Bulletin of Electrical Engineering and Informatics
Vol. 12, No. 3, June 2023, pp. 1684~1692
ISSN: 2302-9285, DOI: 10.11591/eei.v12i3.4498

An innovative method for enhancing advanced encryption standard algorithm based on magic square of order 6

Suhad Muhajer Kareem[1], Abdul Monem S. Rahma[2]
[1]Department of Computer Science, College of Computer Science and Information Technology, University of Basrah, Basrah, Iraq
[2]Department of Computer Science, Al-Maarif University College, Ramadi, Iraq

Article Info

Article history:

Received Aug 1, 2022
Revised Nov 14, 2022
Accepted Dec 5, 2022

Keywords:

Advanced encryption standard
Cryptography
Histogram
Image encryption
Magic square

ABSTRACT

This paper introduces an improved advanced encryption standard (AES) cipher algorithm by proposing a new algorithm based on magic square to decrease the AES execution time. This is done by replacing Mixcolumn function with magic square of order 6. This paper raises the security level of AES cryptosystem by using another key, which is generated using magic square while decreasing the execution time. For application of encrypting a colouring image, visual studio and MATLAB programs have been used as means for computing results. The results of complexity, time execution, National Institute of Standards and Technology (NIST) tests, histogram, differential attacks and peak signal to noise ratio (PSNR) are computed and compared with the original AES cryptosystem, the original and the proposed algorithms. The proposed algorithm results in reasonable findings under several evaluation metrics. For instance, the complexity of our proposed algorithm is higher than the basic AES while decreases the time execution. The experimental results show that the suggested algorithm provides an efficient and secure way for image encryption. The suggested algorithm leads to leverage the complexity of cipher process as well as to make the linear and differential cryptanalysis harder by pre-process the input image initial step of the proposed AES.

This is an open access article under the CC BY-SA license.

Corresponding Author:

Suhad Muhajer Kareem
Department of Computer Science, College of Computer Science and Information Technology
University of Basrah
Basrah, Iraq
Email: suhad.kareem@uobasrah.edu.iq

1. INTRODUCTION

With the exceptional data communication maturity in network mediums and raising the conqueror's susceptibilities, information security has been the most essential method for data storage and communication [1], [2]. Numerous cipher algorithms are vastly obtainable and applicable for securing information. Cipher algorithms can be categorized into two classes: symmetric (private) and asymmetric (public) key cipher. In symmetric keys cipher, only one key is being applied for encrypting and decrypting. on the other hand, in asymmetric keys, two keys have to be applied; private and a public key. For the public key, it is employed for encryption, whereas the private key is employed for decryption (e.g. Rivest Shamir Adleman (RSA)) [3]–[5]. A public key encryption is based on mathematical operations, which is computationally strong. The data encryption standard (DES) uses (64–bit) key, while advanced encryption standard (AES) uses different 128, 192, 256-bit key where there are many examples of strong and weak keys of encryption algorithms [6], [7].

This paper proposes AES as one type of the strongest symmetric block ciphers. The AES cryptosystem which is known as the Rijndael which was pressed to replace the DES cryptosystem. It stands for AES. Moreover, it is a symmetric block encryption that can encrypt data blocks of 128-bit by using variable keys (128, 192, or 256) depending on the number of rounds [8], [9]. It includes certain processes through the encryption and decryption; these processes take input state as (4×4) matrix which acts 16-byte of data. In this respect, four standard operations being utilized at encryption process. Namely, sub-stitution byte by utilizing the sub-stitution box (S-box), shift-rows, mixing-columns and XORing with round key. In the side of decryption, the inverse of previous steps will be utilized to decrypt input data which are: inv-subbytes, inv-shiftrows and inv-mix-columns in addition to add round key transformation [10]. In key scheduling, the sub keys for number of rounds that are produced and then applied in encryption and decryption [11], [12].

