1. Hamed Shawky Zied [1], 2. Ahmed Gamal Abdellatif Ibrahim [2], 3. Ahmed Ibrahim Salem [3]

[1,2]Department of Communications and Electronics Engineering, Air Defense College, Alexandria, Egypt, ,[2] Department of Electrical Engineering, Faculty of Engineering, Damanhur University, Egypt.
ORCID: 1. 0000-0002-3243-3148, 2. 0000-0002-3440-8448, 3. 0000-0002-1457-8781

doi:10.15199/48.2023.04.48

S-Box Modification for the Block Cipher Algorithms

Abstract*. Block cipher algorithm also known as a symmetric key cryptography that depends on substitution boxes (S-boxes) for the purpose of providing the element of data confusion. Therefore, the cryptographic system is being affected by S-box. Performing an effective S-box has become a new defiance for the purpose of bringing up an efficient and safe encryption algorithm. Throughout this paper, Rubik's cube is utilized for the reason of generating AES S-boxes (as an example of the block cipher algorithm) and the shuffling process is executed under the domination of the secret key. The reason of making the security analysis of the modified AES is to discuss the performance of developed AES. The analysis assures that the modified AES is safe for securing vital data. Finally, the experimental results and security analysis show that the proposed modification of the s-box boosts the block cipher security (AES).*

Streszczenie. *Algorytm szyfrowania blokowego znany również jako kryptografia z kluczem symetrycznym, który polega na polach podstawienia (S-boxach) w celu zapewnienia elementu pomieszania danych. Dlatego S-box ma wpływ na system kryptograficzny. Wykonanie skutecznego S-boxa stało się nowym wyzwaniem w celu stworzenia wydajnego i bezpiecznego algorytmu szyfrowania. W całym artykule kostka Rubika jest wykorzystywana do generowania S-boxów AES (jako przykład algorytmu szyfrowania blokowego), a proces tasowania odbywa się pod dominacją tajnego klucza. Powodem przeprowadzenia analizy bezpieczeństwa zmodyfikowanego AES jest omówienie wydajności rozwiniętego AES. Analiza zapewnia, że zmodyfikowany algorytm AES jest bezpieczny dla zabezpieczenia ważnych danych. Wreszcie wyniki eksperymentów i analiza bezpieczeństwa pokazują, że proponowana modyfikacja S-box zwiększa bezpieczeństwo szyfru blokowego (AES). (**Modyfikacja S-Box dla algorytmów szyfru blokowego**)*

Keywords: AES, S-box; Rubik's cube, image encryption, differential attack, statistical attack, encryption quality.
Słowa kluczowe: AES, skrzynka S; Kostka Rubika, szyfrowanie obrazu, atak różnicowy, atak statystyczny, jakość szyfrowania.

Introduction

Due to the high risk in exchanging data in antagonistic environments, Information safety and security is a necessity for the time being. Unauthorized users are liable to get access to the data that are shared over open networks which threaten such data by making it available to the public. For this reason, securing data (audio, image, video, etc.….) has been a serious issue. Cryptography is defined as the knowledge of examining variant methods for the purpose of securing communication to stifle the process of eavesdropping data transferred over insecure channels which is done by the intruders. Many algorithms are being utilized in securing data by using encryption. Each cryptosystem has a diverse method in mingling data in order to be hard for antagonists to bring it back to its genuine form. Cryptosystems is categorized into symmetric-key and asymmetric-key systems. Symmetric-key systems utilize the same key in encryption and decryption processes. It present high safety, but the key exchange is not easy. It relies on S-box to produce data confusion and lessen the correlation that happens between secret key and encrypted data like (DES, Serpent, and AES). S-box has a big influence on the cryptosystem performance because it is the only non-linear component in the system [1-2]. In this paper a modification for the block cipher S-boxes are presented, this proposal applied for serpent algorithm [3], and in this work will be applied on AES. AES also distinguished by its original name Rijndael. This algorithm has the feature of encryption and decryption for sensitive data and can be applied in all devices, whether hardware or software, all over the world to date. AES can handle three different size keys 128, 192 and 256 bits [4]. There are four types of transformation performed in each AES round: Sub-Byte, Shift-Row, Mix-Column, and Add-Round-Key as detected in [5]. In this proposal we replaced the original S-box with Rubik's cube to enhance non-linearity in the AES.

