# A New Encryption Algorithm for Voice Messages on Social Media Using Magic Cube GF (2^8) Technology

Original Scientific Paper

**Mohammed M. Al-Ezzi***
School of Computer Science and Engineering,
Central South University, China
mohd_soft2006@yahoo.com

Ministry of Higher Education and Scientific Research,
Baghdad, Iraq

**Wang Weiping**
School of Computer Science and Engineering,
Central South University, China
wpwang@csu.edu.cn

**Abdul Monem S. Rahma**
Computer Science Department
AL-Maarif University College, Iraq
Monem.rahma@uoa.edu.iq

**Hasnain Ali Al mashhadani**
School of Computer Science and Engineering,
Central South University, China
hasnainalmshhadani@gmail.com

**Mazen R. Hassan**
Department of Electrical Engineering Techniques,
Basrah Engineering Technical College,
Southern Technical University, Basrah, Iraq
mazen.hassan@stu.edu.iq

*Corresponding author

***Abstract*** *– With the rise of multimedia technology, audio file encryption has become increasingly significant, especially for voice messages in popular social media applications like WhatsApp. Voice messages hold great social significance, and to ensure their security, they must be encrypted before being transmitted over the internet. This paper proposes an efficient algorithm to securely encrypt voice messages. The innovative algorithm is based on a magic cube to reduce the execution time of the advanced encryption standard (AES) cipher algorithm. This is achieved by replacing the MixColumn function with a 3 × 3 × 3 magic cube FG (2^8) irreducible polynomial. This work reduces the execution time of the AES cryptosystem and enhances complexity by utilizing additional keys generated by a 3 × 3 × 3 magic cube. to develop a block cipher algorithm that encodes audio files using two types of finite fields: GF (P) and GF (2^8). This algorithm places a key of three cells and a voice message of six cells on each face of a 3 × 3 × 3 magic cube. Time complexity and encryption quality are evaluated according to National Institute of Standards and Technology standards, and the differential attacks' peak signal-to-noise ratio is calculated. The total complexity achieved for both GF (P) =$256^9 \times 251^{18}$ and GF (2^8) = $256^9 \times 256^{18}$ is measured for comparison. Simulation results demonstrate a significant reduction in execution time and increased encryption complexity. Moreover, the magic cube with three faces (3 × 3 × 3) exhibits superior performance in terms of complexity and speed compared to the third-order magic square.*

***Keywords***: *GF (2^8) finite field, GF (P) finite field, Gaussian elimination, magic cube cryptography*

*Received: March 23, 2024; Received in revised form: December 18, 2024; Accepted: December 9, 2024*

## 1. INTRODUCTION

In today's world, when data is transferred between individuals, a high level of security is required. Cryptography focuses on the use of encryption and decryption algorithms to ensure private communication [1, 2, 3]. Due to the rapid development of the internet, wireless voice communication technology has become widely utilized. During the data transmission process, there is a risk of information leakage, making research on audio information encryption highly significant. Many chaos-based encryption algorithms, such as chaotic systems [4, 5] DNA coding, and classical logistic chaotic systems, are used to deal with speech data. In addition, traditional encryption algorithms, the advanced encryption standard (AES) [6-10], have been extensively employed in audio encryption and have yielded unsatisfactory results. AES encodes 128-bit plaintext blocks using master key blocks of 128, 192, or 256 bits. Accordingly, AES is referred to as AES-128, AES-192, and AES-256 based on the key sizes. Before generating the 128-bit ciphertext block, the plaintext block undergoes a predefined number

of rounds using the round function: 10 rounds for AES-128, 12 rounds for AES-192, and 14 rounds for AES-256. A 4 × 4-byte array can represent plaintext, cipher text, intermediate state blocks, and the primary key, which is implemented accordingly. The number of columns in the array is determined by dividing the key length by 32 [11]. The encryption method utilizes the following operations:

1. Sub-byte transformation or inverse sub-byte transformation: This technique involves a non-linear byte-to-byte transformation achieved through a multiplicative inverse operation followed by an affine transformation.
2. Shift rows: The shift row transformation is more significant than the initial arrangement because the state, cipher input, and output are treated as arrays of four 4-byte columns.
3. Mix columns: This operation analyses the state column-by-column, treating each column as a four-term polynomial.
4. Add round key: A round key is added to the state using an XOR operation.

The inverse cipher follows the same procedure as the encryption process but in the opposite direction. The inverse sub-byte transformation comes next after performing the Shift Rows operation in the opposite direction. next, the mixed columns operation is applied, and the add round key operation is performed. The resulting array (either plaintext or encrypted text) is obtained once these state operations are completed [12, 13]. Magic squares have a long history and have served various purposes. They have been the basis for many intelligence-testing games [14, 15]. A magic square of size, n × n is an arrangement of numbers from 1 to $n^2$ in a square such that the sum of every row, column, and diagonal is the same. Alpha magic squares consist of discrete words or numbers engraved or printed. They can be arranged vertically, horizontally, or diagonally to produce the same number or form the same words. When a dimension is added to a magic square [15-26], it becomes a "magic cube" towards computer ethics and information security, as computer security and computer ethics are important components of the management information system. The probability of constructing a magic cube is similar to that of constructing a magic square, especially for large values of n. Our proposed method addresses the weak delay [27] in the mix columns operation in the AES algorithm.

$$\begin{bmatrix} S'1 \\ S'2 \\ S'3 \\ S'4 \end{bmatrix} = \begin{bmatrix} 02030101 \\ 01020301 \\ 01010203 \\ 03010102 \end{bmatrix} \begin{bmatrix} S1 \\ S2 \\ S3 \\ S4 \end{bmatrix} \quad (1)$$

$$\begin{bmatrix} S'1 \\ S'2 \\ S'3 \\ S'4 \end{bmatrix} = \begin{bmatrix} 0e0b0d09 \\ 090e0b0d \\ 0d090e0b \\ 0b0d090e \end{bmatrix} \begin{bmatrix} S1 \\ S2 \\ S3 \\ S4 \end{bmatrix} \quad (2)$$

This multiplication operation can be computationally expensive, especially with large input matrices.

To overcome this, we introduce a 3 × 3 × 3 magic cube [22, 25, 28] in GF (2^8) irreducible polynomial [28-30], which allows for faster processing of the matrices [31]. This approach involves using a more complex key in GF $(2^8)^9$ and voice messages with two types, GF $(251)^{18}$ and $(2^8)^{18}$. The corresponding results demonstrate the new block cipher algorithm is proposed that utilizes three faces of a 3 × 3 × 3 magic cube irreducible polynomial instead of Mixcolumn. The technique proposal focuses on improving and enhancing the security of encrypted messages by increasing the complexity and decreasing encryption and decryption time. Hence, the protection of encrypted audio messages is effectively guaranteed. Thereby, it can be applied to secure and encrypt communications, messages, and voice messages on platforms that hold significant social importance. The contributions of this paper are as follows:

Development of a new and innovative symmetric block cipher algorithm.

