AIMS Mathematics, 9(3): 6207–6237.
DOI: 10.3934/math.2024303
Received: 21 October 2023
Revised: 21 December 2023
Accepted: 02 January 2024
Published: 02 February 2024

http://www.aimspress.com/journal/Math

Research article

Novel substitution-box generation using group theory for secure medical image encryption in E-healthcare

Abdul Razaq[1,*], Louai A. Maghrabi[2], Musheer Ahmad[3] and Qamar H. Naith[4]

[1] Department of Mathematics, Division of Science and Technology, University of Education Lahore, Pakistan
[2] Department of Software Engineering, College of Engineering, University of Business and Technology, Jeddah, Saudi Arabia
[3] Department of Computer Engineering, Jamia Millia Islamia, New Delhi 110025, India
[4] Department of Software Engineering, College of Computer Science and Engineering, University of Jeddah, Jeddah 21959, Saudi Arabia

* **Correspondence:** Email: abdul.razaq@ue.edu.pk; Tel: +92-317-588-0894.

Abstract: With the increasing need for secure transmission and storage of medical images, the development of robust encryption algorithms is of paramount importance. Securing sensitive digital medical imagery information during transmission has emerged as a critical priority in the e-Healthcare systems. Recent research has highlighted the significance of developing advanced medical image encryption algorithms to ensure secure transmission during telediagnosis and teleconsultations. In this study, we propose a novel medical image encryption algorithm which is based on a novel substitution-box generation algebraic method using a combination of a multiplicative cyclic group with an order of 256 and a permutation group with a large order. To evaluate the security performance of the proposed generated S-box, various standard security indicators are assessed and analyzed. The newly proposed medical image encryption algorithm utilizes the generated S-box, along with bit-plane slicing, circular shifting, and XOR operations, to achieve enhanced security and robustness for encrypting sensitive imagery data. In order to assess the effectiveness of the proposed encryption algorithm, a comprehensive benchmarking analyses, specifically designed for evaluating image encryption schemes, have been conducted. The results obtained from the comparison and other analyses serve to validate the optimal features and high cryptographic strength exhibited by the proposed method. Hence, the proposed algorithm demonstrates significant effectiveness and holds considerable promise in the realm of medical image encryption for secure e-Healthcare systems.

Keywords: cyclic group; substitution-box; image encryption; e-healthcare systems
Mathematics Subject Classification: 20D35, 94A60, 68U10

1. Introduction

Telemedicine is a rapidly expanding discipline that provides health services remotely, wherein the patient and the physician do not live in the same geographical region. The patient's personal data, especially medical images, is communicated via online or cellphone-networked routes. This contemporary healthcare system requires an infrastructure that has the ability to preserve medical images in such a manner that they are visible only to permitted users, regardless of their geographic location. This infrastructure could be provided through cloud storage networks. However, such systems are susceptible to cyber-attacks if they are not built according to proper safety standards. The primary focus of many researchers in the information security field has been the development of computing-based tactics aimed at enhancing patient care. However, there is a notable gap in the methodologies employed to achieve the desired level of privacy for sensitive data within communication channels and storage systems. In these circumstances, one option for safeguarding medical images is to utilize encryption algorithms. These algorithms encrypt the images in a manner that renders them indecipherable to users who do not possess the encryption key. References [1–7] highlight several security measures for telemedicine applications.

The substitution-box (S-Box) is a crucial part of the encryption process and one of the most significant components in cryptography [8]. An s×s S-box is a special kind of Boolean function that can be defined as;

$$\psi(u): \big(h_1(u), h_2(u), h_3(u), \dots, h_s(u)\big): Z_2^s \longrightarrow Z_2^s,$$

where Z_2 *is* a finite field of order 2. The substitution-box is used to create perplexity and uncertainty in actual data, and the robustness of the cryptosystem depends upon the ability of the S-box to scramble the information into an unreadable format. The use of the S-box aids in achieving Shannon's confusion characteristics. These characteristics strengthen block ciphers against differential and linear attacks [9,10]. After the successful implementation of AES, which uses 8×8 S-boxes, experts in this field have been interested in the construction of cryptographically robust 8×8 S-boxes [11–18].

