Multi-dimensional cubic symmetric block cipher algorithm for encrypting big data

Omar A. Dawood[1], Othman I. Hammadi[2], Khalid Shaker[3], Mohammed Khalaf[4]
[1,3]Computer Science Department, University of Anbar, Iraq
[2]College of Education for Humanities Science, University of Anbar, Iraq
[4]Computer Science Department, Al-Maarif University College, Iraq

Article Info

Article history:

Received Feb 13, 2020
Revised Apr 20, 2020
Accepted May 4, 2020

Keywords:

Big data
Block cipher
Magic cube
Magic square
Symmetric cipher

ABSTRACT

The advanced technology in the internet and social media, communication companies, health care records and cloud computing applications made the data around us increase dramatically every minute and continuously. These renewals big data involve sensitive information such as password, PIN number, credential numbers, secret identifications and etc. which require maintaining with some high secret procedures. The present paper involves proposing a secret multi-dimensional symmetric cipher with six dimensions as a cubic algorithm. The proposed algorithm works with the substitution permutation network (SPN) structure and supports a high processing data rate in six directions. The introduced algorithm includes six symmetry rounds transformations for encryption the plaintext, where each dimension represents an independent algorithm for big data manipulation. The proposed cipher deals with parallel encryption structures of the 128-bit data block for each dimension in order to handle large volumes of data. The submitted cipher compensates for six algorithms working simultaneously each with 128-bit according to various irreducible polynomials of order eight. The round transformation includes four main encryption stages where each stage with a cubic form of six dimensions.

Corresponding Author:

Omar A. Dawood,
Department of Computer Science,
University of Anbar, Iraq.
Email: Omar-Abdulrahman@uoanbar.edu.iq

1. INTRODUCTION

The cryptographic algorithms are a set of rules and mathematical procedures that are used to convert the clear text to an unintelligible text and vice-versa. There are basically two types of the first is cryptographic algorithms of public key cryptography (PKC) or what is called asymmetric cipher where the sender and receiver use two keys one for encryption and the other for the decryption process. The second is secret key cryptography (SKC) also known as symmetric encryption. The symmetric cipher plays an effective role for a trusted bock of data where the sender and receiver own the same secret key [1]. The proposed cipher represents a smart step in the designing process of symmetric block cipher construction. The submitted algorithm is dedicated to big data applications and it inherited most of its good characteristics from previously published algorithms [2-4]. Big data refers to the large data sets that increased dramatically and grown continuously from different sources. So the data classified today as the traditional data tomorrow will be big data since the data is evolving without stopping due to the advanced technology of the web applications and the electronic business services [5]. The big data is unlike traditional data because it needs a high potential that outweighs the conventional data from all aspects. So it should take into consideration the designing of a large cipher to meet the growth of data and the cipher should be convenient for the big volume of data because it became a necessary demand. The big data is not considered new data due to a huge historical data amount created from the earlier time that belongs to deep roots and an extended origin of old data [6]. Big data become a critical issue in recent years as a result of increased the growth of the internet and electronic communications, cloud services and social networks. The amounts of multimedia data generated within social networks are increasing without stopping [7]. Big data has become everywhere and definitively for several application domains. In a big data scenario, the data itself can be mapped to four distinct prototypes: data at rest, data in motion, data in many forms, and data in doubt. Moreover; there exist three forms of data integration in any enterprise: bulk data movement, real-time, and federation [8].

The big data interests with better analysis of the large bulks of data which support more intelligent decision and apply big profitability represented by smart decision, fast decision and impactful decision. Big data has powerful potential for making faster analysis in many scientific disciplines and the success of many enterprises [9]. Since the big data deals with a volume of data is very big and it generates and increases dramatically. Thus it will require a high processing capability compared with the traditional data need. Big data represents an aggregation of data from different kinds that involve current traditional data and an old one, it also includes a mixture of different types of structured and unstructured or multi-structured data that come from various sources [10]. In terms of unstructured data which instantiated from the data set that is not ordered or easily represented by traditional data models. So, social media or what is known as social networks such as Facebook, Tweeter, YouTube and other media from the point of view posts, comments and publications are considered good examples for this type of data. The case of multi-structured data, it indicates diversities of data sorts and formats that can be generated from users and devices, such as current social networks and web services as well as user interactions. The structured data are good examples of big data that may include the combination of text and images in addition to transactional information [11].

There are several distinct block cipher algorithms available that work with different structures and various mathematical descriptions. The present study will focus on the most common symmetric ciphers especially the standard ciphers that involve: IDEA, Triple-DES, AES, Twofish, Serpent, MARS, and RC6. Xuejia Lai and James Massey submitted an International Data Encryption Algorithm (IDEA). It is a new variant of symmetric cipher that was planned to be a replacement for the DES cipher. IDEA cipher encrypts electronic data of 64-bit using a 128-bit ciphering key under the Lai-Massey structure with 8.5 rounds. The IDEA cipher has been analyzed and broken in 2011 via the man in the middle attack and in 2012 full round was cryptanalytic by bicliques attack [12]. IBM Corporation develops Triple DES. It is a revised version for the IBM oldest cipher of data encryption standard (DES) that encrypts the data with a short secret key of 56-bit and Feistel structure. The Triple-DES or 3DES is the three times implementation process for the DES cipher under the length of secret key 168-bit and 48-rounds, although the Triple-DES suffered from the slow implementation it still applying in several civil applications and electronic financial services [13].

National Institute of Standards and Technology (NIST) released the Rijndael cipher as an advance encryption standard (AES) cipher. AES is the name for the block cipher that selected by NIST under the Rijndael name that designed by Vincent Rijmen and Joan Daemen in 1998. The Rijndael block cipher works with SPN structure and encrypts a block of data with a fixed length of 128-bit under three changeable ciphering keys according to the NIST criteria. The AES cipher is inspired by square cipher and is considered the best ciphering model, which is the most widely used algorithm for large scale applications presently [14]. Bruce Schneier et al., designed a Twofish cipher, Twofish is a revision block cipher algorithm for the previous blowfish block cipher. Twofish encrypts a block size of 128 bits and three of different ciphering key reaches 256 bits. It was a finalist candidate to be advanced encryption standard and as an alternated for the 3DES. Twofish algorithm works with 16-rounds of iterated Feistel structure of key-dependent S-Boxes [15]. Ross Anderson et al., designed a Serpent block cipher that is one of the best five finalist symmetric algorithms with SPN structure. Serpent algorithm encrypts the electronic data with a block size of 128-bits and also three different ciphering keys like the AES cipher. The serpent cipher can be implemented in a parallel structure of 32-rounds according to 32-bit of the bit-slices technique [16].