A magic square is defined as a square matrix of integers with the same sum of the values in the rows, columns and main diagonals. The value numbers of magic squares are integers sorted such that the sum of the *n* numbers in any lines (vertical, horizontal, or main diagonal) is constantly the same number. The formula 1/2 m (m^2+1) is applied to compute the sum of magic. Generally, magic squares residue magic if the same positive integer is combined to each number in the square, or each number in the basic square is multiplied by the same number [13], [14]. Examples of magic square are shown as in the Figures 1-3.

1	6	5
8	4	0
3	2	7

Figure 1. Magic square of order 3

1	2	16	15
13	14	4	3
12	7	9	6
8	11	5	10

Figure 2. Magic square of order 4

17	24	1	8	15
23	5	7	14	16
4	6	13	20	22
10	12	19	21	3
11	18	25	2	9

Figure 3. Magic square of order 5

Magic square is of wide application in recreation mathematics like puzzles. So, it can also be applied in cryptography [15]. Lester S. Hill presented Hill Cipher in 1929 that it uses matrix multiplication in encryption and decryption. Simply, Hill Cipher uses matrix multiplication techniques and inverse techniques for matrices [16]. Then, matrix multiplication techniques to be applied in AES algorithm under Mixcolumn step. Since matrix multiplication requires a complex computation process leading to increase execution times in encryption algorithms. In this paper, a novel AES algorithm applies a magic square of order 6 square instead of Mixcolumn function. The proposal focuses on the improvement on decreasing the execution time of AES while increasing the complexity of AES algorithm. This is done by using magic square with another key. This paper also proposes that input image is prepossessed as an initial step to break the correlation between points in images to increase the security of the encrypted image against differential attacks.

The structure of this paper is arranged as follows: the related works and the proposed work are presented in section 2 and section 3 respectively. The experimental results of the proposed algorithms present in section 4. Finally, section 5 is shown some of conclusions.

2. RELATED WORKS

This section lists some of the related works on using magic square in encryption algorithms. Zhang *et al.* [17] presented encryption algorithm that pre-process for the input image based on the magic square transformation. The overall work is a pre-handling on the base of magic square algorithm developed grads. Then, an arnold cat map was utilized to mix the second image. After that, henon technique was used for producing the image's mixed gray values, which converts the positions of images and gray value at the same time to obtain the output encrypted image.

Abugharsa *et al.* [18] suggested a cipher algorithm depending on turning of surfaces of magic square, where the input image is separated into six sub images, then this result sub-images are separated through a number of blocks and connected to surfaces of a magic square. Later, these surfaces to be mixed using turning of the magic square. The rotated image is provided to the AES algorithm used for the pixels of the image to encrypt the mixed image. The algorithm has shown resistance to the statistical and differential attacks. The mixing of rotation magic square and AES algorithm have used the input image to construct triple encrypted images.

Rahma and Jabbar [19] suggested a cipher protocol using magic square of order 3 for encryption and decryption. This work proposes the improvement of encryption algorithms based on the magic square of order 5 and multi level keys with the addition of matrix keys to enhance execution complexity and speed. ALattar and Rahma [20] proposed work completely relying on the magic sum and added some equations as an enhancement on antecedent research. The suggested research was implemented by using both GF (P) and GF (2^8). Experiential results were computed and compared with the magic square of order 3, the complexity modification according to the selection value of N randomness, also to speed, complexity, National Institute of Standards and Technology (NIST) calculations have been implemented for texts and histogram computations for many images were computed and compared as well.

From the above works, it has been observed that the researchers applied magic square in block encryption algorithm. Moreover, the importance and the necessity of using a magic square in encryption algorithms for increasing the security levels. To increase the security levels of encryption algorithms as much as practically possible, we proposed a new encryption scheme comprised of using magic square of order 6 in AES algorithm instead of Mixcolumn. This proposed will result in enhancing AES encryption and decryption times significantly.

3. PROPOSED METHOD

3.1. Magic square order 6 construction

By taking advantages of magic square of order 6 (MS6) property, 14 sum equations can be obtained, where 6 sums are obtained for the columns, 6 for rows, and two for the main and secondary diagonals, as shown in Figure 4. After checking the resulting equations, it has been found that two of them have dependency. Thus; they are isolated, so the equations for the fourth row and columns (4 and 10) are isolated so that the remaining number of them is 12.