In recent years, there have been numerous advancements in the field of image encryption systems, resulting in the emergence of various schemes that can be categorized based on their underlying encryption methods. These methods include DNA encryption, chaotic system approach, wavelet transform encryption, compressive sensing encryption, and the S-box approach. Ibrahim et al. [19] employed dynamic S-boxes and chaotic maps in their study to effectively encrypt medical images. The proposed system was designed to offer protection against reset attacks, as well as selected plaintext and ciphertext attacks. A comprehensive analysis of multiple image encryption schemes incorporating DNA coding and nonlinear dynamics was presented in [20], uncovering inherent vulnerabilities within these schemes. The authors demonstrated the application of S-boxes in executing chosen-plaintext attacks against the aforementioned schemes. In [21], a novel n-dimensional conservative chaos is generated for the purpose of image encryption utilizing the Generalized Hamiltonian System. Nematzadeh et al. [22] presented a hybrid model that combines an updated genetic scheme and coupled map lattices (CMLs) to enhance the encryption security and

computational efficiency of medical images. Reference [23] elucidated the development of high-speed and low-area architectures specifically designed to accommodate the secure IoT encryption algorithm within resource-constrained IoT environments. The paper also introduced a dynamic block selection technique aimed at enhancing the efficiency of image encryption. Liu et al. proposed image encryption for color images in [24] by utilizing self-adapting permutation and DNA dynamic encoding. Hashim et al. [25] proposed a hybrid encryption technique that combines a quadratic map preprocessing step with AES for secure medical image transmission, thereby addressing the challenge of protecting patient privacy and data confidentiality. Based on the DNA-chaos cryptosystem, [26] revealed an innovative approach to encrypt medical images aimed at keeping telemedicine and other medical applications protected. Experimental results indicated the effectiveness of the proposed approach, which demonstrated its efficient processing time and robust encryption capabilities. Khan et al. [27] designed S-boxes with good cryptographic strength by utilizing true random values derived from medical imaging noise. In [28], a novel hybrid encryption technique based on S-box and Henon mappings for enhancing the security of multidimensional 3D medical images was presented. Hayat et al. [29] introduced an innovative approach to construct S-boxes by leveraging elliptic curves within finite order rings. Upon comparative assessment with contemporary methodologies, it becomes apparent that their proposed technique is better tailored for cryptographic applications. Notably, a resilient S-box exhibiting a substantial non-linearity of 109.75 is delineated in [30], employing the Q-learning naked mole rat method. Furthermore, the authors adeptly applied the suggested S-box for image encryption. In [31], the sine-cosine optimization procedure is employed to generate a bijective S-box, with the authors conducting rigorous testing against other S-boxes to establish its efficacy. Razaq et al. [32] introduced a novel approach that utilized group theory to generate an extensive number of S-boxes possessing algebraic properties similar to those of AES. S-boxes constructed by Ibrahim et al. [33] utilize permutated elliptic curves, exhibiting experimental efficiency an order of magnitude higher than comparable methods. Reference [34] introduces an efficient chaotic S-box, employed in the design of a streamlined cryptosystem demonstrating favorable encryption outcomes and security robustness. Alhadawi et al. [35] incorporated discrete chaotic maps and the cuckoo search algorithm in their S-box generation method, concluding that the resultant S-boxes exhibit robust cryptographic properties resistant to cryptanalysis. In [36], Khan et al. utilized a chaotic partial differential equation to design an S-box, implementing it to construct a secure communication-oriented cryptosystem. Khan et al. [37] proposed a novel S-box construction through the application of a fractional Rossler chaotic model, substantiating its efficacy in ensuring secure communication. Reference [38] introduces an effective S-box generated through the artificial bee colony method and discrete chaotic map. By employing a range of benchmark standard analyses, the authors validate the robustness of the S-box. Soto et al. [39] suggested a novel S-box generation method using a human behavior-based optimization system. Several investigations show that the offered method may efficiently create resilient S-boxes for encryption systems. In [40], Yan et al. employed a Nonlinear-Transform of 1D Chaotic Maps to create the S-box. The authors perform many security evaluations to show the resilience of the constructed S-box. Zhou et al. [41] proposed a chaos-based random S-box design algorithm that generated a large number of S-boxes by utilizing the spatial chaotic nature of spatiotemporal chaos. An innovative algorithm for generating S-boxes based on hyperchaotic systems is presented in reference [42]. The generated S-box is also incorporated into the design of an image encryption algorithm. In [43], a novel technique for deriving random bijective S-boxes using discrete chaotic maps is introduced. The performance test shows that the S-box has good cryptographic characteristics. In [44], a methodology is suggested to generate S-boxes using an efficient method