MARS cipher submitted by IBM Corporation, acts a revised cipher for the DES cipher and encrypts the electronic data with block size and key size similar to any AES candidate cipher. MARS encrypts the data via a variable secret key that ranging from 128-bit to 444-bit. MARS characterized by complex structure since it depends on heavy mathematical operations. Thus; it considers the most complicated cipher among the candidates' algorithms [17]. Rivest *et al.* [18] designed an RC6 algorithm that considers the simplest and easiest model as the AES candidate algorithm. RC6 cipher represents a revision form of the previous RC5 cipher but with double size. RC6 encrypts the electronic data with block length and a key length of 128-bit and the secret ciphering key can be up to 2040-bit. RC6 designed with Feistel network structure of four words each with 32-bit, which is iterated for 20-rounds completely [18].

In response to the security challenge, the proposed cipher is designed to face real attacks and to solve the traditional security problems in this field. The protection of private and confidential data attracted the researchers' attention for a long time. So, the basic challenge for the security of big data is data privacy.

The trusted multimedia issues have become critical and necessary in social network and cloud environments because the malicious attacks are becoming more sophisticated and new active malwares have been developed recently [19]. The vulnerability of security systems or fault of security designs can lead to big losses that may exceed even the worst expectations and introduce irreplaceable damage for a company or organization. Since, sensitive data has become accessible from anywhere and the potential of risks for malicious use is made possible. The questions beyond the ethical usage of data and data privacy become momentous. Since big data platforms introduce a broad array of likelihoods to access internal and external data. Unfortunately, most organizations that deal with big data face the same issues of daily threats [20]. Nowadays, most agencies look forward to ensuring that their information are kept securely. So the protect data with all these trends require an appropriate cipher that satisfies the real issues. The developed cipher must defeat the current challenges of end to end encryption, protected user access control, password management and safeguarding internal and external secret information at all levels. Big data terminology needs special cryptographic algorithms with an extended structure of large size or that one with the multi-dimensional cipher of parallel encryption process [21, 22]. The security in such milieu comprises more data stored, which means more security procedures and more modern policies of secrecy that should be taken into consideration to apply the privacy in an effective form. So, "a big question is to what extent the security and privacy technology are adequate for controlled assured sharing for efficient direct access to big data?" [23].

2. RESEARCH METHOD

The proposed cubic cipher works with 16-bytes as a state matrix of 128-bit for each independent face or dimension in the cubic algorithm. Moreover; the cubic algorithm can work with six dimensions together in a parallel form that meaning the data blocks are 6*128-bit The proposed cipher accepts 128-bits of plaintext from each side in the cube and 128-bits of ciphering secret key as the initial of entry secret key XORed at the first and last rounds according to the whitening concepts. The main operations in the round transformation involve cubic operations with six options according to the cube dimensions. The internal stages for each algorithm aggregated in the round transformation encompass four fundamental stages looped for some rounds. The implementation cubic algorithm as an individual algorithm is subject to the modular arithmetic process. The selected dimension in the cubic algorithm is determined by the least significant byte (LSB) in the ciphering key mod 7 for each round. The result will be less than 7, which represents the dimension number in the cube with range (1-6). Dimension Number (DN)=LSB mod 7. The round transformation of the proposed cipher comprises the following four main stages as stated in Figure 1.

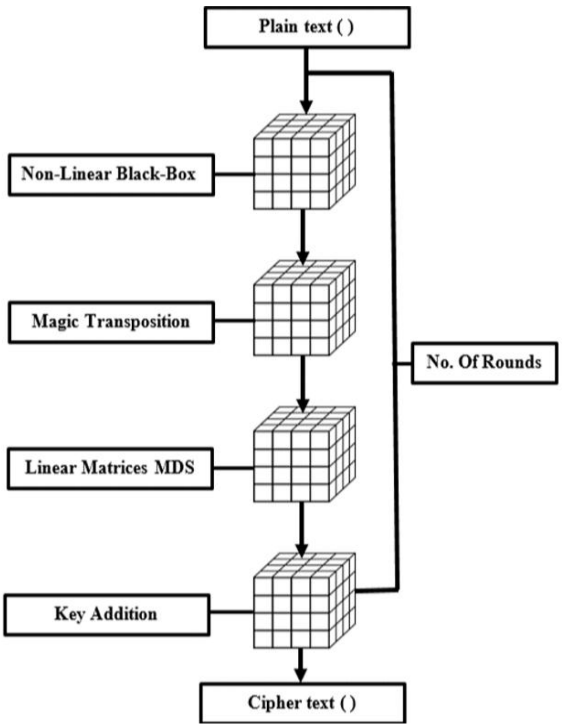

Figure 1. The cubic algorithm structure

2.1. Non-linear black-box stages

This stage is considered the most important part of designing any algorithm which determines the solidity and strength of the algorithm. The proposed black-box consists of six faces or dimensions, whereby each dimension works with the different irreducible polynomial equation as stated in Figures 2-7. The collected dimensions constitute a cube of active black-boxes and each cube face or dimension can be represented as a table lookup of 16*16 values. The intersection of the i^{th} row and j^{th} column in the table for each face gives the desired value. Each Black-box design is constructed similar to the S-Box of AES cipher in terms of taking the multiplicative inverse and applying the affine transform XORed with certain constant vectors of (V1, V2 … V6) as shown in the equations below:

$$\text{Black-S1}[x] = \text{Affine}\ (x^{-1}) + V1 \tag{1}$$

$$\text{Black-S2}[x] = \text{Affine}\ (x^{-1}) + V2 \tag{2}$$

$$\text{Black-S3}[x] = \text{Affine}\ (x^{-1}) + V3 \tag{3}$$

$$\text{Black-S4}[x] = \text{Affine}\ (x^{-1}) + V4 \tag{4}$$

$$\text{Black-S5}[x] = \text{Affine}\ (x^{-1}) + V5 \tag{5}$$

$$\text{Black-S6}[x] = \text{Affine}\ (x^{-1}) + V6 \tag{6}$$

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00	AD	4B	1C	8C	75	4D	3D	63	C1	94	DD	46	E5	F5	CA	8E
01	59	CF	F3	97	95	00	58	E6	89	3A	43	BA	DC	F4	FE	62
02	15	E8	9C	87	82	2D	72	9A	B1	3B	B9	A3	57	A0	08	C9
03	7D	D4	66	0F	18	44	E4	EF	D7	6B	01	13	C6	38	88	4A
04	33	F0	CD	0A	F7	99	B8	21	F8	C8	2F	10	42	C7	36	AB
05	61	BC	24	06	65	B0	68	CC	D0	93	E9	D2	BD	81	5D	76
06	C5	1E	D3	ED	8A	37	3E	54	77	3C	9B	F9	CB	EA	4E	AE
07	52	0D	CE	31	FB	85	F2	D5	DA	FF	A5	DF	3F	2B	5E	A4
08	20	55	03	E7	5F	6D	7E	AC	80	34	B7	E0	27	7C	29	C3
09	07	83	1F	32	EC	D9	73	BE	5A	7A	98	6E	60	6A	6C	B5
0A	09	49	25	BF	69	11	78	D8	0B	05	23	2E	4F	A8	1D	DB
0B	D1	53	70	9F	8F	7F	12	6F	67	D6	79	A1	17	E2	40	B4
0C	5B	30	B6	1A	50	4C	8D	28	FC	AA	22	41	64	0C	51	C2
0D	02	AF	A7	9D	74	92	45	8B	9E	B2	0E	71	5C	39	2C	2A
0E	90	1B	FD	BB	DE	B3	E3	35	86	FA	7B	C4	C0	04	91	19
0F	16	14	84	A2	A9	48	56	E1	26	F1	EE	F6	96	47	EB	A6