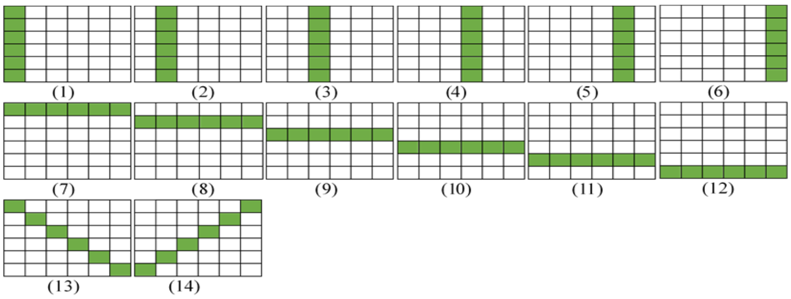


Figure 4. Basic equations obtained from MS6

Depending on the message length that is acceptable in AES algorithm, the length of the message will be 16 bytes and the key will be 20 bytes. To represent the message in MS6, sixteen equations are needed to represent the message. These equations are proposed after examining and analysing equations and canceling equations that have reliance with the remainder (4 and 10 in Figure 4). Additional four equations are required to be added based on the four corners of MS6 as shown in Figure 5. Therefore, the added number of equations will 4 equations. Then, the overall number of equations utilized in this suggested algorithm has become 16 ones, and the residual number is 20 positions for the key that is chosen by the two parties exchanging information, which have flexibility in selected. Furthermore, it is supposed that the locations have chosen as shown in Figure 6.

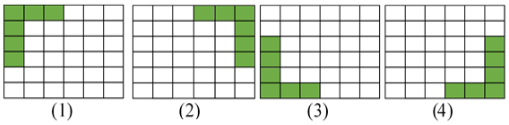


Figure 5. Additional equations added to MS6

K1	K2	M1	M2	K3	M3
M4	M5	K4	M6	K5	K6
M7	K71	K8	K9	M8	M9
K10	K11	M10	K12	M11	K13
M12	K14	K15	M13	K16	M14
K 17	M15	K18	K19	M16	K20

Figure 6. Key and message locations in MS6

Thus, sums which are gained from 16 operations from Figures 4 and 5 are as displayed by the following:

$$Sum1 = K1 + K2 + M1 + M2 + K3 + M3 \tag{1}$$

$$Sum2 = M4 + M5 + K4 + M6 + K5 + K6 \tag{2}$$

$$Sum3 = M7 + K7 + K8 + K9 + M8 + M9 \tag{3}$$

$$Sum4 = M12 + K15 + M13 + K16 + M14 \tag{4}$$

$$Sum5 = K17 + M15 + K18 + K19 + M16 + K20 \tag{5}$$

$$Sum6 = K1 + M2 + M7 + K10 + M12 + K17 \tag{6}$$

$$Sum7 = K2 + M5 + K7 + K11 + K14 + M15 \tag{7}$$

$$Sum8 = M1 + K4 + K8 + M10 + K15 + K18 \tag{8}$$

$$Sum9 = K3 + K5 + M8 + M11 + K16 + M16 \tag{9}$$

$$Sum10 = M3 + K6 + M9 + K13 + M14 + K20 \tag{10}$$

$$Sum11 = K1 + M5 + K8 + K12 + K16 + K20 \tag{11}$$

$$Sum12 = K17 + K14 + M10 + K9 + K5 + M3 \tag{12}$$

$$Sum13 = K1 + M4 + M7 + K10 + K2 + M1 \tag{13}$$

$$Sum14 = M1 + K2 + K1 + M4 + M7 + K10 \tag{14}$$

$$Sum15 = M2 + K3 + M3 + K6 + M9 + K13 \tag{15}$$

$$Sum16 = K19 + M16 + K20 + M14 + K13 + M9 \tag{16}$$

Therefore, there will be 16 message positions (each position matches to an equation) and the residual locations in magic square of order 6 are 20 for the keys. The suggested algorithm does not trap utilize of specific fixed positions, but rather affords elasticity in selecting the position and values of the keys. For instance, it is supposed that the key positions were selection as declared in Figure 6. Afterwards, the sixteen equations will be solved with ten anonymous versus 16 cipher texts to make the input texts of the message (Gaussian elimination were used for solving the equations and the encryption work in this way was also sophisticated utilizing Galois field GF (2^8)).