based on the 3-D four-wing autonomous chaotic system. Comparing the proposed S-box to current ones demonstrates higher cryptographical performance. Furthermore, recent advancements in image encryption methods can be found in references [45–50].

The present study contributes significantly in the following ways:

i. A novel approach is formulated for the generation of substitution-boxes by combining a permutation group and a multiplicative cyclic group of order 256.
ii. To assess the performance of the suggested S-box, many standard algebraic parameters are applied. The findings obtained from various assessment methods confirm the reliability of the proposed S-box in preventing numerous assaults.
iii. A robust image encryption algorithm that integrates the generated substitution-box with bit-plane slicing, circular shifting, and XOR operations is developed.
iv. The security of the encryption algorithm is assessed using benchmark evaluations designed for image encryption techniques. The outcomes show that the proposed encryption approach can encrypt medical images effectively.

2. Mathematical concepts

In this section, we discuss some mathematical concepts utilized to our S-box design scheme.

2.1. Group

A set Ψ is said to constitute a group under the binary operation "*" if the following conditions hold.

i. Closure Law
For all $\mu, \nu \in \Psi$, we have $\mu * \nu \in \Psi$.

ii. Associative Law
For all $\mu, \nu, \sigma \in \Psi$, we have $\mu * (\nu * \sigma) = (, \mu * \nu) * \sigma$

iii. Existence of Identity
For each $\mu \in \Psi$, there is an element $e \in \Psi$ such that $e * \mu = \mu * e = \mu$.
e is called the identity element in Ψ, it has no effect on each element of Ψ under "*".

iv. Existence of Inverse
For each $\mu \in \Psi$, there is an element $\mu^{-1} \in \Psi$ such that $\mu^{-1} * \mu = \mu * \mu^{-1} = e$.
μ and μ^{-1} are called inverses of each other.

2.2. Cyclic group

Let Ψ be a group under some binary operation "*". Then, Ψ is called a cyclic group if it has at least one element a that can generate the entire group Ψ. In other words, for all $b \in \Psi$, there exists at least one element a in Ψ such that $b = \begin{cases} na : n \in \mathbb{Z}, & \text{if } \Psi \text{ is group under addition} \\ a^n : \in \mathbb{Z}, & \text{if } \Psi \text{ is group under multiplication} \end{cases}$.

If such is the case, we say that a is the generator of the cyclic group Ψ. It is important to note that, in a cyclic group Ψ, a is not a unique element that generates Ψ rather Ψ has many elements other than a, acting as generator of Ψ.

The following theorem enables us to identify all generators of any finite cyclic group Ψ.

Theorem 1. Let Ψ be a cyclic group with n elements and a be its one of the generators. Then a^m also generates Ψ if and only if m and n are relatively prime.

Thus, to find all generators of Ψ, we must first manually compute its one generator, say a. Next, we find all the positive integers that are relatively prime to n. Finally, we get the set $\{a^m: (m, n) = 1\}$ of all generators of Ψ.

2.3. The cyclic pattern of the cyclic group and S-box

Let Ψ be a cyclic group with n elements and a be one of the generators. Then, a generates all the elements of Ψ randomly in the following way;

$$a, a^2, a^3, \dots, a^n = 1.$$

We call $a, a^2, a^3, \dots, a^n = 1$, a cycle of Ψ obtained by a. Such cyclic patterns create randomness in the elements of Ψ. For example, the cyclic patterns of $(\mathbb{Z}_{11} - \{0\}, .)$ designed by its all four generators 2,8,7, and 6 are

$$2,4,8,5,10,9,7,3,6,1$$
$$8,9,6,4,10,3,2,5,7,1$$
$$7,5,2,3,10,4,6,9,8,1$$

and

$$6,3,7,9,10,5,8,4,2,1$$

respectively.