Figure 2. Forward black-box1

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00	AD	4B	E6	20	08	D6	6B	1A	47	3F	10	9F	CE	B3	4E	84
01	E0	65	DC	D2	73	6A	8C	58	24	27	A2	F3	5C	6C	39	15
02	33	C5	F1	D4	2D	96	12	C2	FA	B4	76	04	3D	48	57	79
03	69	5D	E8	3A	2A	A8	82	E4	55	01	4D	A3	E7	28	C9	C0
04	DA	59	A1	7C	BB	1F	29	FE	D5	97	30	36	4A	87	22	1E
05	3E	B6	21	FD	40	0F	41	EC	E5	45	67	9E	D0	EE	C7	51
06	F7	9D	ED	A5	37	AA	66	81	56	77	17	5A	02	49	31	94
07	E9	E1	FB	FC	DD	AE	92	DE	B0	19	6F	8A	A7	CA	1B	B7
08	16	74	EF	8E	AB	03	7D	5F	A6	07	F4	C1	D7	4F	3C	F2
09	91	FF	88	B9	5B	B2	60	C6	5E	AC	B8	61	52	46	4C	53
0A	64	AF	18	42	D3	85	BD	CD	63	99	C4	93	DB	3B	35	7F
0B	89	BA	D9	9A	C8	7B	34	0E	2B	54	0C	CB	98	2F	EB	0D
0C	80	78	B5	D1	8D	1D	A9	72	D8	9C	2E	11	70	EA	83	C3
0D	68	13	F8	75	F0	38	6E	9B	7A	50	DF	44	E3	0B	09	F5
0E	8F	F9	8B	E2	86	00	05	43	95	BE	2C	0A	32	BC	14	BF
0F	23	71	CF	A4	CC	62	06	25	90	6D	26	7E	F6	B1	A0	1C

Figure 3. Forward black-box2

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00	AD	4B	CD	ED	8E	70	8D	99	2F	A3	50	07	AE	06	B7	19
01	EC	C1	B9	E2	53	AB	EB	29	2C	7A	78	4A	A0	34	E4	87
02	1E	56	88	8C	B4	5D	0A	25	D2	6F	BD	1F	9D	F0	FC	55
03	6D	5B	46	89	54	8A	5E	98	38	2E	72	80	1A	F6	B8	AF
04	67	4E	43	8F	3F	A5	3D	79	21	59	C6	31	7E	49	FA	F3
05	12	CA	CC	FF	B6	B1	F4	9C	B5	BE	03	94	05	00	C2	4F
06	DE	CE	D6	E6	58	4D	AC	39	51	2A	2D	D8	47	D1	24	FD
07	74	18	7F	FB	42	9F	3B	7B	65	76	13	F1	27	C3	BF	23
08	C8	28	5C	17	C9	7C	BC	6A	F7	AA	A9	1B	E5	66	C7	C5
09	F8	97	C4	DC	0B	60	E3	30	44	02	DF	9E	15	75	82	A1
0A	61	A2	0D	73	1D	6B	84	6C	33	3C	B0	71	01	E0	26	EF
0B	B2	62	37	64	E9	4C	22	9B	F9	8B	68	D0	09	63	CF	95
0C	14	A8	0F	11	10	B3	08	20	57	E1	DD	16	3E	32	E7	48
0D	C0	85	7D	3A	FE	A6	04	0E	CB	D4	93	1C	69	D9	96	36
0E	52	0C	77	83	D7	EE	86	2B	5A	6E	A7	41	F5	BA	D5	D3
0F	DA	35	40	92	F2	81	90	91	E8	5F	9A	45	A4	DB	EA	BB

Figure 4. Forward black-box3

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00	AD	4B	85	9D	E2	42	B5	6B	0A	10	5A	5E	FA	49	CE	65
01	7E	87	73	E9	0D	4E	0F	0E	5D	9B	DF	39	47	03	92	71
02	44	74	B8	57	99	3A	8F	A5	FD	B0	5C	40	A7	4C	7C	EC
03	8E	9F	ED	26	CF	91	E7	1C	83	CC	A1	89	32	E1	C3	61
04	02	16	1A	31	27	43	D0	04	B7	37	66	E0	BC	B1	A9	54
05	DE	FF	23	D1	55	D4	00	B6	F3	3D	06	EE	1E	AC	56	46
06	67	C2	EF	88	8D	FB	33	F7	9C	38	B3	07	D3	6C	75	B2
07	BA	6D	1D	53	AB	15	E4	F2	62	29	8B	A6	9A	F6	90	70
08	7A	19	2B	8C	2D	5F	E3	09	E8	95	81	2E	48	C6	22	DA
09	A0	1B	BB	12	13	6A	50	2C	25	98	F8	30	AF	01	51	C5
0A	14	F0	84	77	EA	DC	93	4F	8A	64	4A	D6	20	72	7B	60
0B	82	35	E5	6F	78	D5	0C	7F	2F	D8	76	21	0B	34	58	A8
0C	C8	24	41	3B	D7	D9	3F	FC	E6	CA	86	63	B9	45	80	08
0D	6E	05	3C	BF	A2	97	A3	CB	C9	BD	4D	DB	C1	69	79	1F
0E	7D	F4	96	C7	AE	94	D2	C0	F5	CD	AA	DD	52	FE	59	C4
0F	11	9E	B4	F1	BE	EB	28	2A	36	A4	5B	3E	68	F9	18	17

Figure 5. Forward black-box4

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00	AD	4B	54	FC	51	6E	05	3D	59	DD	C6	EA	F9	1B	E5	EC
01	5D	6D	95	D5	92	94	0E	33	0D	34	F6	8E	89	6F	87	17
02	5F	37	47	F5	B1	20	91	E0	32	F2	BB	25	7C	BF	68	39
03	FD	01	EB	12	8A	7A	B6	15	35	2B	CC	0A	B8	DA	F0	BA
04	D4	A0	6A	99	52	19	0B	80	29	AB	6B	DC	B3	3C	81	90
05	62	6C	88	36	A6	CB	63	AE	CF	C5	A4	ED	4F	9D	E7	1F
06	0F	3E	FB	DB	04	96	F8	18	B4	69	46	14	AA	43	7B	D6
07	E1	2D	EE	3A	1D	E3	7E	5C	27	06	16	98	03	2A	AC	09
08	9B	C2	A1	5A	C4	F7	B7	D0	D8	C8	7D	38	74	BE	3B	9A
09	65	5B	24	DE	CE	D3	9F	41	A2	F1	EF	C7	31	4E	B9	97
0A	C0	2F	4D	23	3F	8C	60	1A	28	CD	9E	FE	CA	85	2C	48
0B	9C	84	13	BC	A3	22	8D	08	56	83	B5	E2	02	C9	F4	D2
0C	76	75	64	A5	86	B2	1C	A8	F3	49	30	A9	07	40	77	C1
0D	21	4A	45	11	58	72	71	D1	2E	E9	50	AF	4C	82	10	DF
0E	8B	C3	67	93	0C	57	66	42	7F	D9	00	79	44	61	55	5E
0F	E8	73	78	1E	FA	D7	BD	B0	70	53	E4	26	A7	E6	FF	8F