Algorithm 1. Encryption algorithm based on MS6

```
Input: 16 bytes of message, 20 bytes of key
Output: 16 bytes of cipher text
Begin
Step1: Place message and key bytes at the positions in Magic Square of Order 6.
Step2: Repeat the following steps for a number of rounds:
   Step2.1: Apply multiplication between mask encryption and Magic Square over Galois
                Field.
   Step2.2: Apply summation of Magic Square using the equations (1-16).
   Step2.3: the result of Step2.2 is cipher text
End
```

Algorithm 2. Decryption algorithm based on MS6

```
Input: 16 bytes of cipher text, 20 bytes of key.
Output: 16 bytes of message.
Begin
Step1: Place cipher text and key bytes at the positions in magic Square of Order 6.
Step2: Repeat the following steps for a number of rounds:
   Step2.1: Apply multiplication between inverse mask encryption and Magic Square over
             Galois Field.
   Step2.2: solve sixteen equations of Magic Square using the equations (1-16).
   Step2.3: the result of Step2.2 is message.
End
```

3.2. Proposed AES with magic square (MS6)

As known that the AES cryptosystem suffers from high calculation and computational overhead problems. Subsequently, to overcome such problems. The AES has been analysed to make certain modifications. A good encryption system should be secure against different attacks without additional time in encryption and decryption. This is to decrease the calculation of well-known AES algorithm and get better the encryption efficiency. The AES rounds consist of basic steps: sub byte, shift row, Mixcolumn and add round key. Thus, we improve and execute a proposed AES based on using MS6 instead of Mixcolumn function in encryption and the inverse process in decryption side as explained in Algorithms 1 and 2.

The basic purpose behind the modification of AES is to shorten the time of computating and improving data security by increasing the complexity. The suggested AES algorithm has been modified to provide better-encryption-speed. The proposed AES accepts message block length (128 bit) and the key length (128 bit). The encryption and decryption processes are applied using the basic steps of original AES algorithm, except the Mixcolumn function which is replaced with MS6, as explained in Algorithm 3. So, another key was generated randomly to fill 20 bytes of MS6 to raise the security level of the suggested algorithm. The proposed algorithm can be applied to encrypt colour image. For getting good results to encrypt image, additional initial step is used for breaking the correlations between the points in the input image by applying XORed operation between input image state and image state that generated randomly as shown in Figure 7.

Algorthm 3. The proposed AES

```
Input: Plaintext 128 bit, Key 128 bit
Output: Ciphertext 128 bit
Begin
     step1. Initialize state for plaintext (state (Plt)).
      step2. Permutation step (Plt xor Im).
      step3. Initialize state for key rounds using key schedule (state (Kn))
      step4. Add round key state (Plt xor K0)
      step5. For nine rounds do
        step 5.1 Sub-Byte (State)
          step 5.2 Shift-Row (State)
          step 5.3 Magic Square (State) (section 4.1)
          step 5.4 Add round Key State (Plt Xor Kn)
          End for
     step6. Compute final step as:
         step 6.1 Sub-Byte (State)
         step 6.2 Shift-Row (State)
         step 6.3 Add round Key State (Plt Xor K10)
End
```