S-BOX Characteristics

The characteristics of S-boxes have frequently been used as the foundation for novel encryption techniques such as rigorous avalanche criterion, differential uniformity, and nonlinearity [6].

A (x,y)-S-box is a map, S :{0,1}x →{0,1}y.

It comprises of n-variable component Boolean functions: (f_1 (x_1 ,…,x_n),f_2 (x_1 ,…,x_n),…,f_n(x_1 ,…,x_n)) each of which need to satisfy S-box properties. The following are the list of several properties in S-box.

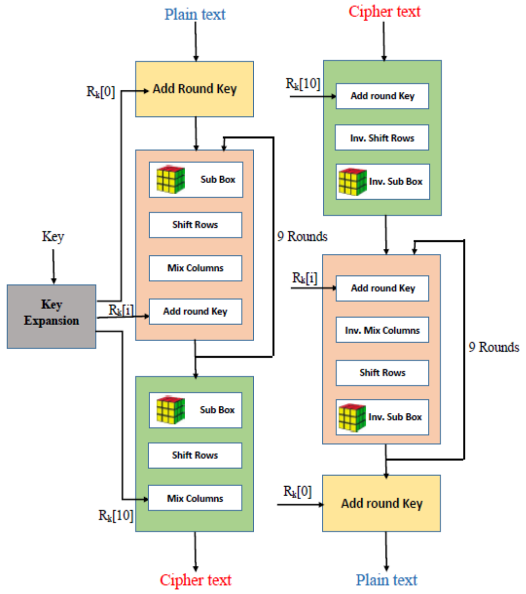

Fig.1. The modified AES encryption algorithm.

A) Robustness

Let F = (f1 ,f2 ,...,fn) be an n × n S-box, where fi is an S-box mapping component function.
fi : {0, 1}n →{0, 1}

$$(1)\quad R = \left(1-\frac{N}{2^n}\right)\left(1-\frac{L}{2^n}\right)$$

F must be Robust to against differential cryptanalysis.

B) Balancing

The greater the degree of function imbalance, so the higher the likelihood of attaining a linear approximation, according to the importance of the balancing feature. And can be defined from:

S:{0,1}n→{0,1}m balanced, if HW(f) = 2n-1.

C) Strict Avalanche Criterion (SAC)

A change in one bit of the S- box's input bits should result in a change in half of the S- box's output bits. When trying to devise an attack, it is more difficult to analyze cipher text. A cryptographic function is said to meet the strict avalanche criteria if it satisfies the requirement.

D) Nonlinearity

S :{0,1}x →{0,1}y is defined as the least value of non linearity of all nonzero linear combinations of x Boolean functions

fi : {0,1}→{0,1}, i= x-1,…,1,0.

To withstand linear cryptanalysis, an S-box must have strong nonlinearity.

E) Differential Uniformity

The S-box is more resistant to differential cryptanalysis the smaller the Differential Uniformity.

F) Linear Approximation

The S-box is more resistant to linear cryptanalysis the lower the Linear Approximation value.

G) Algebraic Complexity

To defend against interpolation assaults and other problematic algebraic attacks, algebraic complexity is crucial.

H) Fixed (Fp) and Opposite Fixed Points (OFp)

For the purpose of preventing leakage in any statistical cryptanalysis, the number of these Fp and OFp should be maintained as low as possible.

I) Bit independence criterion

Bit independence is a highly desirable characteristic since it makes the system's design harder to comprehend and predict as bit independence increases.