- Utilize a magic cube with three faces and 27 cells, where the sum of each row, column, or diagonal is equal.
- The block cipher incorporates 9 keys and is represented by a system of 18 linear equations, solved using Gaussian elimination.
- The algorithm's key complexity enhances security and makes hacking more challenging.
- Implement the magic cube GF (2^8) algorithm to increase complexity and achieve high speed.
- The algorithm is computationally inexpensive.
- It provides a secure environment for transmitting and receiving audio files, specifically voice messages.

The rest of the paper is organized as follows: Section 1 provides an overview of related work. Section 2 describes the proposed methodology, while Section 3 describes the algorithm used to build the magic cube. Section 5 thoroughly evaluates the results, and finally, Section 6 concludes the paper.

## 2. RELATED WORKS

In [31], the cipher employs a substitution permutation network structure with six dimensions for parallel encryption of 128-bit data blocks in six directions, enhancing processing efficiency for large data volumes. The proposed multi-dimensional symmetric cipher algorithm focuses on encryption and does not address decryption procedures. However, the research paper does not provide information on the proposed algorithm's comparative analysis with other symmetric block ciphers to showcase its efficiency and effectiveness.

An advanced method named 3D-BERC for encrypting images in three dimensions, using Rubik's cube principles and bit-level encryption, was introduced in

[32]. This advanced encryption scheme ensures image security by implementing effective permutation and diffusion techniques to scramble and spread changes across cipher images. Experimental results and simulation analysis prove this. However, there is no mention of a comparative study with existing encryption schemes to demonstrate the superiority or effectiveness of the proposed 3D-BERC method.

The authors in [21] have proposed a data-hiding strategy that utilizes modification directions (EMD) to embed large payload information without causing distortion. The traditional EMD technique encodes a secret digit using the $(2n+1)$–ary system, with a maximum payload capacity of 1.161 bits per pixel (bpp). This study involves concealing a secret digit using the $(3n)$ 3–ary notational system. The secret digit is buried within a group of 3 pixels selected based on a random sequence. This process results in a payload of $log2(n)$. An increase in the dimension, $n$, of the neighborhood set leads to a higher payload. Nevertheless, the research primarily addresses the effectiveness of embedding in terms of efficiency and visual quality of the stego image without delving into a thorough analysis of the computational complexity or processing time involved in the embedding process.

In [20] introducing a cryptographic method known as the symmetric magic cube. This method focuses on constructing magic cubes of the form $m \times 2l$. It enables encryption and decryption of various types of images, including numeric digits and special characters, while also addressing the issue of repetition in the ciphertext. However, the proposed algorithm was applied only to medical images, and no other files were taken into consideration to demonstrate the validity of the application

The paper [33] proposes a lightweight image encryption algorithm based on Rubik's Revenge cube move patterns. The study primarily focuses on creating highly nonlinear S-boxes derived from the cube's permutations for improved security and effectiveness. However, the algorithm's efficiency in practice needs to be evaluated further to ensure it can handle real-world image encryption requirements.

The paper [34] presents a multiple remote sensing image (MRSI) encryption scheme that enhances salient image regions' security and transmission efficiency. The scheme uses a 4D-IDTLN chaotic system and knowledge-oriented and vision-oriented saliency techniques to create a mask contour positioning model (MCPM) and then fuses the MRSIs into a cube. The encryption is then further encrypted using closed-loop diffusion. The security of the proposed scheme is evaluated, showing higher security and better transmission efficiency. However, the paper does not address potential decryption methods or the process.

This paper [24] proposes a method for recognizing and restoring the color block of the magic cube using machine vision. The magic cube color block is recognized by machine vision, followed by image color space transformation and K-means clustering. The color block information is packaged and sent to the cube explore 5.14 through negotiation. This paper focused on a specific type of robot (a magic cube-solving robot), limiting the generalizability of the findings to other robotics applications involving color recognition and manipulation.

This paper [22] proposes a multiple remote sensing image (MRSI) encryption scheme based on saliency extraction and magic cube circular motion to improve salient regions' security and transmission efficiency in remote sensing images. The scheme provides two tiers of privacy protection for airport locations in the images. First, a 4D improved discrete tabu learning neuron (4D-IDTLN) chaotic system is proposed, which exhibits rich dynamic behaviors. Second, the salient regions of the images are classified and extracted using knowledge-oriented saliency (KOS) and vision-oriented saliency (VOS) techniques to create a mask contour positioning model (MCPM), which is then encrypted. The MRSIs are fused into a cube, encrypted using magic cube circular motion and chaotic sequences, and further encrypted using closed-loop diffusion. The security of the proposed encryption scheme is evaluated, indicating that it provides higher security and better transmission efficiency for MRSIs. However, the paper focuses on encryption techniques but does not delve into potential decryption methods or address the decryption process, which is crucial for understanding the complete security framework. Proposed Methodology

This paper addresses the security concerns related to voice messages on social media platforms. To tackle this problem, a new block cipher algorithm is proposed, which utilizes the three faces of a $3 \times 3 \times 3$ magic cube. The algorithm will be discussed in detail in the remaining sections.

## 3. PROPOSED ALGORITHM TO BUILD A MAGIC CUBE USING GF (2^8)

The audio file [35] media is divided into two main parts:

The first part is the structure, which contains information about the file, such as file type (single channel, dual channel, etc.), sampling rate, representation depth, file length (duration), and any other information that defines the file's properties [4].

The second part is the data containing the audio samples' numerical values. These samples are arranged chronologically according to the sampling rate, and each sample represents the sound level at a particular moment. The digital audio file is split into digital audio files [36]. The structure (header), which contains information about the file and the data, represents the audio's numeric values. These two parts go hand in hand and together form the digital audio file [4]. The proposed algorithm for encrypting the data of any audio file has preserved the file structure, and the algorithm's output is an encrypted audio file.

A finite field, commonly known as a Galois field, is named after the mathematician 'Evariste Galois', who discovered it. A restricted number of components characterizes finite fields and are increasingly used, particularly in translating computer data. The designated domains are extensively used in several scientific disciplines, including mathematics, programming, and number theory. The finite field was used for the decimal number, with the whole field constructed upon a prime number (P), represented succinctly as GF(P).