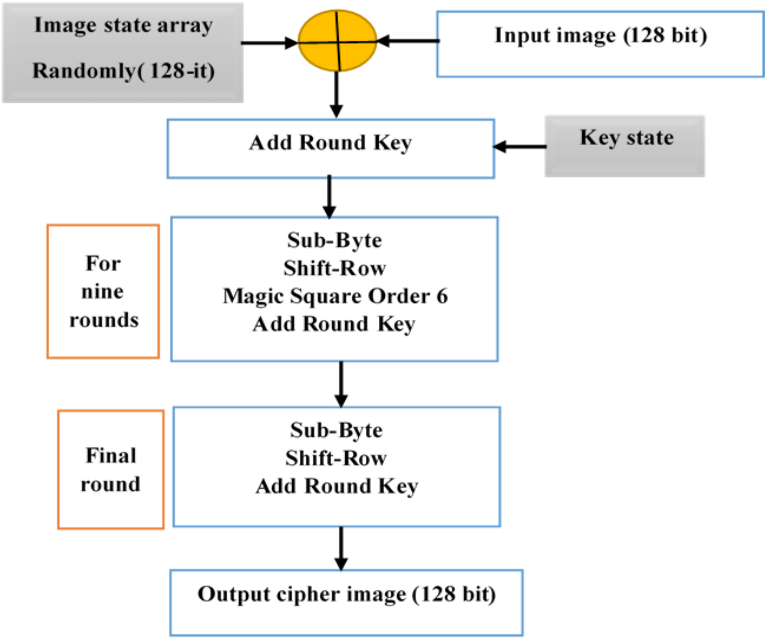


Figure 7. Diagram of the proposed AES for colour image encryption

4. RESULTS AND DISCUSSION

In this section, many of the safety tests are used for testing the accuracy of the suggested algorithm based on complexity, execution time, NIST testing peak signal to noise ratio (PSNR) and differential attacks (number of pixels changes rate (NPCR) and unified average-changing intensity (UACI)) tests to evaluate the performance on encrypted images.

4.1. Complexity

The results complexity is presented as the comparison between the basic AAES technique and our proposed algorithm. The complexity in this section is calculated for magic square of order 6; where the key is randomly selected in range (1-255) and repeated in 20 locations:

$$Complexity\ of\ magic\ square = (K)^{20} \times (255)^{20} \tag{17}$$

Then complexity for AES is computed as:

$$Complexity\ of\ AES\ algorithm\ in\ ten\ rounds = (2^{24} \times 2^{40} \times 2^{16} \times 2^{46})^{10} = (2^{126})^{10} \tag{18}$$

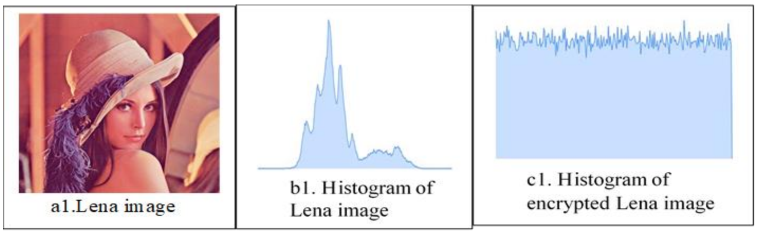
Finally, we computed the overall complexity as (19):

$$Complexity\ of\ the\ proposed\ AES\ algorithm\ with\ magic\ square\ in\ ten\ rounds = (2^{24} \times 2^{40} \times 2^{16} \times 2^{46})^{10} \times (K)^{20} \times (255)^{20} \tag{19}$$

The complexity of our proposed algorithm is more complex than that of well-known AES algorithm as displayed in (19).

4.2. Histogram analysis

Histogram calculations have been made for the distribution of pixels of images, the basic image have disparate distributions while the pixels of encrypted images distributed in regular manner. So, regular histogram is the best to withstand the statistic attacks. The results of histogram are calculated and compared with the basic and encrypted images as shown Figures 8 and 9.