An 8-bit S-box has 256 number of distinct elements presented randomly in a square matrix of order 16. In this work, we have used the cycle of multiplicative cyclic group $(\mathbb{Z}_{257} - \{0\}, .)$ of order 256 to design our S-box. It is easy to verify that $(\mathbb{Z}_{257} - \{0\}, .)$ is generated by 2. Also, the positive integers that are relatively prime to 256 are all odd positive integers. Thus,

$$\{2^m \ (mod\ 257): m \text{ is odd}\} =$$

$$\left\{ \begin{array}{c} 3, 27, 243, 131, 151, 74, 152, 83, 233, 41, 112, 237, 77, 179, 69, 107, 192, 186, 132, 160, 155, 110, \\ 219, 172, 6, 54, 229, 5, 45, 148, 47, 166, 209,82, 224, 217, 154, 101, 138, 214, 127, 115, 7, 63, 53, \\ 220,181, 87, 12, 108, 201, 10, 90, 39, 94, 75, 161, 164, 191, 177, 51, 202, 19, 171,254, 230, 14,126, \\ 106,183, 105, 174, 24, 216,145, 20, 180, 78, 188, 150, 65, 71, 125, 97, 102, 147, 38, 85, 251, 203, 28, \\ 252,212, 109, 210, 91, 48, 175, 33, 40, 103, 156, 119, 43, 130, 142,250, 194, 204, 37, 76, 170, 245, \\ 149, 56, 247, 167, 218, 163, 182, 96, 93, 66, 80, 206, 55, 238, 86 \end{array} \right\}$$

is the set of all generators of $(\mathbb{Z}_{257} - \{0\}, .)$. Each of these *128* generators produce randomness in $(\mathbb{Z}_{257} - \{0\}, .)$, which further evolves an S-box.

3. The proposed scheme of S-box generation

The proposed technique for the generation of S-boxes considers the ideas of cyclic and permutation groups. Here, we detail the steps required to use them effectively and complete the task.

Step 1.

In this step, the trivial sequence $0,1,2,\dots,255$ is randomised to generate the initial S-box. It is achieved using a cyclic pattern of $(\mathbb{Z}_{257} - \{0\}, .)$ designed by one of its generators in association with the translation and mod (256) operation.

Step 1.1.

Generate $(\mathbb{Z}_{257} - \{0\}, .)$ with the help of one of the generators 74. Consequently, a cycle shown in Figure 1 is formed.

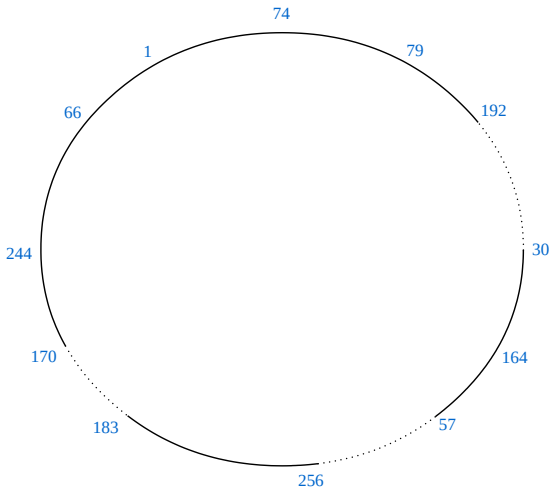


Figure 1. Cyclic form of $\mathbb{Z}_{257} - \{0\}$ generated by 74.

Step 1.2.

In Step *1.1*, we acquire *256* random data points ranging from *1* to *256*. The initial S-box (see Table 1) is formed by adding *84* to each data input and then applying mod-256. That is, for each data input n, the corresponding entry of the S-box is $n + 84 \bmod (256)$. The non-linearity of our initial S-box is 106.25, which demonstrates the effectiveness of using cyclic groups in the S-box construction.

Table 1. Initial S-box.