A polynomial is termed an "irreducible polynomial" if it cannot be expressed as the product of two or more lower-degree polynomials. Additionally, all non-zero elements possess a multiplicative inverse. Irreducible polynomials are utilized in various encryption methods, particularly in modern encryption techniques such as AES and elliptic curve cryptography.

A finite field has limited elements, and all outcomes of operations conducted inside it are within its range. We can execute mathematical operations for polynomial expressions like addition, subtraction, multiplication, division, and positive integer exponents.

The transition from decimal to polynomial numbers has occurred due to the need for modern electronics to operate on 8 bits. The coefficients of the polynomial may rely on 8 bits, represented as GF (2^8). To elucidate the need to transition to GF (2^8), using GF(P) will provide all resultant numbers that are less than the selected (P), given the present circumstances[11].

AES Where provides a convenient and efficient representation of operations on bytes. The arithmetic in GF (2^8) is typically implemented using a primitive polynomial of degree eight, which defines the structure of the field [11, 37-40].

A magic cube [21, 41, 42] is similar to a magic square[45], but it has multiple sizes, such as order 3, 4, 5, 6, 7, and so on. The size of a magic square determines the number of elements it contains, with larger sizes having more numbers.

In the AES algorithm, the mix columns transformation involves a computationally expensive multiplication operation, especially when dealing with large input matrices. To mitigate this, the multiplication operation can be replaced by utilizing a $3 \times 3 \times 3$ magic cube in GF (2^8), filled with the cells from 1 to 27.

### 3.1. DETAILS OF THE ALGORITHM

Based on the known characteristics of a $3 \times 3 \times 3$ magic cube, as shown in Fig. 1, the cube can be divided into three faces, each resembling a $3 \times 3$ square. This division allows us to obtain six equations for the rows, six for the columns, and six for the main and secondary diagonals. In total, we have 24 equations derived from the magic cube structure.

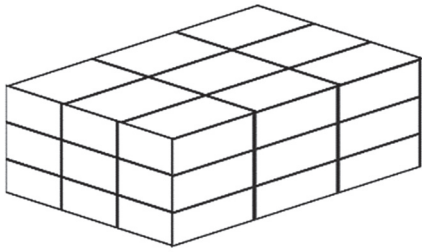


**Fig. 1.** Illustration of a $3 \times 3 \times 3$ magic Cube dissected into three faces

Face 1 of the magic cube consists of 1 to 9 cells. As a result, the message to be encrypted will contain only six cells corresponding to the number of equations derived from the rows, columns, and diagonals of face 1. The key will occupy the remaining three positions on face 1, as depicted in Fig. 2. Two equations are excluded from the resulting sums obtained from the equations. These excluded sums will be treated as encrypted voice messages, and their number will be comparable to the number of positions in the message (as shown in Figs. 2b and 2f).

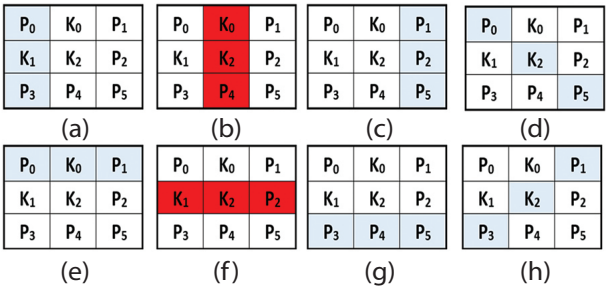



**Fig. 2.** Cube face 1. The highlighted sums are used in the magic cube algorithm

Face 2 of the magic cube consists of 1 to 9 cells. As a result, the message will contain six cells, equivalent to the number of equations. There will be three remaining positions designated for the key, as shown in Fig. 3. The resulting sums obtained from these equations will be treated as encrypted voice messages, and their number will correspond to the number of positions in the message. Two equations have been removed from the calculations (as depicted in Figs. 3j and 3n).

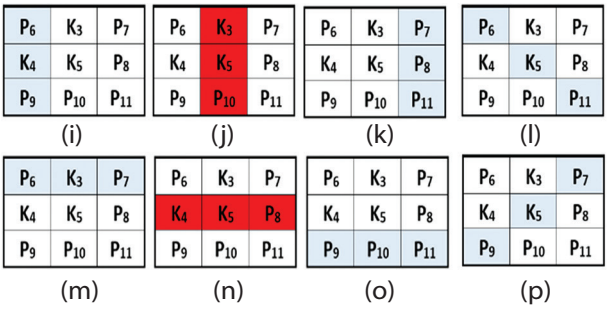



**Fig. 3.** Cube face 2. The highlighted sums are used in the magic cube algorithm.

Face 3 of the magic cube consists of 1 through 9 cells. Consequently, the message will consist of six cells, equal

to the number of equations, and the remaining key positions will only contain three cells, as illustrated in Fig. 4. The sums obtained from these equations will be treated as encrypted voice messages. Their number will match the number of message positions. The calculations have excluded two equations (as shown in Figs. 4r and 4w).

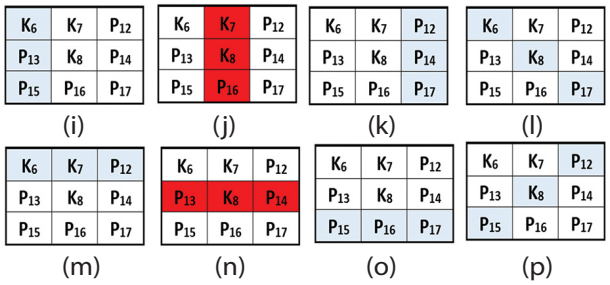



**Fig. 4.** Cube face 3. The highlighted sums are used in the magic cube algorithm

A total of 18 equations are to be employed in the proposed method. The positions and values of the keys within the magic cube are not restricted to fixed locations. Instead, a flexible selection process is employed, and the locations are expected to be chosen using GF (2^8), as shown in Fig. 5.