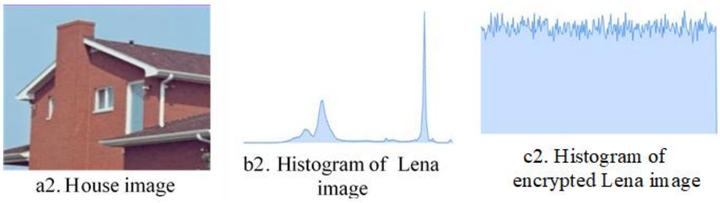


a1.Lena image

b1. Histogram of Lena image

c1. Histogram of encrypted Lena image

Figure 8. Histogram for Lena image



a2. House image

b2. Histogram of Lena image

c2. Histogram of encrypted Lena image

Figure 9. Histogram for house image

4.3. NIST analysis

NIST is an alternative statistic utilized as another security metric to calculate the randomness of encryption system. Experiments are carried on the suggested approaches as stated in the following Table 1. The randomness of the cipher texts is examined using NIST tests which have been applied to the encrypted images utilizing the basic and modified AES algorithms. Furthermore, another random key in each round of the proposed AES rises the randomness and security levels of the algorithm. Table 1 offers the results of the NIST tests that clarify the proposed encryption algorithm which is better-than the basic algorithm in most of the tests.

Table 1. NIST test analysis of proposed algorithm

Test name	For original AES	For proposed AES
Approximate entropy	0.1	0.981
Block frequency	0.001	0.372
FFT	0.041	0.666
Frequency	0.062	0.861
Linear complexity	0.211	0.999
Longest runs	0.173	0.322
Rank	0.260	0.775
Run	0.199	0.946
Random excursions	0.643	0.780
Random excursions variant	0.046	0.683

4.4. Execution times

Execution time is one of the tests that used for measuring the security of the encryption algorithms. The results of execution time have been calculated for the proposed algorithm and then compared with the original algorithm for encrypting three colour images, which finally presented in Table 2 and Figure 10, showing the speed of the proposed algorithm is lower than the original.

Table 2. Speed results of the proposed algorithm

Encrypted image	For original AES (ms)	For proposed AES (ms)
Lena	61	33
Peppers	82	56
House	14	8

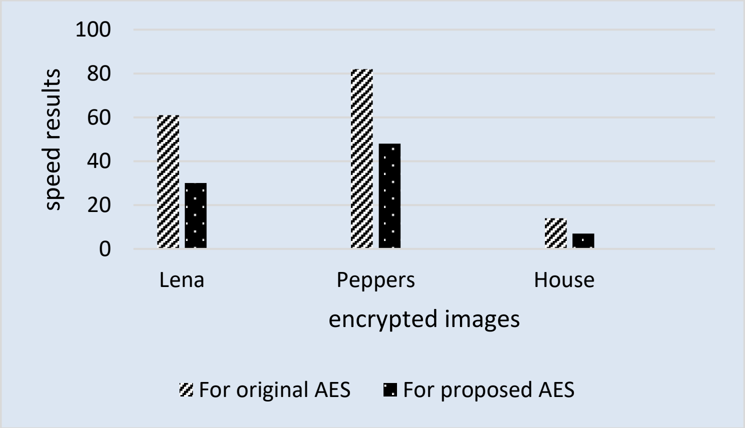


Figure 10. Results of execution time as rapprochement between well-known and suggested AES algorithms

4.5. Differential attack

The good algorithms should be more secure against many attacks such as differential attacks, so the NPCR and UACI are employed as security metrics for testing the influence of one pixel alteration on the full encrypted image, the equations of this metrics referenced in [21], [22]. Table 3 displays the result of differential attacks for the proposed algorithm.

Table 3. Results of differential attacks of proposed algorithm

Encrypted Image	NPCR	UACI
Lena	99.98	33.71
Peppers	99.91	33.78
House	99.99	33.86

4.6. Peak signal to noise ratio

PSNR calculates the similarity between an input image and a retrieved image according to MSSE [23]. The PSNR and MSE equations are referenced in [24], [25]. Table 4 displays the results of PSNR and MSE tests.