Rubik's Cube

Rubik's Cube (RC) was created by Ernő Rubik in a form of a puzzle game. It is 3D cubic object with six faces each one is having different colored stickers (red, orange, green, blue, yellow, and white). The inner design of the cube permits the different faces to turn, that gives the ability to these colors to be mingled. For the reason of solving the paradigm, each color must be in the exact face. A 3x3x3 RC has 43 quintillion combinations. In this modification, the RC is utilized to substitute AES S-box after being controlled by secret key [7].

The Proposed Modification

In the proposed modification, the 7x7x7 RC will be shuffled using the 21 most significant digits in the secret key to rotate the six faces. Each 7 decimal values are placed in the direction of the Cartesian coordinates as shown in figure 2. After shuffling RC by utilizing the secret key as mentioned, the RC will be expanded and re-ordered to represent 256-bit as explained in fig. 2.

1) Spatial Domain Technique

Spatial domain steganographic techniques sometimes referred to as replacement techniques are a collection of very straightforward methods that provide a hidden channel in the areas of the cover picture where changes are likely to be a little scarce in comparison to the Human Visual System (HVS). Among the methods for doing this is to conceal data in the Least Significant Bit (LSB) of the picture data [8-9].

2) Transform Domain Technique

Transform domain embedding is a class of embedding methods for which several algorithms have been proposed. This approach is more resistant to raid than others like compression and filtering since the secret data is added by modifying the transform coefficients of the picture. The alternative techniques included discrete wavelet transform (DWT) and discrete cosine transform (DCT) [10].

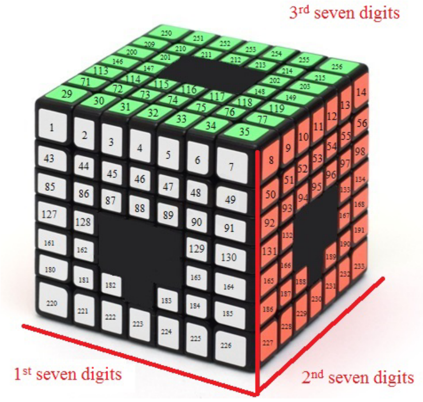

Fig.2. The RC key dependent.

In this modification the RC will be shuffled to produce the S-box used in AES algorithm. The proposed S-boxes produced from shuffling RC is shown in table 1. This modification will enhance the security of AES algorithm by generating a key dependent S-box [11] and this shown in fig. 3.

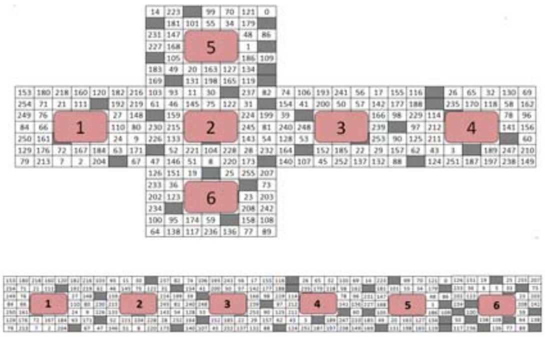

Fig.3. The block diagram of the proposed system.

Table. 1. The proposed S-BOX.

153	180	218	160	120	182	216	103	93	11	30	237	82	74	106	193
241	56	17	155	116	26	65	32	225	130	69	14	223	99	70	121
0	126	151	19	25	255	207	254	71	21	111	192	219	61	46	145
75	122	31	154	41	200	50	57	142	177	188	235	170	118	58	162
10	91	181	101	55	34	179	249	76	206	83	13	27	148	159	68
150	85	224	199	39	44	12	246	166	98	229	114	94	194	78	96
231	147	209	35	139	86	233	36	6	5	33	73	202	123	135	214
227	168	40	201	244	1	234	144	191	208	242	250	161	23	203	84
66	87	4	37	110	80	230	215	42	243	245	81	240	248	175	190
196	239	97	212	115	205	92	141	156	129	176	72	167	184	63	171
52	221	104	228	28	232	164	38	195	24	9	226	133	217	113	143
54	128	53	15	16	253	90	125	211	18	112	222	60	105	172	102
178	186	109	67	47	146	51	8	220	173	140	107	45	252	137	132
88	152	185	22	29	157	62	43	3	189	247	210	183	49	20	163
127	134	100	95	174	59	158	108	79	213	7	2	204	124	251	187
197	238	149	169	64	138	117	236	136	77	89	131	198	165	119	35