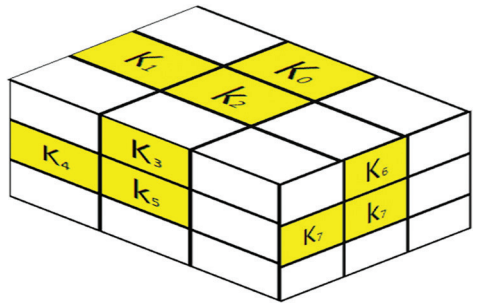


**Fig. 5.** The keys presumed selected for GF (2^8).

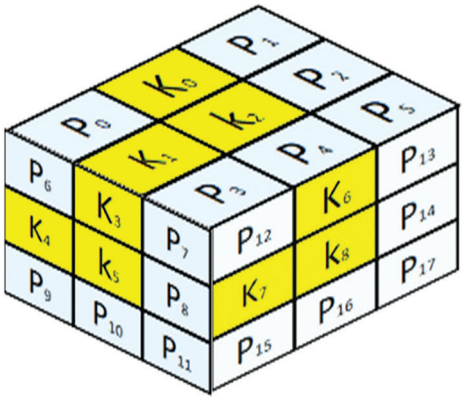


**Fig. 6.** The message on the created magic cube (colored sections) and keys (remaining areas)

Fig. 6 depicts the formation of 18 sites corresponding to 18 sums in 3 × 3 × 3 magic cubes after filling in the essential locations. Referring to Fig. 6, the sums of the 18 equations for each of the 3 faces are found, and the equations are formed as in (3).

$$
\begin{aligned}
&e1: P0 + K1 + P3 = Sum1\\
&e2: P1 + P2 + P5 = Sum2\\
&e3: P0 + K0 + P1 = Sum3\\
&e4: P0 + K0 + P1 = Sum4\\
&e5: P3 + P4 + P5 = Sum5\\
&e6: P1 + K2 + P3 = Sum6\\
&e7: P6 + K4 + P9 = Sum7\\
&e8: P7 + P8 + P11 = Sum8\\
&e9: P6 + K5 + P11 = Sum9\\
&e10: P6 + K3 + P7 = Sum10\\
&e11: P9 + P10 + P11 = Sum11\\
&e12: P7 + K5 + P9 = Sum12\\
&e13: K6 + P13 + P15 = Sum13\\
&e14: P13 + P14 + P17 = Sum14\\
&e15: K6 + K8 + P17 = Sum15\\
&e16: K6 + K7 + P12 = Sum16\\
&e17: P15 + P16 + P17 = Sum17\\
&e18: P12 + K8 + P5 = Sum18
\end{aligned}
\qquad (3)
$$

Consequently, we obtain 18 quanta representing the encoded voice message to be sent to the recipient. Each data packet will be encrypted using the magic cube algorithm. The keys will be placed in the agreed-upon positions on the recipient's end. In contrast, the remaining positions will remain unknown, with their number matching the number of encoded voice messages. The issue will be solved mathematically by arranging the elements so that the primary diameter does not equal zero at any of its coordinates. The computations and analyses in this work used the Gaussian elimination method to solve the equations and derive the communication.

After completing and implementing this work, a further development was made by replacing the phonetic letters GF (P) with the key complexity of GF (2^8). This modification was introduced because of the magic cube, as illustrated in Fig. 7.

**Algorithm 1-a: The proposed algorithm for encryption symmetric cipher based on a magic cube.**

**Input:** voice message, key values, and key positions.
**Output:** Cipher text.
**Begin:**
**Step 1:** Placing the key values in the agreed positions.
**Step 2:** The remaining positions are filled with the values of the message.
**Step3:** Find the final results for each equation of (1), of which there are 18 equations. The end result of the algorithm will be the encrypted voice message sent to the other party
**End.**

**Algorithm 1-b: The proposed algorithm for decryption symmetric cipher based on a magic cube.**

**Input:** Cipher text, key positions, and key value.
**Output:** voice message
**Begin:**
**Step 1:** The key value is placed at the agreed positions.

**Step 2:** The remaining positions will remain unknown. They will be found by solving 18 mathematical after arranging the equations by not making the main diagonal = 0. The final results will be the original data (voice message).

**End.**

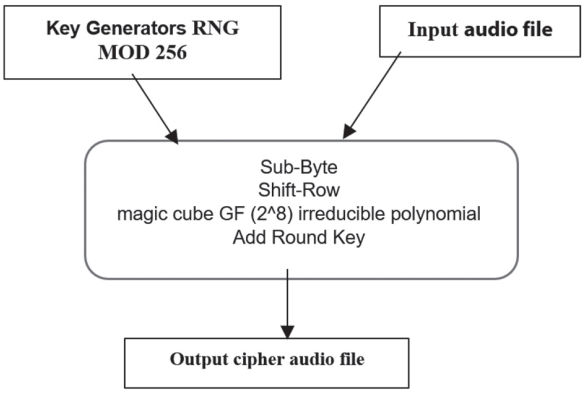



**Fig. 7.** Diagram replacement of a magic cube Instead of a mix column for the proposed AES technique for encrypting audio file

## 4. EVALUATION

Cryptology is concerned with encryption and decryption using specific algorithms. To ensure message integrity and security, the decryption process requires a private key that is kept confidential between the communicating parties. It is important to maintain the privacy of the key to protect the encrypted messages. This study will discuss the speed, complexity, and statistics measures defined by the (NIST), (PSNR) tests. These measures will be applied to analyze the performance of the proposed algorithm for voice messages (encryption and decryption). The statistics of the voice messages will be plotted and compared with earlier algorithms that operate on similar data types, considering both types of finite fields. The proposed algorithm was implemented using Python 3.10.5 and Jupyter Notebook Anaconda 3. The simulation was conducted with an Intel(R) Core (TM) i7-6500U CPU @ 2.50GHz, 2.60 GHz, and 8.00 GB (7.88 GB usable) of RAM. The operating system used was a 64-bit version with x64-based processor.

### 4.1. COMPLEXITY OF THE KEY

Key complexity is a computed statistic that quantifies the difficulty of a brute-force attack on a cryptographic key. It indicates the number of attempts required to crack the key successfully through an exhaustive search.

Using GF (P), the solution to the $3 \times 3 \times 3$ magic cube is the value of the prime number employed raised to the power of the number of keys, represented by three keys per face:

For GF (2^8), the key's strength is $2^8$ raised to the power of 3:

the complexity of face 1 key using GF (2^8) = $256^3$ (7)

the complexity of face 2 key using GF (2^8) = $256^3$ (8)

the complexity of face 3 key using GF (2^8) = $256^3$ (9)

### 5.2. GENERALIZED COMPLEXITY OF THE PROPOSED SYSTEM

The data complexity of the proposed system is constant for both variants, GF (P) and GF (2^8). It is determined by the number of possible ASCII codes, which is 256, raised to the power of the number of message sites in the system, which is 18. This represents the total number of possible combinations of the message data. The total complexity of the system, when using GF (2^8) and keeping the keys secret, can be calculated as in (14):

complexity in face 1 using GF (P) = $256^3 \times 251^6$ (10)

complexity in face 2 using GF (P) = $256^3 \times 251^6$ (11)

complexity in face 3 using GF (P) = $256^3 \times 251^6$ (12)

total complexity using GF (P) = $256^9 \times 251^{18}$ (13)

total complexity using GF (2^8) = $256^9 \times 251^{18}$ (14)

The complexity of the $3 \times 3 \times 3$ magic cube system is compared with the system based on a magic square of order 3 (MS3) in Fig. 8, using both types of finite field.

