise Technologies, 1(9 (109)), 2021.

[11] S. William, "Cryptography and network security: principles and practice 6 Edition," Person Education Inc, (2014).

[12] W. Lin , Y. Zhao , C. Cui and Z. Cai , " A High-Speed Elliptic Curve Cryptography Processor for Teleoperated Systems Security" , Advanced Control and Applications of Medical Robots , Volume 2021 , 2021.

[13] J. Li , W. Wang , J. Zhang , Y. Luo and S. Ren , " Innovative Dual-Binary-Field Architecture for Point Multiplication of Elliptic Curve Cryptography" , IEEE Access (Volume: 9) , 2021.

[14] V. Nandalal and V. A. Kumar , " Design and Analysis of (5, 10) Regular LDPC Encoder Using MRP Technique" , Wireless Personal Communications volume 118, pages1295–1311 , 2021.

[15] A. S. Rahma and Z. M. Hussein , "Modified the RC4 Stream Cipher Algorithm Based on Irreducible Polynomial", Eng. &Tech.Journal, Vol.33,Part (B), No.4 , 2015.

[16] O. A. Dawood , A.S. Rahma and A. J. Abdul Hossen ," New Variant of Public Key Based on Diffie-Hellman with Magic Cube of Six-Dimensions", (IJCSIS), Vol. 13, No. 10, 2015.

[17] 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.

Received 19/4/2021; Accepted 8/6/2021

 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.21.2.8

[18] R. L. Burden and J. D. Faires , " Numerical Analysis" , ninth edition .

[19] A. Rukhin, J. Soto, J. Nechvatal ,M. Smid , E. Barker , S. Leigh , M. Levenson , M. Vangel ,D. Banks , A. Heckert, J. Dray and S. Vo, "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications", 2008.

Appendix

Full example using MS3 with the use of the suggested algorithm for sorting equations (alattar) with explanation of the gaussian elimination to retrieve the message:

Example using MS3 using key = { 1,2,3} , message ={5,5,5,5,5,5}.
The MS3 will be as shown bellow

1	2	5
5	3	5
5	5	5

Will find the sums according to figure1.
Sum1= 11,Sum2=15,Sum3=8,Sum4=15,
Sum5=9,Sum6=13.
And these sums will represent the ciphertexts.

Decryption , the receiver will have these data in addition to the ciphertext:

1	2	X_1
X_2	3	X_3
X_4	X_5	X_6

Where the unknowns represented by X1-X6.
And from figure 1 will build this matrix if the unknown found will put 1 else put 0 and minus the value from the sum as shown:

X_1	X_2	X_3	X_4	X_5	X_6	The reminder of sum
0	1	0	1	0	0	10
1	0	1	0	0	1	15
1	0	0	0	0	0	5
0	0	0	1	1	1	15
0	0	0	0	0	1	5
1	0	0	1	0	0	10

And according suggested algorithm will sort the equations as shown
Step1

X_1	X_2	X_3	X_4	X_5	X_6
-1	1	-1	3	-1	-1
0	-1	2	-1	-1	5
0	-1	-1	-1	-1	-1
-1	-1	-1	3	4	5
-1	-1	-1	-1	-1	5
0	-1	-1	3	-1	-1

Step2

X_1	X_2	X_3	X_4	X_5	X_6	
-1	1	-1	3	-1	-1	
0	-1	2	-1	-1	5	
0	-1	-1	-1	-1	-1	
-1	-1	-1	3	4	5	
-1	-1	-1	-1	-1	5	
0	-1	-1	3	-1	-1	
3	1	1	3	1	3	Sum of items

And continue in step2
If (sum==1)

X_1	X_2	X_3	X_4	X_5	X_6	
-1	-1	-1	-1	-1	-1	
0	-1	2	-1	-1	5	
0	-1	-1	-1	-1	-1	
-1	-1	-1	3	4	5	
-1	-1	-1	-1	-1	5	
0	-1	-1	3	-1	-1	
3	0	1	2	1	3	Sum of items

Put the index of the equation (0) in Z (the position (1) that the value changed) and other positions in Z remain empty as follow:
Z= { ,0, , , , }
Continue in Step2
If (sum==1)

X_1	X_2	X_3	X_4	X_5	X_6	
-1	-1	-1	-1	-1	-1	
-1	-1	-1	-1	-1	-1	
0	-1	-1	-1	-1	-1	
-1	-1	-1	3	4	5	
-1	-1	-1	-1	-1	5	
0	-1	-1	3	-1	-1	
2	0	0	2	1	2	Sum of items

Z= { ,0,1, , , }
.
.
.
And countinue until reach to
Z= {2 ,0,1,6 ,3,4}
And the matrix will be sorted accorodig to Z as follow

X_1	X_2	X_3	X_4	X_5	X_6	The reminder of sum
1	0	0	0	0	0	5
0	1	0	1	0	0	10
1	0	1	0	0	1	15
1	0	0	1	0	0	10
0	0	0	1	1	1	15
0	0	0	0	0	1	5

The formed matrix will be solve by Gaussian elimination where the values outside the main diameter of the matrix will be eliminated by adding two rows or multiplying by a specific number and depending on GF(P) to reach the following matrix:

X_1	X_2	X_3	X_4	X_5	X_6	The reminder of sum
1	0	0	0	0	0	5
0	1	0	0	0	0	5
0	0	1	0	0	0	5
0	0	0	1	0	0	5
0	0	0	0	1	0	5
0	0	0	0	0	1	5

Then the sums now represent the message.

Received 19/4/2021; Accepted 8/6/2021

 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352