Figure 6. Forward black-box5

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00	AD	4B	A1	A5	AB	00	A9	A8	D1	51	04	F2	AF	1E	50	63
01	93	BD	AC	C9	06	C1	7D	96	D3	A6	0B	F9	53	98	CA	9D
02	CD	42	DA	D9	52	77	E0	BE	78	66	E4	FE	C5	CB	30	FA
03	ED	DF	28	F7	81	24	F8	01	D2	11	48	5F	61	D8	B5	89
04	E2	B1	5A	3C	16	32	97	2B	2D	DD	BF	6C	74	56	5B	C3
05	38	EC	37	7C	76	64	7B	A2	E6	36	9E	A0	1C	10	79	7F
06	8D	6A	EB	5D	6F	7E	80	46	C4	09	69	F0	07	90	FB	4E
07	12	35	8C	C8	20	83	D4	8F	B4	0C	68	41	DE	9C	C0	D5
08	0A	7A	DC	B2	29	94	1A	17	0F	E9	62	67	CF	A3	EE	8A
09	92	5E	95	70	A4	71	4D	D0	3E	B3	2F	0E	D6	F6	9A	B7
0A	18	8B	72	45	9F	FD	3A	F5	40	F4	49	E7	B9	E5	2A	B6
0B	08	59	60	43	34	CE	54	13	75	25	73	9B	C7	33	BB	05
0C	C2	84	31	F3	F1	88	AA	15	CC	85	44	2C	3B	23	58	27
0D	19	22	FF	EF	B0	B8	03	AE	87	55	4C	D7	86	47	5C	A7
0E	0D	E3	E1	82	3D	65	1F	39	6B	2E	BA	8E	6E	FC	BC	3F
0F	21	26	02	6D	4F	1D	DB	C6	14	57	4A	E8	1B	99	91	EA

Figure 7. Forward black-box6

2.2. Inverse-non-linear black-box

The inverse Black box stage involves the construction of inverse-cube of six inv-black box lookup tables, where each with 256-bytes and with different irreducible polynomial as stated in Figures 8-13. When the encryption is done by the forward black-box1 the decryption should be by backward inv-black-box1 to ensure the compatibility operations, because the black-box tables are designed with different affine equations, different irreducible polynomials and various constant vectors.

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00	15	3A	D0	82	ED	A9	53	90	2E	A0	43	A8	CD	71	DA	33
01	4B	A5	B6	3B	F1	20	F0	BC	34	EF	C3	E1	02	AE	61	92
02	80	47	CA	AA	52	A2	F8	8C	C7	8E	DF	7D	DE	25	AB	4A
03	C1	73	93	40	89	E7	4E	65	3D	DD	19	29	69	06	66	7C
04	BE	CB	4C	1A	35	D6	0B	FD	F5	A1	3F	01	C5	05	6E	AC
05	C4	CE	70	B1	67	81	F6	2C	16	10	98	C0	DC	5E	7E	84
06	9C	50	1F	07	CC	54	32	B8	56	A4	9D	39	9E	85	9B	B7
07	B2	DB	26	96	D4	04	5F	68	A6	BA	99	EA	8D	30	86	B5
08	88	5D	24	91	F2	75	E8	23	3E	18	64	D7	03	C6	0F	B4
09	E0	EE	D5	59	09	14	FC	13	9A	45	27	6A	22	D3	D8	B3
0A	2D	BB	F3	2B	7F	7A	FF	D2	AD	F4	C9	4F	87	00	6F	D1
0B	55	28	D9	E5	BF	9F	C2	8A	46	2A	1B	E3	51	5C	97	A3
0C	EC	08	CF	8F	EB	60	3C	4D	49	2F	0E	6C	57	42	72	11
0D	58	B0	5B	62	31	77	B9	38	A7	95	78	AF	1C	0A	E4	7B
0E	8B	F7	BD	E6	36	0C	17	83	21	5A	6D	FE	94	63	FA	37
0F	41	F9	76	12	1D	0D	FB	44	48	6B	E9	74	C8	E2	1E	79

Figure 8. Backward black-box1

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00	E5	39	6C	85	2B	E6	F6	89	04	DE	EB	DD	BA	BF	B7	55
01	0A	CB	26	D1	EE	1F	80	6A	A2	79	07	7E	FF	C5	4F	45
02	03	52	4E	F0	18	F7	FA	19	3D	46	34	B8	EA	24	CA	BD
03	4A	6E	EC	20	B6	AE	4B	64	D5	1E	33	AD	8E	2C	50	09
04	54	56	A3	E7	DB	59	9D	08	2D	6D	4C	01	9E	3A	0E	8D
05	D9	5F	9C	9F	B9	38	68	2E	17	41	6B	94	1C	31	98	87
06	96	9B	F5	A8	A0	11	66	5A	D0	30	15	06	1D	F9	D6	7A
07	CC	F1	C7	14	81	D3	2A	69	C1	2F	D8	B5	43	86	FB	AF
08	C0	67	36	CE	0F	A5	E4	4D	92	B0	7B	E2	16	C4	83	E0
09	F8	90	76	AB	6F	E8	25	49	BC	A9	B3	D7	C9	61	5B	0B
0A	FE	42	1A	3B	F3	63	88	7C	35	C6	65	84	99	00	75	A1
0B	78	FD	95	0D	29	C2	51	7F	9A	93	B1	44	ED	A6	E9	EF
0C	3F	8B	27	CF	AA	21	97	5E	B4	3E	7D	BB	F4	A7	0C	F2
0D	5C	C3	13	A4	23	48	05	8C	C8	B2	40	AC	12	74	77	DA
0E	10	71	E3	DC	37	58	02	3C	32	70	CD	BE	57	62	5D	82
0F	D4	22	8F	1B	8A	DF	FC	60	D2	E1	28	72	73	53	47	91