Security Analysis

In this section, we will deal with the performance evaluation and security strength analysis of the modified algorithm. For these tests, we will use a set of images (512 * 512) pixels in 256 gray scales. It is known that any cipher algorithm can be said to be secure if it passes these tests. Simulations have been carried out using Java and MATLAB R2021a [12].

A) Statistical Random Test

This trial is utilized for any series of data to see how random it is or not [13]. As the randomness of any series of data gives an indication of the strength of the algorithm, any sequence of data is perfect random if the value of P is 1 and it is non-random if this value is equal to zero, where P is called the tail probability. The 15 tests suggested by NIST are applied to the original and modified AES algorithm; the comparison between them is shown in table 2. A P-value ≥0.01 means that the encrypted data is random and P-value <0.01 means that the encrypted data considered being non-random.

Table 2. NIST random test values.

Test	P-values		Status	P-values		Status
	Baboon	Peppers		Engage	Lena	
(1)	0.0620	0.7273	Pass	0.7691	0.7544	Pass
(2)	0.8408	0.6339	Pass	0.4834	0.8679	Pass
(3)	0.2703	0.0250	Pass	0.1470	0.8740	Pass
(4)	0.6261	0.9604	Pass	0.7559	0.9028	Pass
(5)	0.2959	0.3375	Pass	0.3536	0.9836	Pass
(6)	0.3981	0.9717	Pass	0.1871	0.9617	Pass
(7)	1.0000	1.0000	Pass	1.0000	1.0000	Pass
(8)	0.3466	0.7755	Pass	0.2261	0.4966	Pass
(9)	0.9996	0.9996	Pass	0.9988	0.9986	Pass
(10)	0.7493	0.4708	Pass	0.9656	0.3698	Pass
(11)	0.6009	0.1428	Pass	0.1568	0.4857	Pass
(12)	0.6004	0.1425	Pass	0.2451	0.5881	Pass
(13)	0.0813	0.4720	Pass	0.4029	0.3073	Pass
(14)	0.1660	0.1608	Pass	0.0003	0.0376	Fail
(15)	0.0132	0.0155	Pass	0.0385	0.0127	Pass

B) Key Sensitivity Analysis

This analysis is used to establish how sensitive the cryptosystem is to the input secret key, and even if the decryption procedure is carried out using a key that is only slightly different from the secret key, no data can be recovered. The test image is encrypted with a random key (Key1) for the key sensitivity study, and then it is decrypted with five different decryption keys. The five decryption keys, in the worst scenario, differ from the original encryption key by one bit. Next, a correlation between the encrypted and unencrypted images is produced. The table displays the relationship between the two photos following the decryption procedure (3).And the correlation values less than that it's corresponding in the original AES. Note that the values will be multiplied by 10^{-4}. As shown in table 3, the modified AES hides all attributes of the original image and the decrypted image using slightly different keys are entirely different from the original one, meaning that a one-bit difference in the secret-key can produce encrypted image that is highly uncorrelated with it.

Tab. 3. Correlation among native and decrypted image.

Test image	Correlation (original)			Correlation (modified)		
	Key2	Key3	Key4	Key2	Key3	Key4
(a)Girl face	35	66	-3.4	-15	10	5
(b)Baboon	19	-43	24	18	-14	32
(c)Peppers	19	27	17	-1.8	20	1.9
(d)Engage	-34	12	3.2	-18	39	2.1
(e)Lena	34	7.2	-8.4	-28	3.3	4.4

Therefore, the modified AES is extremely sensitive to any small changes in the secret-key and it passes the key sensitivity analysis and shows less average correlation that the original AES. And fig. 4 presents the visual correlation.