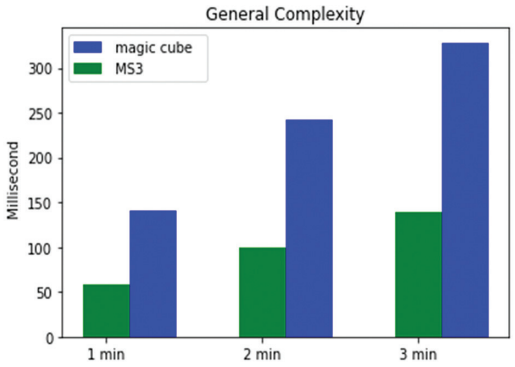



**Fig. 7.** The general complexity of the MS3 system and the $3 \times 3 \times 3$ magic cube system

### 4.2. EXECUTION TIME

The encryption and decryption times were measured for audio messages using GF (P) and GF (2^8), as shown in Table 1, and for voice messages using GF (p) and GF (2^8), as shown in Table 1.

Table 1 shows that the proposed algorithm is faster than the original. Using the finite field to type GF (P) and GF (2^8) irreducible polynomial gives a relatively good advantage as it gives faster execution. correspondingly, the original AES algorithm suffers from high calculation and computational overhead problems. However, the encryption and decryption process is equal in execution time. In the proposed algorithm, additional calculations are involved in performing Gaussian demodulation for decoding.

The corresponding plots illustrating the execution times can be found in Figs. (9-10). Furthermore, Figs.

(11-12) Compare the execution times of the proposed magic cube algorithm and the older MS3 method.

**Table 1.** Compare the execution time of the magic cube algorithm and the original AES algorithm for encrypting and decrypting voice

| GF | Audio file size (MB) | Audio file duration (min.) | Basic AES encryption time (ms) Ref.[45] | Encryption time (ms) | Decryption time (ms) |
|---|---|---|---|---|---|
| GF (2^8) | 1.61 | 1 | 61 | 140.670 | 142.560 |
| GF (2^8) | 2.76 | 2 | 82 | 241.392 | 243.490 |
| GF (2^8) | 3.90 | 3 | 14 | 328.218 | 330.115 |
| GF (251) | 1.61 | 1 | 61 | 184.394 | 186.415 |
| GF (251) | 2.76 | 2 | 82 | 316.028 | 326.567 |
| GF (251) | 3.90 | 3 | 14 | 362.494 | 365.631 |

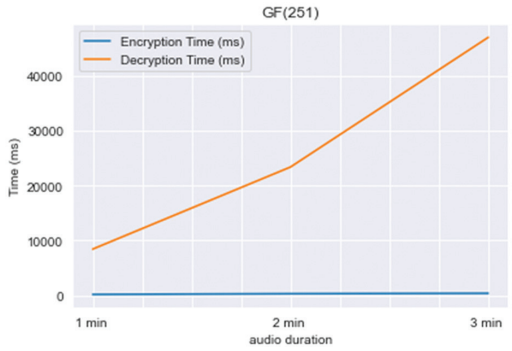



**Fig. 9.** Comparison of the execution time of the proposed algorithms using GF (P)

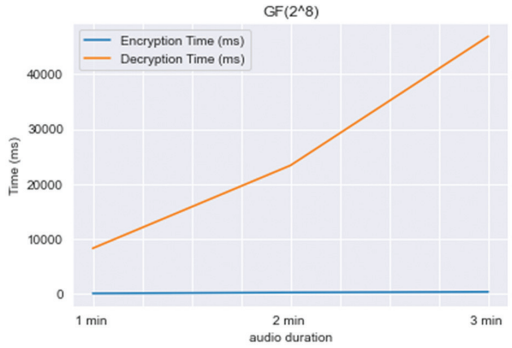



**Fig. 10.** Comparison of the execution time of the proposed algorithms using GF(2^8)

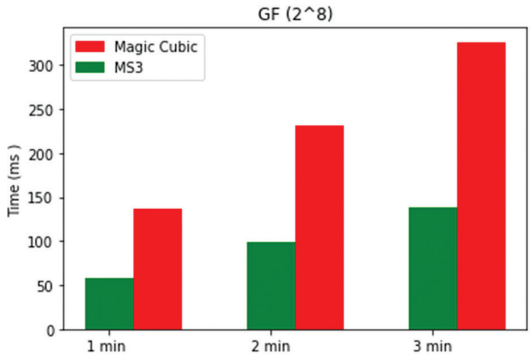



**Fig. 11.** Encryption time (m.s) and decryption time (m.s) when using the magic cube GF(P) algorithm for a voice

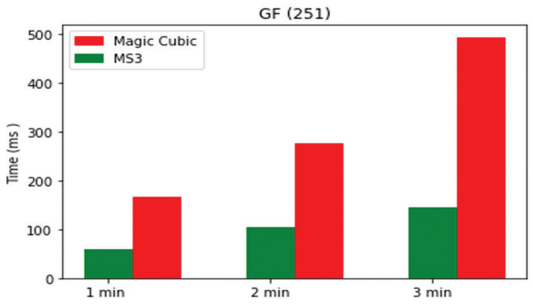



**Fig. 12.** A comparison in terms of execution time between MS3 and magic cube GF (2^8) for a voice

### 4.3. PSNR TEST

PSNR measures the ratio between the original signal and the encrypted signal. When it comes to encrypted audio, a lower PSNR [42] indicates a higher noise presence in the cryptogram. This means that the ciphertext is more resistant to attacks. The mathematical equation the PSNR [44], of the voice messages can be calculated using equation (15).

$$PSNR = 10 \log_{10} \left( \frac{MAX^2}{MSE} \right) \quad (15)$$

Where MSE is the mean square error used to measure the error in voice messages, equation (16) calculates the MSE for voice messages.

$$MSE = \frac{1}{M \times N} \sum_{i,j} (A[i,j] - B(i,j)^2 \quad (16)$$

In this context, $M$ and $N$ denote the width and height of the audio, respectively, whereas $(i, j)$ indicates the position of the sample value point. $A$ and $B$ denote the original and encrypted voice messages, respectively, while representing the highest value inside the message. shown in Table 2 presents the results.