Figure 9. Backward black-box2

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00	5D	AC	99	5A	D6	5C	0D	0B	C6	BC	26	94	E1	A2	D7	C2
01	C4	C3	50	7A	C0	9C	CB	83	71	0F	3C	8B	DB	A4	20	2B
02	C7	48	B6	7F	6E	27	AE	7C	81	17	69	E7	18	6A	39	08
03	97	4B	CD	A8	1D	F1	DF	B2	38	67	D3	76	A9	46	CC	44
04	F2	EB	74	42	98	FB	32	6C	CF	4D	1B	01	B5	65	41	5F
05	0A	68	E0	14	34	2F	21	C8	64	49	E8	31	82	25	36	F9
06	95	A0	B1	BD	B3	78	8D	40	BA	DC	87	A5	A7	30	E9	29
07	05	AB	3A	A3	70	9D	79	E2	1A	47	19	77	85	D2	4C	72
08	3B	F5	9E	E3	A6	D1	E6	1F	22	33	35	B9	23	06	04	43
09	F6	F7	F3	DA	5B	BF	DE	91	37	07	FA	B7	57	2C	9B	75
0A	1C	9F	A1	09	FC	45	D5	EA	C1	8A	89	15	66	00	0C	3F
0B	AA	55	B0	C5	24	58	54	0E	3E	12	ED	FF	86	2A	59	7E
0C	D0	11	5E	7D	92	8F	4A	8E	80	84	51	D8	52	02	61	BE
0D	BB	6D	28	EF	D9	EE	62	E4	6B	DD	F0	FD	93	CA	60	9A
0E	AD	C9	13	96	1E	8C	63	CE	F8	B4	FE	16	10	03	E5	AF
0F	2D	7B	F4	4F	56	EC	3D	88	90	B8	4E	73	2E	6F	D4	53

Figure 10. Backward black-box3

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00	56	9D	40	1D	47	D1	5A	6B	CF	87	08	BC	B6	14	17	16
01	09	F0	93	94	A0	75	41	FF	FE	81	42	91	37	72	5C	DF
02	AC	BB	8E	52	C1	98	33	44	F6	79	F7	82	97	84	8B	B8
03	9B	43	3C	66	BD	B1	F8	49	69	1B	25	C3	D2	59	FB	C6
04	2B	C2	05	45	20	CD	5F	1C	8C	0D	AA	01	2D	DA	15	A7
05	96	9E	EC	73	4F	54	5E	23	BE	EE	0A	FA	2A	18	0B	85
06	AF	3F	78	CB	A9	0F	4A	60	FC	DD	95	07	6D	71	D0	B3
07	7F	1F	AD	12	21	6E	BA	A3	B4	DE	80	AE	2E	E0	10	B7
08	CE	8A	B0	38	A2	02	CA	11	63	3B	A8	7A	83	64	30	26
09	7E	35	1E	A6	E5	89	E2	D5	99	24	7C	19	68	03	F1	31
0A	90	3A	D4	D6	F9	27	7B	2C	BF	4E	EA	74	5D	00	E4	9C
0B	29	4D	6F	6A	F2	06	57	48	22	CC	70	92	4C	D9	F4	D3
0C	E7	DC	61	3E	EF	9F	8D	E3	C0	D8	C9	D7	39	E9	0E	34
0D	46	53	E6	6C	55	B5	AB	C4	B9	C5	8F	DB	A5	EB	50	1A
0E	4B	3D	04	86	76	B2	C8	36	88	13	A4	F5	2F	32	5B	62
0F	A1	F3	77	58	E1	E8	7D	67	9A	FD	0C	65	C7	28	ED	51

Figure 11. Backward black-box4

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00	EA	31	BC	7C	64	06	79	CC	B7	7F	3B	46	E4	18	16	60
01	DE	D3	33	B2	6B	37	7A	1F	67	45	A7	0D	C6	74	F3	5F
02	25	D0	B5	A3	92	2B	FB	78	A8	48	7D	39	AE	71	D8	A1
03	CA	9C	28	17	19	38	53	21	8B	2F	73	8E	4D	07	61	A4
04	CD	97	E7	6D	EC	D2	6A	22	AF	C9	D1	01	DC	A2	9D	5C
05	DA	04	44	F9	02	EE	B8	E5	D4	08	83	91	77	10	EF	20
06	A6	ED	50	56	C2	90	E6	E2	2E	69	42	4A	51	11	05	1D
07	F8	D6	D5	F1	8C	C1	C0	CE	F2	EB	35	6E	2C	8A	76	E8
08	47	4E	DD	B9	B1	AD	C4	1E	52	1C	34	E0	A5	B6	1B	FF
09	4F	26	14	E3	15	12	65	9F	7B	43	8F	80	B0	5D	AA	96
0A	41	82	98	B4	5A	C3	54	FC	C7	CB	6C	49	7E	00	57	DB
0B	F7	24	C5	4C	68	BA	36	86	3C	9E	3F	2A	B3	F6	8D	2D
0C	A0	CF	81	E1	84	59	0A	9B	89	BD	AC	55	3A	A9	94	58
0D	87	D7	BF	95	40	13	6F	F5	88	E9	3D	63	4B	09	93	DF
0E	27	70	BB	75	FA	0E	FD	5E	F0	D9	0B	32	0F	5B	72	9A
0F	3E	99	29	C8	BE	23	1A	85	66	0C	F4	62	03	30	AB	FE

Figure 12. Backward black-box5

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00	05	37	F2	D6	0A	BF	14	6C	B0	69	80	1A	79	E0	9B	88
01	5D	39	70	B7	F8	C7	44	87	A0	D0	86	FC	5C	F5	0D	E6
02	74	F0	D1	CD	35	B9	F1	CF	32	84	AE	47	CB	48	E9	9A
03	2E	C2	45	BD	B4	71	59	52	50	E7	A6	CC	43	E4	98	EF
04	A8	7B	21	B3	CA	A3	67	DD	3A	AA	FA	01	DA	96	6F	F4
05	0E	09	24	1C	B6	D9	4D	F9	CE	B1	42	4E	DE	63	91	3B
06	B2	3C	8A	0F	55	E5	29	8B	7A	6A	61	E8	4B	F3	EC	64
07	93	95	A2	BA	4C	B8	54	25	28	5E	81	56	53	16	65	5F
08	66	34	E3	75	C1	C9	DC	D8	C5	3F	8F	A1	72	60	EB	77
09	6D	FE	90	10	85	92	17	46	1D	FD	9E	BB	7D	1F	5A	A4
0A	5B	02	57	8D	94	03	19	DF	07	06	C6	04	12	00	D7	0C
0B	D4	41	83	99	78	3E	AF	9F	D5	AC	EA	BE	EE	11	27	4A
0C	7E	15	C0	4F	68	2C	F7	BC	73	13	1E	2D	C8	20	B5	8C
0D	97	08	38	18	76	7F	9C	DB	3D	23	22	F6	82	49	7C	31
0E	26	E2	40	E1	2A	AD	58	AB	FB	89	FF	62	51	30	8E	D3
0F	6B	C4	0B	C3	A9	A7	9D	33	36	1B	2F	6E	ED	A5	2B	D2

Figure 13. Backward black-box6

2.3. Internal magic transposition

The Magic transposition acts as the second stage of the round transformation in the proposed algorithm. The main notation beyond the internal magic transposition is to map the values' positions to other different positions. The magic transposition stage also involves a cube of six dimensions whereby each dimension is arranged according to the doubly even magic square of 4*4 as shown in Figure 14. The magic square of doubly even order is a matrix of (4 m), whereby the order of matrix can be divided by 2 and 4 [24]. The core idea for the design magic cube basically depends on a folded magic square notation that has presented in [25].