158	*163*	*20*	*157*	*89*	*197*	*222*	*17*	*192*	*109*	*135*	*4*	*2*	*110*	*209*	*83*
193	*183*	*214*	*195*	*75*	*115*	*66*	*220*	*125*	*35*	*239*	*246*	*250*	*33*	*91*	*88*
123	*143*	*82*	*119*	*104*	*23*	*122*	*70*	*3*	*184*	*32*	*18*	*10*	*188*	*71*	*77*
7	*223*	*90*	*15*	*45*	*208*	*9*	*114*	*248*	*141*	*190*	*218*	*234*	*133*	*112*	*100*
240	*64*	*73*	*224*	*164*	*93*	*236*	*25*	*14*	*227*	*129*	*74*	*42*	*243*	*29*	*53*
30	*126*	*108*	*62*	*181*	*67*	*38*	*204*	*226*	*56*	*251*	*106*	*170*	*24*	*196*	*148*
194	*1*	*37*	*130*	*147*	*120*	*178*	*101*	*58*	*142*	*8*	*41*	*169*	*206*	*117*	*213*
121	*252*	*180*	*249*	*215*	*13*	*153*	*51*	*138*	*225*	*238*	*172*	*171*	*97*	*19*	*84*
11	*6*	*149*	*12*	*80*	*228*	*203*	*152*	*233*	*60*	*34*	*165*	*167*	*59*	*216*	*86*
232	*242*	*211*	*230*	*94*	*54*	*103*	*205*	*44*	*134*	*186*	*179*	*175*	*136*	*78*	*81*
46	*26*	*87*	*50*	*65*	*146*	*47*	*99*	*166*	*241*	*137*	*151*	*159*	*237*	*98*	*92*
162	*202*	*79*	*154*	*124*	*217*	*160*	*55*	*177*	*28*	*235*	*207*	*191*	*36*	*57*	*69*
185	*105*	*96*	*201*	*5*	*76*	*189*	*144*	*155*	*198*	*40*	*95*	*127*	*182*	*140*	*116*
139	*43*	*61*	*107*	*244*	*102*	*131*	*221*	*199*	*113*	*174*	*63*	*255*	*145*	*229*	*21*
231	*168*	*132*	*39*	*22*	*49*	*247*	*68*	*111*	*27*	*161*	*128*	*0*	*219*	*52*	*212*
48	*173*	*245*	*176*	*210*	*156*	*16*	*118*	*31*	*200*	*187*	*253*	*254*	*72*	*150*	*85*

Step 2.

The Step *2* of the proposed S-box generation method is based on a permutation group G generated by three elements a, b and c, where

a=(1,111,86,50,227,104,210,144,172,255,68,200,91,157,88,24,216,72,115,247,112,188,39,41,184,51,177,170,7,147,54,254,162,196,94,128,201,213,214,99,175,166,224,65,130,117,181,161,15,212,141,233,22,129,61,113,118,136,252,28,235,89,44,204,37,223,14,30,164,131,85,35,21,241,82,234,122,108,193,9,90,217,67,109,195,62,146,63,137,92,42,101,150,189,93,5,47,246,107,10,244,34,98,148,145,218,56,76,182,190,43,53,73,38,48,18)

b=(2,29,225,125,71,106,156,52,124,202,165,46,251,33,12,3,81,197,250,126,11,138,160,120,199,143,4,215,194,13,57,248,96,176,154,230,69,23,26,103,31,198,45,8,49,142,97,209,158,20,192,231,66,116,169,127,149,75,84,114,207,239,16,55,132,155,58,153,206,232,32,237,87,139,178,102,105,121,140,134,40,59,25,123,220,159,219,203,245,80,226,173,249,70,236,79,78,151,163,191,6,208,185,187,242,100,222,95,228,186,168,211,221,60,135,27,77,171,19)

*c=(*17,167,183,110,83,205,243,229,253,256,180,133,240,119,174,74,238,152,179*).*

Using GAP, we note that the finite presentation of G is

$$\langle a, b, c : a^{116} = b^{119} = c^{19} = aba^{-1}b^{-1} = aba^{-1}c^{-1} = bcb^{-1}c^{-1} = 1 \rangle.$$

Furthermore, the order of G is 262276. Each element of G acting on the original S-box generates a new S-box. We apply all elements of G and determine that $a^{15}b^{76}c^{7}$ is the most effective element in G as it converts the initial S-box into the most resilient S-box in terms of non-linearity score. This S-box is referred to as our generated S-box (see Table 2).