A) Statistical Analysis

The following statistical tests are 1st seven digits executed to check the security of the modified AES:

1) Information Entropy

Information entropy measures the randomness in the encrypted image. The entropy value for a 256 gray levels image should be equal to 8. The calculated average entropy value for the original images is 7.14584 and the entropy value for the encrypted images using modified AES is 7.99932. While the entropy value of the original AES is 7.99743. It is quite clear that the entropy values are very close to the theoretical value. Therefore, the modified AES has a high entropy level.

2) Correlation of Adjacent Pixels

In any image, the pixels are connected to each other in all directions (horizontal, vertical and diagonal), but after encryption, the adjacent pixels should not be interconnected. The correlation occurring between the adjacent pixels can be visually represented by randomly selecting (P_0) pairs of contiguous pixels in all directions of the image. The value of P_0 is within 2000 and the distribution of the adjacent pixels is plotted using each pair as values for the XY coordinate. It is known that any cryptography system is considered effective in its ability to reduce the correlation between adjacent pixels to make statistical attacks ineffective in this system. It is essential for any cryptosystem that is used to encrypt images to pass that test.

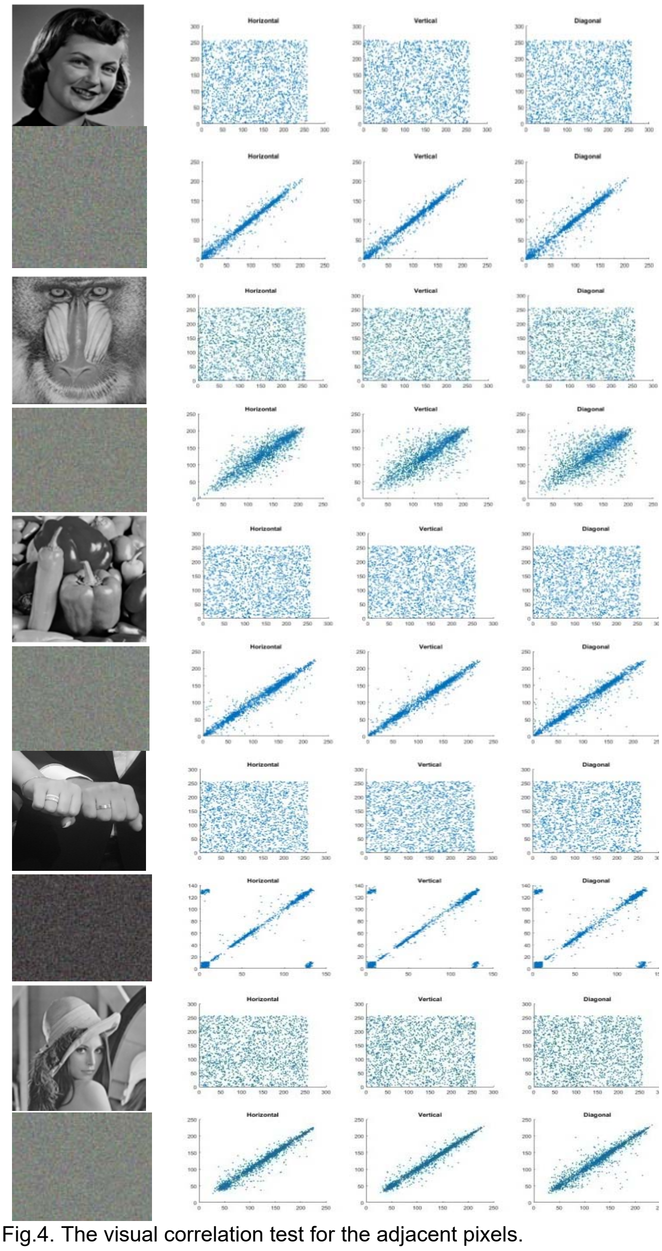

Fig.4. The visual correlation test for the adjacent pixels.