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

32	18	19	29
21	27	26	24
25	23	22	28
20	30	31	17

64	50	51	61
53	59	58	56
57	55	54	60
52	62	63	49

80	66	67	77
69	75	74	72
73	71	70	76
68	78	79	65

96	82	83	93
85	91	90	88
89	87	86	92
84	94	95	81

112	98	99	109
101	107	106	104
105	103	102	108
100	110	111	97

Figure 14. Six dimensions of doubly even magic square transposition

2.4. The internal linear matrices stages

The proposed cipher adopts six of new linear MDS codes with their inverses coefficients dedicated for each dimension cube as stated in (7-12). The linear stage is implemented with addition and multiplication operations. The essence mathematical clue is based on Galois field GF (2^8) that works separately with each face in the cubic structure. The proposed linear codes can be represented as maximum distance separable (MDS) matrices. The linear MDS matrices code is implemented as a column-by-column multiplication modulo the reducible polynomial of x^4+1.

$$\begin{bmatrix} S'_{0,c} \\ S'_{1,c} \\ S'_{2,c} \\ S'_{3,c} \end{bmatrix} \otimes \begin{bmatrix} 04 & 07 & 04 & 06 \\ 06 & 04 & 07 & 04 \\ 04 & 06 & 04 & 07 \\ 07 & 04 & 06 & 04 \end{bmatrix} = \begin{bmatrix} S_{0,c} \\ S_{1,c} \\ S_{2,c} \\ S_{3,c} \end{bmatrix} \otimes \begin{bmatrix} 04 & 06 & 04 & 07 \\ 07 & 04 & 06 & 04 \\ 04 & 07 & 04 & 06 \\ 06 & 04 & 07 & 04 \end{bmatrix} = \begin{bmatrix} S'_{0,c} \\ S'_{1,c} \\ S'_{2,c} \\ S'_{3,c} \end{bmatrix} \quad (7)$$

$$\begin{bmatrix} S'_{0,c} \\ S'_{1,c} \\ S'_{2,c} \\ S'_{3,c} \end{bmatrix} \otimes \begin{bmatrix} 05 & 07 & 05 & 06 \\ 06 & 05 & 07 & 05 \\ 05 & 06 & 05 & 07 \\ 07 & 05 & 06 & 05 \end{bmatrix} = \begin{bmatrix} S_{0,c} \\ S_{1,c} \\ S_{2,c} \\ S_{3,c} \end{bmatrix} \otimes \begin{bmatrix} 05 & 06 & 05 & 07 \\ 07 & 05 & 06 & 05 \\ 05 & 07 & 05 & 06 \\ 06 & 05 & 07 & 05 \end{bmatrix} = \begin{bmatrix} S'_{0,c} \\ S'_{1,c} \\ S'_{2,c} \\ S'_{3,c} \end{bmatrix} \quad (8)$$

$$\begin{bmatrix} S'_{0,c} \\ S'_{1,c} \\ S'_{2,c} \\ S'_{3,c} \end{bmatrix} \otimes \begin{bmatrix} 07 & 05 & 06 & 05 \\ 05 & 07 & 05 & 06 \\ 06 & 05 & 07 & 05 \\ 05 & 06 & 05 & 07 \end{bmatrix} = \begin{bmatrix} S_{0,c} \\ S_{1,c} \\ S_{2,c} \\ S_{3,c} \end{bmatrix} \otimes \begin{bmatrix} 07 & 05 & 06 & 05 \\ 05 & 07 & 05 & 06 \\ 06 & 05 & 07 & 05 \\ 05 & 06 & 05 & 07 \end{bmatrix} = \begin{bmatrix} S'_{0,c} \\ S'_{1,c} \\ S'_{2,c} \\ S'_{3,c} \end{bmatrix} \quad (9)$$

$$\begin{bmatrix} S'_{0,c} \\ S'_{1,c} \\ S'_{2,c} \\ S'_{3,c} \end{bmatrix} \otimes \begin{bmatrix} 04 & 05 & 06 & 06 \\ 06 & 04 & 05 & 06 \\ 06 & 06 & 04 & 05 \\ 05 & 06 & 06 & 04 \end{bmatrix} = \begin{bmatrix} S_{0,c} \\ S_{1,c} \\ S_{2,c} \\ S_{3,c} \end{bmatrix} \otimes \begin{bmatrix} 0e & 0a & 0c & 09 \\ 09 & 0e & 0a & 0c \\ 0c & 09 & 0e & 0a \\ 0a & 0c & 09 & 0e \end{bmatrix} = \begin{bmatrix} S'_{0,c} \\ S'_{1,c} \\ S'_{2,c} \\ S'_{3,c} \end{bmatrix} \quad (10)$$

$$\begin{bmatrix} S'_{0,c} \\ S'_{1,c} \\ S'_{2,c} \\ S'_{3,c} \end{bmatrix} \otimes \begin{bmatrix} 03 & 04 & 01 & 07 \\ 07 & 03 & 04 & 01 \\ 01 & 07 & 03 & 04 \\ 04 & 01 & 07 & 03 \end{bmatrix} = \begin{bmatrix} S_{0,c} \\ S_{1,c} \\ S_{2,c} \\ S_{3,c} \end{bmatrix} \otimes \begin{bmatrix} 09 & 0b & 0b & 08 \\ 08 & 09 & 0b & 0b \\ 0b & 08 & 09 & 0b \\ 0b & 0b & 08 & 09 \end{bmatrix} = \begin{bmatrix} S'_{0,c} \\ S'_{1,c} \\ S'_{2,c} \\ S'_{3,c} \end{bmatrix} \quad (11)$$

$$\begin{bmatrix} S'_{0,c} \\ S'_{1,c} \\ S'_{2,c} \\ S'_{3,c} \end{bmatrix} \otimes \begin{bmatrix} 03 & 06 & 01 & 05 \\ 05 & 03 & 06 & 01 \\ 01 & 05 & 03 & 06 \\ 06 & 01 & 05 & 03 \end{bmatrix} = \begin{bmatrix} S_{0,c} \\ S_{1,c} \\ S_{2,c} \\ S_{3,c} \end{bmatrix} \otimes \begin{bmatrix} 09 & 09 & 0b & 0a \\ 0a & 09 & 09 & 0b \\ 0b & 0a & 09 & 09 \\ 09 & 0b & 0a & 09 \end{bmatrix} = \begin{bmatrix} S'_{0,c} \\ S'_{1,c} \\ S'_{2,c} \\ S'_{3,c} \end{bmatrix} \quad (12)$$

The proposed MDS matrices size is 4*4 like the MDS of AES cipher which is responsible for achieving the confusion and diffusion scheme to the whole structure. The proposed matrices transformations have been chosen from the best solutions we have acquired. The search process for getting the proposed linear equations of order four was computerized automatically. The mathematical software was programmed with Visual Studio C# 2013 under the Windows-10 operating system of 64-bit CPU Intel (R) Core i7 2.65GHz and RAM 8-GB. The inverse MDS matrices linear codes are implemented by using the inverse matrix coefficients in backward operations. All the submitted MDS matrices have been verified as active equations by multiplying the forward matrices by backward matrices. The multiplication result gives the identity matrix for each couple of corresponding matrices. So, the decryption process in each round is implemented by multiplying the Inv-MDS code according to the dimension number with the corresponding encryption MDS code.