**Table 2.** illustrates the outcomes of the (PSNR and MSE) tests conducted on both the input and output voice messages

| Audio file duration second | Audio file size | MSE | PSNR |
|---|---|---|---|
| 96.6 s | 256 bytes | 0.00 | Inf dB |
| 165.6 s | 256 bytes | 0.00 | Inf dB |
| 234 s | 256 bytes | 0.00 | Inf dB |
| 96.6 s | 251 bytes | 0.00 | Inf dB |
| 165.6 s | 251 bytes | 0.00 | Inf dB |
| 234 s | 251 bytes | 0.00 | Inf dB |

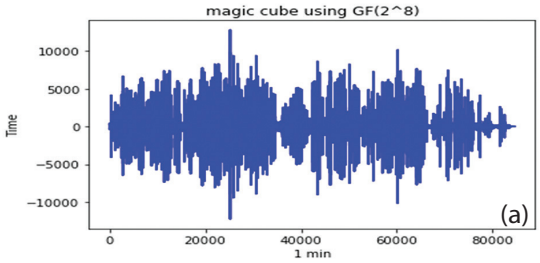
### 4.4. ANALYSES OF NIST TESTS

The proposed magic cube algorithm comprehensively evaluated its encryption capabilities using seven statistical tests recommended by the NIST. These tests assess the randomness of the binary sequences generated by the algorithm, ensuring its effectiveness in encryption. One of the devised tests is the randomization test, which examines the encrypted output audio file of the encryption methods. This test encompasses various

randomization techniques, including frequency tests, frequency testing within blocks, and entropy tests. The results of these tests are presented in Table 3. In particular, the entropy measure is utilized to assess the randomness of the binary sequences. A higher entropy value indicates a higher probability when the number of zeros and one's equals (entropy = 1.000000). A lower entropy value suggests a lower probability when the number of ones and zeros differs (entropy 0.000000). When employing various blocks, any variation in the distribution of ones and zeros leads to a corresponding variation in the entropy value.

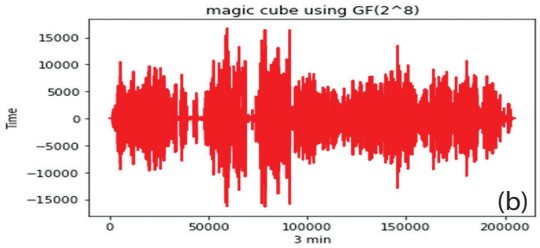
**Table 3.** The NIST test results for the two different forms of finite field

| GF | Audio file size (MB.) | Audio duration (min.) | Block Frequency | Cumulative Sums | FFT | Frequency | Longest Run | Rank | Runs |
|---|---|---|---|---|---|---|---|---|---|
| GF (2^8) | 1.61 | 1 | 1.000000 | 0.288242 | 0.767097 | 0.144127 | 1.000000 | 0.000000 | 0.674990 |
| GF (2^8) | 2.76 | 2 | 1.000000 | 0.727622 | 0.468160 | 0.654721 | 1.000000 | 0.000000 | 0.342806 |
| GF (2^8) | 3.90 | 3 | 1.000000 | 0.917917 | 0.468160 | 0.654721 | 1.000000 | 0.000000 | 0.342806 |
| FG (251) | 1.61 | 1 | 1.000000 | 0.115559 | 0.123812 | 0.057780 | 1.000000 | 0.000000 | 0.843325 |
| FG (251) | 2.76 | 2 | 1.000000 | 0.359368 | 0.468160 | 0.371093 | 1.000000 | 0.000000 | 0.852179 |
| FG (251) | 3.90 | 3 | 1.000000 | 0.727622 | 0.468160 | 0.371093 | 1.000000 | 0.000000 | 0.456057 |
| **Condition Final results** | | | <=1.000000 **All success** | <=1.000000 **All success** | <=1.000000 **All success** | <=1.000000 **All success** | <=1.000000 **All success** | <=1.000000 **All success** | <=1.000000 **All success** |



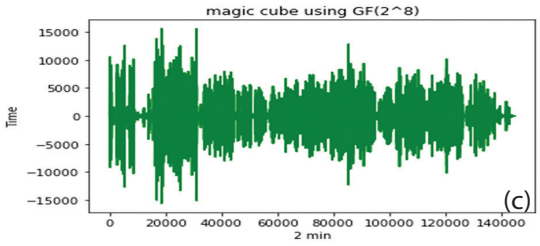

Sample Cipher voice messages 1min. GF (2^8)

b5000000c4000000ce0000003201000004
0100004600000130100008a0100000c00
0000b5000000df0100001c0000003e0100
006b010000d4000000a300000031010000
cc000000b5000000c4000000ce00000032



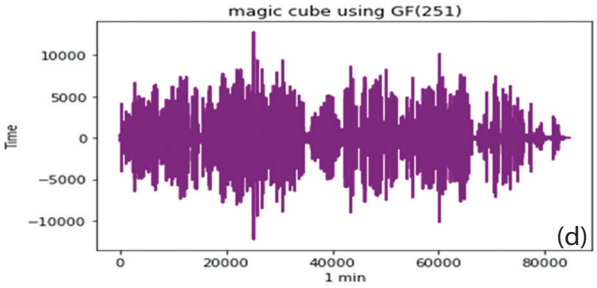

Sample Cipher voice messages 2 min. GF (2^8)

00308000001060000e0050000260500008
3020000e2080000a203000020050000600
300004d0500003007000052030000a70a0
0001a07000061050000b0070000c708000
0a1050000030800000 1060000e00500002



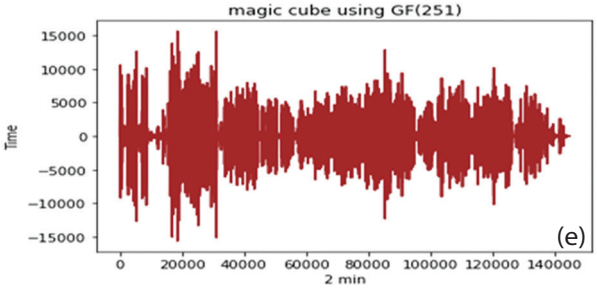

Sample Cipher voice messages 3 min. GF (2^8).