Table 2. Final S-box.

143	17	62	68	56	189	175	174	104	96	9	129	38	111	201	130
79	176	10	31	152	244	70	158	179	190	178	6	7	115	238	218
94	242	13	119	107	8	86	236	151	27	89	46	78	166	199	109
40	232	224	69	71	220	145	147	34	28	142	66	37	181	75	100
222	29	33	45	228	5	139	67	156	237	197	54	91	135	97	123
252	246	206	116	121	230	239	183	124	229	23	126	192	16	118	120
53	112	55	2	225	214	125	114	163	136	169	18	50	160	1	101
98	177	223	243	208	146	212	141	250	226	15	247	194	83	87	213
102	211	234	196	154	171	35	21	48	12	42	231	84	210	182	217
106	82	204	233	57	41	60	219	99	138	39	195	77	159	198	186
26	25	81	11	249	162	193	134	103	251	76	36	20	153	90	58
144	137	205	85	72	191	47	150	157	92	131	43	185	170	51	93
95	0	149	180	140	63	44	14	207	64	188	209	108	61	235	216
168	74	49	24	122	3	88	117	110	184	65	172	164	248	167	241
59	4	113	148	245	165	128	255	155	161	215	200	203	227	173	80
253	105	127	133	187	73	132	202	30	52	19	240	22	221	32	254

4. Algebraic performance of the generated S-box

The generated S-box has been evaluated using certain well-known performance metrics. These include non-linearity, differential and linear approximation probabilities, bit independence criterion, and strict avalanche criterion. The findings of these security analyses in relation to the suggested S-box are briefly summarized in this subsection.

An S-Box is needed to create a particular level of disorder in the data to secure it from different security assaults by unauthorized individuals. The capacity of an S-Box to cause confusion is tested using the non-linearity analysis [51]. In general, the greater the nonlinearity score of an S-box, the more reliable it is. The average non-linearity of the suggested S-box is 111, which is sufficient to assert that the created S-box can protect the transmitted data against linear assaults.

Biham and Shamir [52] proposed differential uniformity (DU) as an essential criterion for S-box assessment. To compute the DU score, the mapping between input and output bits is analyzed. This analysis is designed to ensure differential homogeneity. The differential δh at the input must be uniquely connected to differential δk at the output. The newly constructed S-box has a DU score of 6, confirming its immense resistance to differential attacks.

Linear approximation probability (LP) is an analysis for determining the efficiency of an S-box against linear cryptanalysis [53]. This test examines an event's imbalance and calculates its maximum score. The maximum LP score of the constructed S-box is 0.078, reflecting its resistance to various linear assaults.

Large avalanche effects are required to construct a robust cryptographic system. Strict avalanche criteria (SAC) were first proposed by Websters and Tavares [54]. According to this criterion, if a single binary bit in the input is reversed, the output will also have a 50% chance of bit reversal. The optimal SAC value is 0.5. The mean SAC score of our S-box is 0.5017 indicating that the designed S-box fulfils the SAC standards.

The bit independence criterion (BIC), developed in [54], is another significant criterion for determining the quality of S-boxes. BIC requires that the Boolean mappings of the two output bits satisfy the NL and SAC requirements. The Boolean mapping of the two output bits in the proposed S-box satisfies the condition of nonlinearity, with an average BIC-NL value of 111.43. The average BIC-SAC score of our S-box is 0.5018, which indicates that the constructed S-box satisfies the SAC criteria.

Table 3 provides a comprehensive comparison of the outcomes of the aforementioned analyses obtained from the proposed S-box with those obtained from recently constructed S-boxes.

Table 3. Comparison of the various analyses between different S-boxes.