3) Histogram Analysis

The histogram the encrypted image should have a uniform distribution to prevent performing frequency analysis to recover any sensitive data. One of the indicators that the cryptography system secures is the distribution of pixels in the histogram analysis; this is evident in the fig. 5.

4) S-Box Strict Avalanche Criteria (SAC)

S-box is employed as a measure of diffusion when a single bit change in the input results in a large change in the output bits. So, Webster and Tavares created a method to determine whether the S-box meets the SAC. Finally, near to 2n-1=128 should be the SAC values and demonstrates in table 4.

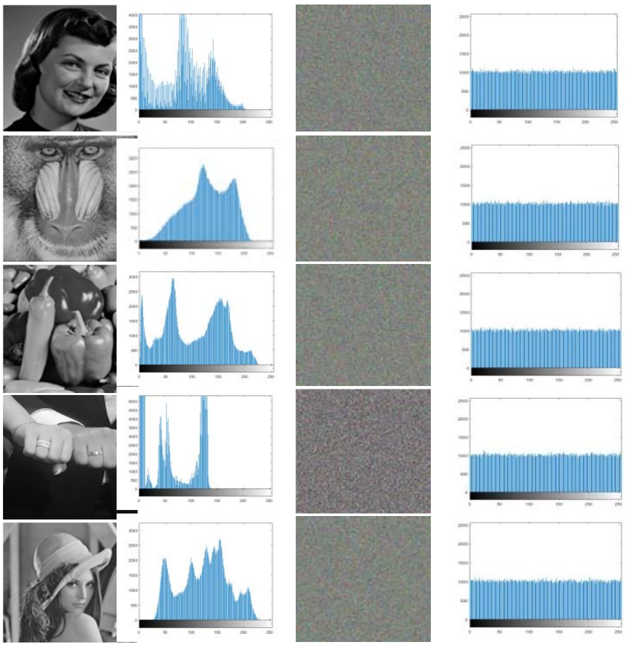

Fig.5. The original image and its histogram in column 1 and 2 and encrypted image and its histogram in column 3 and 4 respectively.

Table 4. SAC Values.

SAC	f1	f2	f3	f4	f5	f6	f7	f8
1	120	124	136	132	140	116	136	128
2	120	140	124	116	116	132	140	120
4	132	136	128	128	136	128	116	136
8	140	120	128	124	136	128	120	144
16	116	132	144	116	132	136	128	128
32	140	128	120	140	140	140	124	140
64	128	136	140	128	136	136	120	132
128	120	136	132	140	124	116	136	124

Table 5. NPCR and UACI test values

Test image	Original AES		Modified AES	
	NBCR(%)	UACI (%)	NBCR (%)	UACI (%)
(a) Girl face	99.4297	33.3173	99.4267	33.3641
(b) Baboon	99.4141	33.5276	99.4111	33.4656
(c) Peppers	99.4156	33.4427	99.4202	33.4187
(d) Engage	99.4328	33.4163	99.4198	33.3847
(f) Lena	99.4343	33.3679	99.4267	33.3641

5) Differential Analysis

The encrypted image resists the differential attack when it passes the NPCR and UACI through which it is possible to test the change of pixels and the number of average intensity variable among cipher text images, respectively. Although NPCR and UACI are easy to do, it is difficult for them to judge a good system. For example, the upper limit of NPCR is 100%, and therefore the more results are close to this value, we say that the encryption system is secure, but the extent of this proximity has not been determined, as is the case in UACI, it is required to be higher than 33%, as listed in table 5.

Conclusion

Data security is one of the most significant issues nowadays. The modified AES presented in this paper utilizes RC as a source to produce S-boxes. This amendment presents a key-dependent S-box for the purpose of enhancing AES safety and security. Security analysis refers that the modified AES can stop most common hostilities, statistical and differential. The modified AES passed the key sensitivity analysis and the entropy analysis. Histogram analysis displays a uniform distribution of pixel intensities as well; there is no correlation between adjacent pixels. NPCR and UACI exceeds the expected values so, even a slight change in original image results in an important alteration in encrypted image. The modified AES shows good results in key sensitivity, Entropy passed most of the NIST Tests and boosts the non-linearity of the original S-box but it shows a less value in the NPCR and UACI analysis with the comparison to the original AES. As a result, the modified AES shows excellent potential for practical encryption application.