Table 4. The results for (PSNR and MSE) test between an input image and a retrieved image

Images	MSE	PSNR
Lena	0.00	Inf dB
Peppers	0.00	Inf dB
House	0.00	Inf dB

5. CONCLUSION

In this paper, a new modification on AES is introduced based on magic square of order 6 by replacing the Mixcolumn function in basic AES with magic square of order 6. The aim of such replacement is to reduce computation complexity in AES and development the safely level of the algorithm. This is accomplished by using another random key used with magic square. From the experimental results, the suggested algorithm has higher complexity and less execution time compared with the original algorithm. Using initial step in the proposed AES as pre-processing of an input image and another random key will increase the randomness of the proposed algorithm as show in the results. Also, the proposed algorithm gives a good result against statistical analysis, such as histogram and differential attacks, such as NPCR and UACI metrics.

REFERENCES

[1] O. K. J. Mohammad, S. Abbas, E.-S. M. El-Horbaty, and A.-B. M. Salem, “Innovative method for enhancing key generation and management in the AES-algorithm,” *International Journal of Computer Network and Information Security*, vol. 7, no. 4, pp. 14–20, Mar. 2015, doi: 10.5815/ijcnis.2015.04.02.

[2] C. A. Sari, G. Ardiansyah, D. R. I. M. Setiadi, and E. H. Rachmawanto, “An improved security and message capacity using AES and Huffman coding on image steganography,” *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 17, no. 5, pp. 2400–2409, Oct. 2019, doi: 10.12928/telkomnika.v17i5.9570.

[3] S. M. Kareem and A. M. S. Rahma, “New modification on feistel DES algorithm based on multi-level keys,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 3, pp. 3125–3135, Jun. 2020, doi: 10.11591/ijece.v10i3.pp3125-3135.

[4] S. P. Kumar, K. N. Kumar, S. Sreenadh, B. Aravind, and K. H. Kumar, “Novel advent for add-on security by magic square intrication,” *Global Journal of computer science and technology*, vol. 11, no. 21, pp. 1–5, 2011.

[5] S. M. Kareem and A. M. 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, Apr. 2020, doi: 10.12928/telkomnika.v18i2.13556.

[6] P. Mahajan and A. Sachdeva, “A study of encryption algorithms AES, DES and RSA for security,” *Global Journal of Computer Science and Technology*, vol. 13, no. 2, pp. 64–69, 2013.

[7] M. A. Albahar, O. Olawumi, K. Haataja, and P. Toivanen, “Novel hybrid encryption algorithm based on AES, RSA, and Twofish for Bluetooth encryption,” *Journal of Information Security*, vol. 9, no. 2, pp. 168–176, 2018, doi: 10.4236/jis.2018.92012.

[8] S. M. Kareem and A. M. S. Rahma, “New method for improving add round key in the advanced encryption standard algorithm,” *Information Security Journal: A Global Perspective*, vol. 30, no. 6, pp. 371–383, Nov. 2021, doi: 10.1080/19393555.2020.1859654.

[9] A. Y. Hindi, “A novel method for digital data encoding-decoding,” *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 18, no. 5, pp. 2772–2779, Oct. 2020, doi: 10.12928/telkomnika.v18i5.14279.

[10] M. E. Hameed, M. M. Ibrahim, and N. A. Manap, “Compression and encryption for ECG biomedical signal in healthcare system,” *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 17, no. 6, pp. 2826–2833, Dec. 2019, doi: 10.12928/telkomnika.v17i6.13240.

[11] S. N. Patil, R. M. Vani, and P. V Hunagund, “Data security using advanced encryption standard (AES) in reconfigurable hardware for SDR based wireless systems,” *International Journal of Computer Engineering and Technology (IJCET)*, vol. 6, no. 1, pp. 95–100, 2015.

[12] A. Arab, M. J. Rostami, and B. Ghavami, “An image encryption method based on chaos system and AES algorithm,” *The Journal of Supercomputing*, vol. 75, no. 10, pp. 6663–6682, Oct. 2019, doi: 10.1007/s11227-019-02878-7.

[13] R. H. AL-Hashemy and S. A. Mehdi, “A new algorithm based on magic square and a novel chaotic system for image encryption,” *Journal of Intelligent Systems*, vol. 29, no. 1, pp. 1202–1215, Feb. 2019, doi: 10.1515/jisys-2018-0404.