S-box	Nonlinearity			SAC	BIC-SAC	BIC-NL	DU	LP
	min	max	Avg					
Suggested S-box	110	112	111	0.5017	0.5018	111.43	6	0.0703
Ref [29]	106	108	106.25	0.5112	0.4975	103.93	12	0.1484
Ref [30]	108	110	109.75	0.4998	0.5041	104.14	10	0.1171
Ref [31]	108	110	109.50	0.4985	0.5012	104.07	10	0.1328
Ref [32]	108	112	110	0.5010	0.5007	104	10	0.1250
Ref [33]	106	110	106.5	0.5010	0.4987	103.93	10	0.1250
Ref [34]	106	108	107	0.4949	0.5019	102.29	12	0.1410
Ref [35]	106	110	108.5	0.4995	0.5011	103.85	10	0.1090
Ref [36]	98	108	104.25	0.4946	0.5036	102.85	16	0.1406
Ref [37]	100	108	104.50	0.4978	0.4974	103.64	12	0.1328

Continued on next page

S-box	Nonlinearity			SAC	BIC-SAC	BIC-NL	DU	LP
	min	max	Avg					
Ref [38]	108	110	109.75	0.5042	0.4987	110.6	6	0.0859
Ref [39]	102	110	106.5	0.4943	0.5019	103.35	12	0.1468
Ref [40]	104	108	105.5	0.5065	0.5031	103.57	10	0.1328
Ref [41]	104	110	107	0.4993	0,5050	103.29	10	0.1328
Ref [42]	104	110	107	0.5007	0.5039	104.50	10	0.1250
Ref [43]	106	108	106.75	0.5034	0.5016	103.79	10	0.1250
Ref [44]	104	108	105.75	0.4976	0.5002	104.50	10	0.1250
Ref [45]	102	108	104.50	0.4980	0.4995	104.64	12	0.1172
Ref [46]	100	106	104.00	0.5027	0.4947	103.21	12	0.1250
Ref [47]	106	110	108.25	04985	0.5011	103	10	0.1250
Ref [48]	106	108	106.25	0.5010	0.5001	103.14	12	0.132
Ref [49]	108	112	110	0.5034	0.4995	103.50	10	0.132
Ref [50]	98	106	102.75	0.4978	0.5020	103.36	12	0.1328

5. Development of image encryption algorithm using proposed S-box

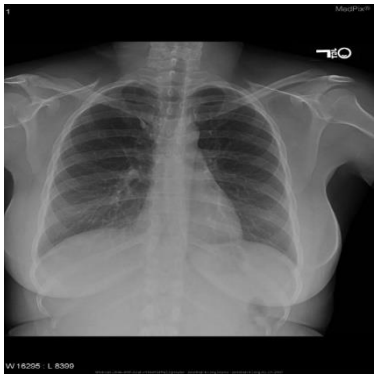
Medical imaging plays a crucial role in diagnosing and treating various medical conditions. However, the sensitive nature of medical images necessitates their protection against unauthorized access and tampering during transmission and storage. Encryption is a fundamental technique used to secure such images. This section introduces a new encryption scheme for medical images that addresses their exclusive security needs.

An image P is turned into a one-dimensional series and then into hexadecimal form. The SHA-512 method generates a 512-bit hash, which is then split into two components and placed back together in a 16×16 matrix. Further modification requires dividing the hash into 64 8-bit pieces. New S-boxes and images undergo bit-plane slicing. The hash components and S-box planes are combined via bitwise XOR. Modulus operations with pre-set values $p1$ to $p6$ choose bitplanes for circular shifting. Block-wise exclusive OR operations occur between image bitplanes and the modified S-box. Integrating the processed bitplanes creates an 8-bit encoded image, C, with planes rearranged. C undergoes substitution procedures based on T values and S-box elements. Finally, the encrypted image E is reshaped into a $2D$ matrix. The simulation settings include predefined values for $p1$ to $p6$ and an initial value $C0$ within the range $[0,255]$. The encryption procedure aims to enhance the security of the image data through a combination of hash functions, bit-plane manipulations, and substitution operations.