2.5. Key addition layer

This is the last stage in the round transformation and the most sensitive stage that determines the strength of the secret ciphering key. The key addition stage involves the key expansion technique for the key generation process that covers all the rounds. The ciphering sub-keys are generated by two complex functions for only one dimension can be shown in Figure 15. Each function consists of three complex operations that increase the complexity of the ciphering key and each one accepts 128-bit of initial entry key. The complex function includes three internal operations of subbyte operation, complement operation and XORed with the constant vector or byte-rotate process. The LSB byte in the ciphering key takes the mod operation for the number seven (mod 7) to determine which face or dimension in the cube through which the encryption process will be implemented in each round.

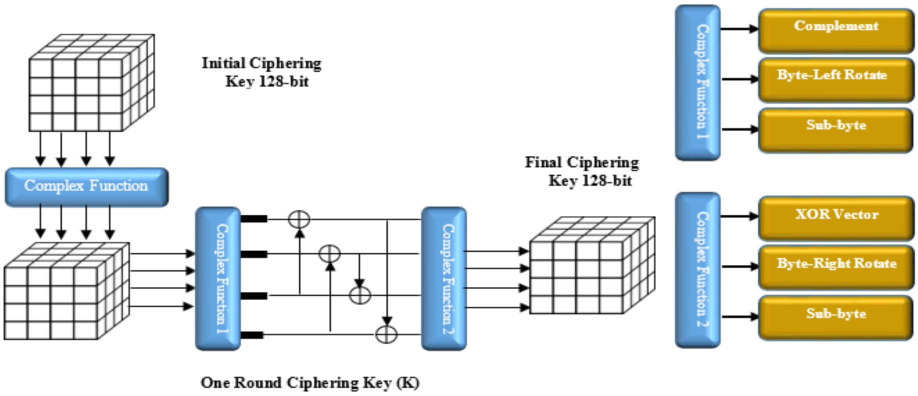

Figure 15. One dimension key generation algorithm of one-round

3. RESULTS AND DISCUSSION

Big data opened the door in front of several sophisticated challenges and numerous information security responsibilities. The proposed cipher can be analyzed from all directions to cover all design details and to figure out the internal operations. The cubic algorithm is designed with a solid round transformation that has six separate paths each of them traverses an independent algorithm. The selection path determines which cube dimension is selected and will be dedicated to encryption. The proposed algorithm adopts a strong secret key that makes the linear and differential attacks very hard. The proposed structure is a composed structure with multi-similar structures that work in parallel simultaneously. Moreover, each algorithm can work as an individual autonomous algorithm. The secret ciphering key is provided with two complex functions that work to prevent the weak/semi-weak sub-keys from appearance through the generation process. The round symmetry for the key scheduling adds an extra layer against the related-key attacks and the square attack. The proposed structure includes six active Black-box tables that apply a high nonlinearity and confusion against the linear and differential attacks. The magic shifting with six dimensions is a new direction for the design secrets with an optimal diffusion to defend the correlation attack. The six different linear MDS codes have been distributed into the proposed cubic dimensions independently. The product cipher with collected stages is affected greatly to the different propagation probabilities of the plaintext and ciphertext for the whole rounds. Furthermore, the product cipher will distribute the number of trails and weights for each bricklayer function iteratively. The differential properties for the algebraic aspects and the multiplicative inverse over Galois Field (GF 2^8) have been extended for multi-power.

The timing attack becomes impossible for the mathematical internal operations since the algorithm has a balance cubic structure. The balanced structure means that the same implementation time for the encryption and decryption operations in all dimensions. The multiplication process by the MDS code for the linear layer tends to be converged due to equality linear coefficients. The proposed MDS coefficients are almost convergent because they carry the same upper bound of coefficients. Thus, probably there is no leakage information throughout the computation process and consequently, the power analysis attack and timing attacks are very hard. The proposed cipher is focusing on increasing the security layer by preventing the attack from detecting the statistics' weakness. The ciphering sub-keys are implemented to enhance the security level by encountering all types of cryptanalysis attacks. The proposed cipher adopts an effective strategy for defeating the linear and differential attacks within a multi-dimensional framework. The whole randomness tests released by the National Institute and Standard Technology (NIST) have experimented on the acquired results. The outcome of these tests did not give any fluctuation at randomness boundaries. All of these aspects and tests are taken into account through the designing process. Simple tests for the speed measurement and a number of code lines of the proposed cipher and the original AES is shown in Table 1.

Table 1. Comparison between the proposed model and the original AES

Algorithm cipher	Block cipher	Key length	No. of rounds	Clock cycle of key scheduling	Clock cycle of encryption process	Code size-assembly language
Cubic-dimension1	128-bit	128-bit	10-rounds	12050	13580	10430
Cubic-dimension2	128-bit	128-bit	10-rounds	12850	13595	10520
Cubic-dimension3	128-bit	128-bit	10-rounds	12670	13860	10380
Cubic-dimension4	128-bit	128-bit	10-rounds	12400	14670	10480
Cubic-dimension5	128-bit	128-bit	10-rounds	12890	14400	10600
Cubic-dimension6	128-bit	128-bit	10-rounds	12760	14870	10510
The standard AES	128-bit	128-bit	10-rounds	11050	12930	9150

The encryption and decryption implementation time is measured for the proposed cipher according to each dimension independently and compared with the AES standard cipher as shown in Figure 16. The implementation time of the decryption process for the proposed ciphers is varied smoothly from one- dimensional algorithm to another. The time differentiation is occurred due to the coefficients differences in the proposed mathematical equations.