99020000b70100004c0100009501000061010
0009502000086010000530400 00ae030000be
0300006203000048040000b4020000ad03000
0a7020000f3020000680400 00c10200009902
0000b70100004c0100009501000061010000 95



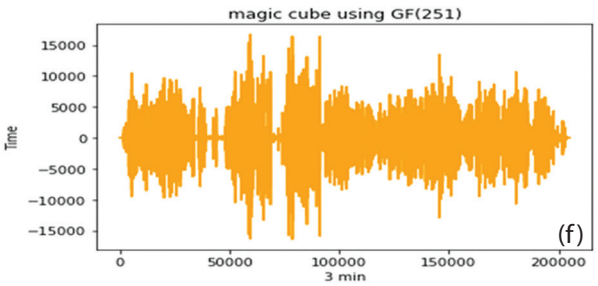

Sample Cipher voice messages 1min. GF (251)

df0100001c0000003e0100006b010000d4
000000a300000031010000cc000000b5
000000c4000000ce00000032010000040
100004100000c000000b50000000a3000
00031010000cc000000b5000000c40000




Sample Cipher voice messages 2 min. GF (251)

000061050000b0070000c7080000a1050
000030800000 1060000e0050000260500
0083020000e2080000a20300002005000
0600300004d0500003007000052030000
a70a00001a07000061050000b0070000c




Sample Cipher voice messages 3 min. GF (251)

ce0000003201000004010000460000001 30
100008a0100000c000000b5000000df01000
01c0000003e0100006b010000d4000000a3
00000031010000cc000000b5000000c40000
00ce0000003201000004010000460000001

**Fig. 13.** Samples of encoded voice messages with corresponding Cipher voice messages using : (a) 1 min. GF(2^8), (b) 2 min. GF(2^8), (c) 3 min. and (d) 1 min. GF(P), (e) 2 min. GF(P), (f) 3 min. GF(P)

## 5. CONCLUSION

Developing a new block cipher algorithm by replacing the MixColumn function with a $3 \times 3 \times 3$ magic cube GF (2^8) irreducible polynomial. Introduced several noteworthy characteristics. Firstly, it exhibited a higher key complexity and an increased number of equations compared to the MS3 algorithm GF (2^8), where the magic cube was larger but resulted in faster execution. Additionally, two peculiarities were observed in the case of voice messages: GF (P) demonstrated faster execution time, while the GF (2^8) variant showed lower execution times. The complexity of the keys in the algorithm depends on the desired level of security and the specific implementation. In the magic cube algorithm, the keys play a crucial role in the encryption and decryption processes, involving linear equations solved using Gaussian elimination. The complexity of the keys enhances the randomness and unpredictability between messages, as confirmed by statistical analysis using NIST and PSNR tests. The complexity of the algorithm is enhanced by utilizing the three faces of the magic cube for keys. Consequently, this would increase the system's overall security and complexity. The proposed algorithm can be applied to various platforms, including smartphones, computers, and other devices involved in the exchange of voice messages. Its effectiveness in securing voice message communications makes it a suitable choice for ensuring privacy and security in such scenarios.

## 6. REFERENCES:

[1] R. Dunn, J. Kim, Z. A. Poucher, C. Ellard, K. A. Tamminen, "A Qualitative Study of Social Media and Electronic Communication among Canadian Adolescent Female Soccer Players", Journal of Adolescent Research, Vol. 39, No. 2, 2024.

[2] J. Hofhuis, J. Gonçalves, P. Schafraad, B. Wu, "Examining strategic diversity communication on social media using supervised machine learning: Development, validation and future research directions", Public Relations Review, Vol. 50, No. 1, 2024, p. 102431.

[3] L. S. Macca, J. Ballerini, G. Santoro, M. Dabić, "Consumer engagement through corporate social responsibility communication on social media: Evidence from Facebook and Instagram Bank Accounts", Journal of Business Research, Vol. 172, 2024, p. 114433.

[4] X. Wang, Y. Su, "An Audio Encryption Algorithm Based on DNA Coding and Chaotic System", IEEE Access, Vol. 8, 2020, pp. 9260-9270.

[5] D. Herbadji, A. Herbadji, I. Hadad, A. Belmeguenai, N. Derouiche, "An Enhanced Logistic Chaotic Map based tweakable Speech encryption algorithm", Integration, Vol. 97, 2024, p. 102192.

[6] A. Vishwakarma, B. Singh, "Implementation Study of AES Standard for IoT Systems", Proceedings of the IEEE Global Conference on Computing, Power and Communication Technologies, New Delhi, India, 23-25 September 2022.

[7] H. J. Mohammed, A. H. Al-Adhami, Y. Yaseen, L. Abed, "A Developed Cryptographic Model Based on AES Cryptosystem", AIP Conference Proceedings, Vol. 2400, 2022.

[8] B. J. Al-Khafaji, A. M. S. Rahma, "Proposed new modification of AES algorithm for data security", Global Journal of Engineering and Technology Advances, Vol. 12, No. 3, 2022, pp. 117-122.

[9] C. Zhang, Y. Jia, L. Zhu, Z. Zhang, "Research on Simple Power Consumption Based on AES Algorithm", Proceedings of the IEEE 2nd International Conference on Electrical Engineering, Big Data and Algorithms, Changchun, China, 24-26 February 2023, pp. 1883-1886.

[10] K. Li, H. Li, G. Mund, "A reconfigurable and compact subpipelined architecture for AES encryption and decryption", EURASIP Journal on Advances in Signal Processing, Vol. 2023, No. 1, 2023.

[11] W. Stallings, "Cryptography and Network Security: Principles and Practice", Pearson Education, 2020.

[12] J.-J. Wang, Y.-H. Chen, G.-H. Liaw, J. Chang, C.-C. Lee, "Efficient schemes with diverse of a pair of circulant matrices for AES MixColumns-InvMixcolumns transformation", Communications of the CCISA, Vol. 26, No. 2, 2020, pp. 1-20.

[13] A. Vasselle, A. Wurcker, "Optimizations of Side-Channel Attack on AES MixColumns Using Chosen Input", Proceedings of the ACM SIGSAC Conference on Computer and Communications, 2017.

[14] J. Sesiano, "Sources and Studies in the History of Mathematics and Physical Sciences Magic Squares Their History and Construction from Ancient Times to AD 1600", Springer, 2019.

[15] N. Rani, V. Mishra, S. R. Sharma, "Image encryption model based on novel magic square with differential encoding and chaotic map", Nonlinear Dynamics, Vol. 111, No. 3, 2023, pp. 2869-2893.

[16] M. Tahbaz, H. Shirgahi, M. R. Yamaghani, "Evolutionary-based image encryption using Magic Square Chaotic algorithm and RNA codons truth table", Multimedia Tools and Applications, Vol. 83, No. 1, 2024, pp. 503-526.

[17] H. K. Wang, G. B. Xu, D. H. Jiang, "Quantum grayscale image encryption and secret sharing schemes based on Rubik's Cube", Physica A: Statistical Mechanics and its Applications, Vol. 612, 2023.