Authors:
Dr. Hamed SHAWKY ZIED and Dr. Ahmed GAMAL ABDEL LATIF, are academic staff Lecturers in the Department of Communications and Electronics, Air Defense College, Egypt.
Email:Dr.Hamedzied@gmail.com,ag.abdellatef@zu.edu.eg.
Dr. Ahmed IBRAHIM SALEM is an academic staff Lecturer in the Department of Electrical Engineering, Faculty of Engineering, Damanhur University, Egypt.
Email: Ahmed.Salem@dmu.edu.eg.

REFERENCES

1 A. Gamal, M. Saleh, and A. Elmahallawy, "De-Noising of Secured Stego-Images using AES for Various Noise Types," Przeglad Electrotechniczny, vol. 2, no.2 pp. 21–26, 2023.
2 M. Tayel, G. Dawood, and H. Shawky, "Serpent S-box Modification using Rubik Cube," International Journal of Industrial Electronics and Electrical Engineering, ISSN (p): 2347-6982, ISSN (e): 2349-204X Volume-6, Issue-9, 2018.
3 A. Gamal M. Tayel, and H. Shawky "De-Noising of Stego-Images for different noise models," 17th IEEE International Conference on Advanced Communication Technology (ICACT), July 1-3, 2015, Korea.
4 A. Gamal M. Tayel, and H. Shawky "A Proposed Implementation Method of an Audio Steganography Technique," 18th IEEE International Conference on Advanced Communication Technology (ICACT), 2015.
5 Manjula .G, Mohan HS"A Secure Framework for Medical Image Encryption Using Enhanced AES Algorithm" International Journal of Scientific & Technology Research vol 9, issue 02 Feb. 2020.
6 M. Tayel, G. Dawood, and H. Shawky, "Block Cipher S-box Modification Based on Fisher-Yates Shuffle and Ikeda Map," 7th International Conference on Advances in Computing, Communicationsand Informatics (ICACCI), 2018.
7 Nur Rachmat1, Samsuryadi, "Performance Analysis of 256-bit AES Encryption Algorithm on Android Smartphone" IOP Conf. Series: Journal of Physics: Conf. Series1196, 2019.
8 A. Gamal, M. Mostafa, A. Masiero, A. Zaghloul ,M. Naser et al.,"Indoor positioning system based on magnetic fingerprinting image," Bulletin of Electrical Engineering and Informatics, vol. 10,no.3 pp. 1325–1336, 2021.
9 H.Fiyad ,A. Gamal, M. Mostafa,A. Zaghloul ,M. Naser et al.," An improved real visual tracking system using particle filter," Przeglad Electrotechniczny, vol. 11,no.1 pp. 164–169, 2021.
10 M. M. Abu-Faraj and Z.Alqadi, "Using Highly Secure Data Encryption Method for Text File Cryptography", International Journal of Computer Science and Network Security, vol. 20, issue 11, pp.53-60, 2021.
11 Zi. A. Alqadi and M. Abu -Faraj, "Improving the Efficiency and Scalability of Standard Methods for Data Cryptography" International Journal of Computer Science and Network Security, vol. 21, pp.451-458, 2021.
12 K. Ali, A. N. Quershi, A. Alauddin, M. S. Bhatti, A. Sohail et al., "Deep image restoration model: A defense method against adversarial attacks," Computers, Materials & Continua, vol. 71, no. 2, pp. 2209–2224, 2022.
13 A. Khompysh, N. Kapalova, K. Algazy, D. Dyusenbayev & K. Sakan "Design of substitution nodes (S-Boxes) of a block cipher intended for preliminary encryption of confidential information", Cogent Engineering, 2022.