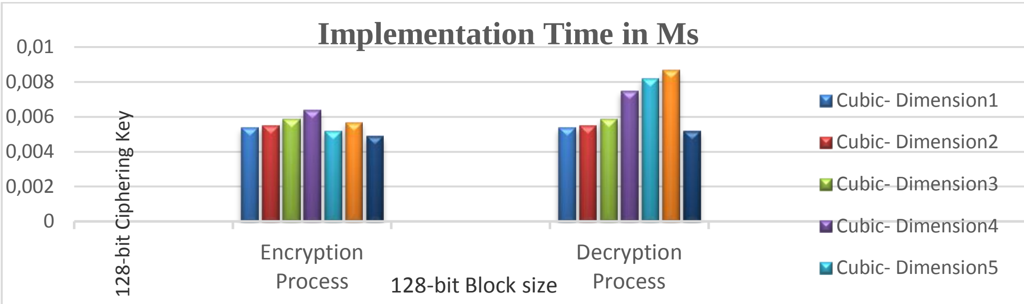

Figure 16. Comparison of time implementation encryption/decryption process

4. CONCLUSION

A novel cubic symmetric cipher algorithm has been proposed and developed of round transformation with six dimensions and ten iterated rounds. The proposed cipher has the ability to encrypt the data with multi-dimensional algorithms that compensate for six collected cryptographic algorithms working together. The proposed algorithm includes various mathematical backgrounds of the finite field over $GF(2^8)$ and magic square mathematical formula. The developed cipher works to encrypt the128-bit block of data for each dimension independently. Moreover, the main structure can be implemented in parallel from all directions of the cube to increase the speed of the encryption rate in busy servers. The cubic cipher provides a high margin of confidentiality and flexibility in the implementation. The implementation process can be individual or in parallel with a multi-dimensional structure to satisfy the big data needs and the development of technology in different disciplinary fields. The cubic cipher algorithm introduces a modern design structure with accepted results that are almost close to the results of the standard algorithms.

REFERENCES

[1] Chandrashekhar Meshram, “The beta cryptosystem”, *Bulletin of Electrical Engineering and Informatics*, vol. 4, no. 2, pp. 155-159, June 2015.
[2] A. Seghier and J. Li, “Advanced encryption standard based on key dependent S-Box cube”. *IET Information Security*, vol. 13, no. 6, pp.552-558, Mar. 2019.
[3] O. Dawood, A. M. S. Rahma, and A. M. J. Abdul Hossen, “New symmetric cipher fast algorithm of revertible operations’ queen (FAROQ) cipher,” *Int. J. Comput. Netw. Inf. Secur.*, vol. 9, no. 4, pp. 29-36, Apr. 2017.
[4] O. Dawood, M. Khalaf, F. M. Mohammed, and H. K. Almulla, “Design a compact non-linear s-box with multiple-affine transformations,” *In International Conference on Applied Computing to Support Industry,* Springer, Cham, pp. 439-452. Sep. 2019.
[5] A. H. Al-Hamami and A. A. Flayyih, “Enhancing Big Data analysis by using map-reduce technique,” *Bulletin of Electrical Engineering and Informatics*, vol. 7, no. 1, pp. 113-116, March 2018.
[6] J. H. Abawajy, A. Kelarev, and M. Chowdhury, “Large iterative multitier ensemble classifiers for security of big data,” *IEEE Trans. Emerg. Top. Comput.*, vol. 2, no. 3, pp. 352-363, 2014.
[7] S. H. Kim, N. U. Kim, and T. M. Chung, “Attribute relationship evaluation methodology for big data security,” *2013 Int. Conf. IT Converg. Secur. ICITCS IEEE 2013*, pp.1-4.
[8] T. Mahmood and U. Afzal, “Security analytics: Big Data analytics for cybersecurity,” *2nd Natl. Conf. Inf. Assur.*, pp. 129-134, 2013.
[9] G. Markowsky, “Crowdsourcing, Big Data and homeland security,” in *2013 IEEE International Conference on Technologies for Homeland Security, HST 2013*, pp. 772-778, 2013.
[10] Xinhua Dong, Ruixuan Li, Heng He, Wanwan Zhou, Zhengyuan Xue, and Hao Wu, “Secure sensitive data sharing on a big data platform,” *Tsinghua Sci. Technol.*, vol. 20, no. 1, pp. 72-80, 2015.
[11] V. Yadav, M. Verma, and V. Dixit Kaushik, “A biometric approach to secure big data,” *2016 1st Int. Conf. Innov. Challenges Cyber Secur. ICICCS 2016*, pp. 75-79, 2016.
[12] X. Lai and J. L. Massey, “A proposal for a new block encryption standard,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 473 LNCS, pp. 389-404, 1991.

[13] C. Mitchell, "On the security of 2-key triple DES," *IEEE Transactions on Information Theory*. vol. 62, no. 1, pp. 6260-6267, Sep. 2016.
[14] J. Daemen and V. Rijmen, "The design of Rijndael: AES-the advanced encryption standard," Springer Science & Business Media, p. 238, 2013.
[15] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson, "The Twofish Encryption Algorithm: a 128-Bit Block Cipher," John Wiley & Sons, 1999.
[16] E. Biham, R. Anderson, L. Knudsen and H. Technion, "Serpent: A flexible block cipher with maximum assurance," *in The first AES Candidate Conference*, pp. 589-606, 1998.
[17] I. B. M. Mars and T. May, "MARS and the AES selection criteria," Security, *3rd International AES Conference*, NY, USA, April 2000.
[18] R. L. Rivest, M. J. B. Robshaw, R. Sidney, and Y. L. Yin, "The RC6 block cipher," *Proc. of the 1st AES candidate conference*, CD-1: Documentation, pp.1-16, 1998.
[19] Yan Yan, Hao Xiaohong, and Wang Wanjun, "Location-based services and privacy protection under mobile cloud computing," *Bulletin of Electrical Engineering and Informatics*, vol. 4, no. 4, pp. 345-354, December 2015.
[20] A. Sagheer, S. Al-Rawi, and O. Dawood, "Proposing of developed advance encryption standard", *4th Int.Conf. on Developments in eSystems Engineering DeSE.*, *IEEE*, Dubai, pp. 197-202, 2011.
[21] O. Dawood, A. M. Sagheer, and S. S. Al-Rawi, "Design large symmetric algorithm for securing Big Data," in *11th International Conference on Developments in eSystems Engineering (DeSE)*, pp. 123-128, 2018.
[22] R. Kashyap and A. Piersson, "Impact of Big Data on security," In *Handbook of Research on Network Forensics and Analysis Techniques*, IGI Global, pp. 283-299, 2019.
[23] A. Cuzzocrea, "Privacy and security of big data: current challenges and future research perspectives," in *Proceedings of The First International Workshop on Privacy and Security of Big Data*, pp. 45-47, Nov. 2014.
[24] O. Dawood, A. Rahma, and A. Hossen, "Generalized method for constructing magic cube by folded magic squares," *Int. J. Intell. Syst. Appl.*, vol. 8, no. 1, pp. 1-8, 2016.
[25] H. Behforooz, "Behforooz-Franklin Magic Square with US Election Years," *Journal of Recreational Mathematics*, vol. 35, no. 1, pp.37-38, 2009.