[18] A. De Schepper, J. Schillewaert, H. Van Maldeghem, M. Victoor, "Construction and characterisation of the varieties of the third row of the Freudenthal-Tits magic square", Geometriae Dedicata, Vol. 218, No. 1, 2024.

[19] X. Zhang, M. Liu, "Multiple-image encryption algorithm based on the stereo Zigzag transformation", Multimedia Tools and Applications, Vol. 83, No. 8, 2024, pp. 22701-22726.

[20] N. Rani, S. R. Sharma, V. Mishra, "Grayscale and colored image encryption model using a novel fused magic cube", Nonlinear Dynamics, Vol. 108, No. 2, 2022, pp. 1773-1796.

[21] J. J. Ranjani, F. Zaid, "Pseudo magic cubes: A multidimensional data hiding scheme exploiting modification directions for large payloads", Computers and Electrical Engineering, Vol. 89, 2021, p. 106928.

[22] C. Cai, Y. Wang, Y. Cao, B. Sun, J. Mou, "Multiple remote sensing image encryption scheme based on saliency extraction and magic cube circular motion", Applied Intelligence, Vol. 54, No. 8, 2024, pp. 5944-5960.

[23] S. I. Hernández, L. F. del Castillo, R. M. del Castillo, A. García-Bernabé, V. Compañ, "Memory kernel formalism with fractional exponents and its application to dielectric relaxation", Physica A: Statistical Mechanics and its Applications, Vol. 612, 2023.

[24] M. U. Hassan, A. Alzayed, A. A. Al-Awady, N. Iqbal, M. Akram, A. Ikram, "A Novel RGB Image Obfuscation Technique Using Dynamically Generated All Order-4 Magic Squares", IEEE Access, Vol. 11, 2023, pp. 46382-46398.

[25] N. Rani, V. Mishra, B. Singh, "Piecewise symmetric magic cube: application to text cryptography", Multimedia Tools and Applications, Vol. 82, No. 13, 2023, pp. 19369-19391.

[26] A. Santos, M. López de Haro, "A heuristic approach for the densest packing fraction of hard-sphere mixtures", Physica A: Statistical Mechanics and its Applications, Vol. 612, 2023.

[27] K. Gavaskar, "AES Algorithm using Dynamic Shift Rows, Sub Bytes and Mix Column Operations for Systems Security wih Optimal Delay", Research Square, 2022, https://www.researchsquare.com/article/rs-1973978/v1 (accessed: 2024)

[28] R. Gupta, A. Rai, "A class of permutation quadrinomials over finite fields", Communications in Algebra, Vol. 52, No. 4, 2024.

[29] M. Singh, D. Sehrawat, "Equal-degree factorization of binomials and trinomials over finite fields", Journal of Applied Mathematics and Computing, Vol. 70, No. 2, 2024, pp. 1647-1672.

[30] M. Yu, J. Xia, J. E. Feng, S. Fu, H. Shen, "Event-Triggered Synchronization of Multiagent Systems Over Finite Fields", IEEE Transactions on Circuits and Systems II: Express Briefs, Vol. 71, No. 1, 2024, pp. 370-374.

[31] O. A. Dawood, O. I. Hammadi, K. Shaker, M. Khalaf, "Multi-dimensional cubic symmetric block cipher algorithm for encrypting big data", Bulletin of Electrical Engineering and Informatics, Vol. 9, No. 6, 2020, pp. 2569-2577.

[32] H. Zhu, L. Dai, Y. Liu, L. Wu, "A three-dimensional bit-level image encryption algorithm with Rubik's cube method", Mathematics and Computers in Simulation, Vol. 185, 2021, pp. 754-770.

[33] A. Yousaf, A. Razaq, H. Baig, "A lightweight image encryption algorithm based on patterns in Rubik's revenge cube", Multimedia Tools and Applications, Vol. 81, No. 20, 2022, pp. 28987-28998.

[34] H. K. Wang, G. B. Xu, D. H. Jiang, "Quantum gray-scale image encryption and secret sharing schemes based on Rubik's Cube", Physica A: Statistical Mechanics and its Applications, Vol. 612, 2023.

[35] Z. N. Al-kateeb, S. J. Mohammed, "A novel approach for audio file encryption using hand geometry", Multimedia Tools and Applications, Vol. 79, No. 27-28, 2020, pp. 19615-19628.

[36] X. Wang, Y. Su, "An Audio Encryption Algorithm Based on DNA Coding and Chaotic System", IEEE Access, Vol. 8, 2020, pp. 9260-9270.

[37] M. B. Lin, J. H. Chuang, "The Design of a High-Throughput Hardware Architecture for the AES-GCM Algorithm", IEEE Transactions on Consumer Electronics, Vol. 70, No. 1, 2024, pp. 425-432.

[38] A. Malal, C. Tezcan, "FPGA-friendly compact and efficient AES-like 8 × 8 S-box", Microprocessors and Microsystems, Vol. 105, 2024, p. 105007.

[39] S. Gupta, M. Singh, M. Harish, "On the Study of Families of Linearized Polynomials over Finite Fields", Contemporary Mathematics, Vol. 4, No. 3, 2023.

[40] A. Cintas-Canto, M. M. Kermani, R. Azarderakhsh, "Reliable Architectures for Finite Field Multipliers Using Cyclic Codes on FPGA Utilized in Classic and Post-Quantum Cryptography", IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Vol. 31, No. 1, 2023, pp. 157-161.

[41] O. A. Dawood, A. M. S. Rahma, A. M. J. Abdul Hossen, "Generalized method for constructing magic cube by folded magic squares", International Journal of Intelligent Systems and Applications, Vol. 8, No. 1, 2016, pp. 1-8.

[42] S. Dhawan, "Secure and resilient improved image steganography using hybrid fuzzy neural network with fuzzy logic", Journal of Safety Science and Resilience, Vol. 5, No. 1, 2024.

[43] S. M. Kareem, A. M. S. Rahma, "An innovative method for enhancing advanced encryption standard algorithm based on magic square of order 6", Bulletin of Electrical Engineering and Informatics, Vol. 12, No. 3, 2023, pp. 1684-1692.

[44] S. Talasila, G. Vijaya Kumar, E. Vijaya Babu, K. Nainika, M. Veda Sahithi, P. Mohan, "The Hybrid Model of LSB—Technique in Image Steganography Using AES and RSA Algorithms", Proceedings of the International Conference on Soft Computing and Signal Processing, Vol. 2, Hyderabad, India, June 2023.