[14] 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, Oct. 2020, doi: 10.11591/ijeecs.v20.i1.pp510-520.

[15] M. Maity, “A modified version of polybius cipher using magic square and western music notes,” *International Journal For Technological Research In Engineering*, vol. 1, no. 10, pp. 1117–1119, 2014.

[16] M. D. L. Siahaan and A. P. U. Siahaan, “Application of Hill Cipher algorithm in securing text messages,” *International Journal For Innovative Research in Multidisciplinary Field*, vol. 4, no. 10, pp. 55–59, 2018.

[17] Y. Zhang, P. Xu, and L. Xiang, “Research of image encryption algorithm based on chaotic magic square,” in *Advances in Electronic Commerce, Web Application and Communication*, 2012, pp. 103–109, doi: 10.1007/978-3-642-28658-2_16.

[18] A. B. Abugharsa, A. Samad, B. Hasan, and H. Almangush, “A novel image encryption scheme using an integration technique of

blocks rotation based on the magic cube and the AES algorithm," *International Journal of Computer Science Issues*, vol. 9, no. 4, pp. 41–47, 2012.

[19] A. M. S. Rahma and D. A. Jabbar, "Development cryptography protocol based on magic square and linear Algebra system," *Journal of Al-Qadisiyah for computer science and mathematics*, vol. 11, no. 1, pp. 72–75, 2019, doi: 10.29304/jqcm.2019.11.1.470.

[20] I. M. ALattar and A. M. S. Rahma, "A new block cipher algorithm using magic square of order five and galois field arithmetic with dynamic size block," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 15, no. 16, pp. 63–78, Aug. 2021, doi: 10.3991/ijim.v15i16.24187.

[21] B. Yousif, F. Khalifa, A. Makram, and A. Takieldeen, "A novel image encryption/decryption scheme based on integrating multiple chaotic maps," *AIP Advances*, vol. 10, no. 7, pp. 1–9, Jul. 2020, doi: 10.1063/5.0009225.

[22] H. Khanzadi, M. Eshghi, and S. E. Borujeni, "Image encryption using random bit sequence based on chaotic maps," *Arabian Journal for Science and Engineering*, vol. 39, no. 2, pp. 1039–1047, Feb. 2014, doi: 10.1007/s13369-013-0713-z.

[23] N. Thakur and S. Devi, "A new method for colour image quality assessment," *International Journal of Computer Applications*, vol. 15, no. 2, pp. 10–17, Feb. 2011, doi: 10.5120/1921-2565.

[24] N. Mahendiran and C. Deepa, "A comprehensive analysis on image encryption and compression techniques with the assessment of performance evaluation metrics," *SN Computer Science*, vol. 2, no. 1, pp. 1–12, Feb. 2021, doi: 10.1007/s42979-020-00397-4.

[25] A. Susanto, I. U. W. Mulyono, M. R. F. Febrian, and G. A. Rosyida, "A combination of Hill Cipher and LSB for image security," *Scientific Journal of Informatics*, vol. 7, no. 1, pp. 155–165, Jun. 2020, doi: 10.15294/sji.v7i1.24393.

BIOGRAPHIES OF AUTHORS

Suhad Muhajer Kareem she is lecture at College of Computer Science and Information Technology, University of Basrah, Iraq. She holds a Ph.D degree in Computer Science with Data Security. Her research areas are image/signal processing, security, data mining and text mining. She can be contacted at email: suhad.kareem@uobasrah.edu.iq.

Prof. Abdul Monem S. Rahma have an extensive background in the field of Cryptography and Information Security. In 1984, he received his Ph.D in Computer Science from the Loughborough University of Technology in the United Kingdom, and become a professor in Computer Science since 2008. He was the Deputy Dean of the Department of Computer Science, University of Technology, Baghdad, Iraq from 2005 to 2013; and then from 2013 to 2015 become the Dean of the department. Now Prof. Rahma the head of the Department of Computer Science, Al-Maarif University College, Anbar Iraq. He can be contacted at email: monem.rahma@uoa.edu.iq.