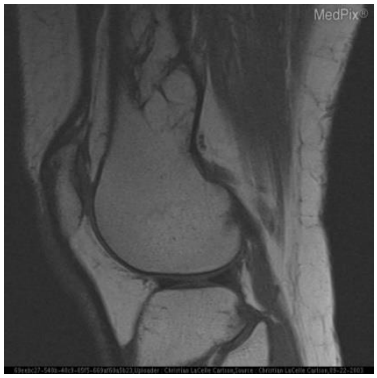
In this study, a set of six grayscale medical images, along with three additional grayscale images (Lena, Barabara, and Tree), all with dimensions of 256×256, were subjected to encryption. The purpose was to determine whether significant statistical differences exist between the encrypted images and their corresponding original versions. The experimental findings presented in this paper substantiate the robustness and high level of security exhibited by the proposed algorithm. All experimental simulations were carried out using the MATLAB software. The collection of nine

plaintext images utilized in this research was obtained from reputable sources such as (https://medpix.nlm.nih.gov/home) and (https://sipi.usc.edu/database/). Figure 2 displays both the original and encrypted images, illustrating their distinctiveness and indicating the efficacy of the encryption algorithm in successfully encrypting the tested images.

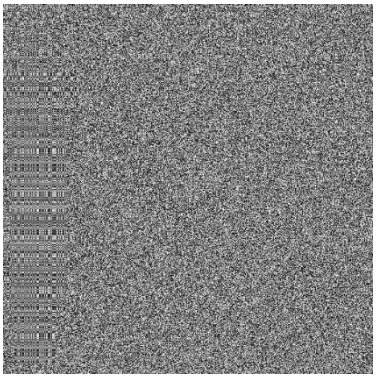
Med-Image 1-Org



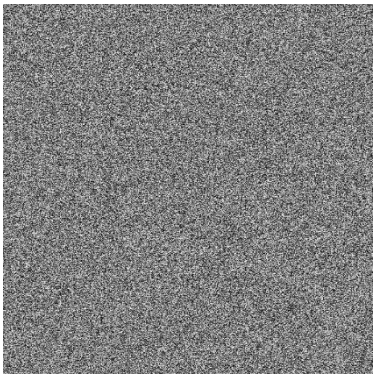
Med-Image 2-Org



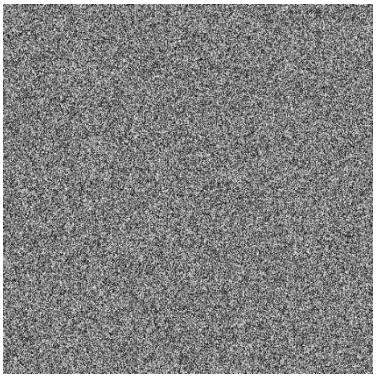
Med-Image 3-Org



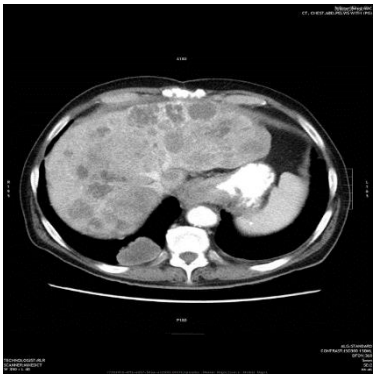
Med-Image 1-Enc



Med-Image 2-Enc



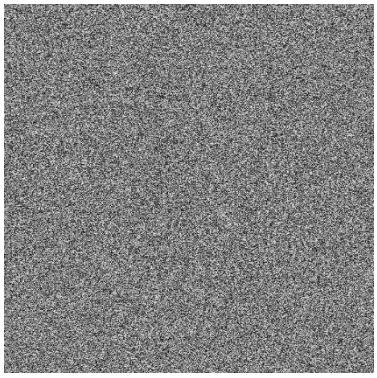
Med-Image 3-Enc



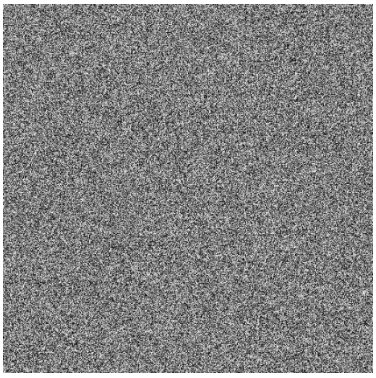
Med-Image 4-Org

Med-Image 5-Org

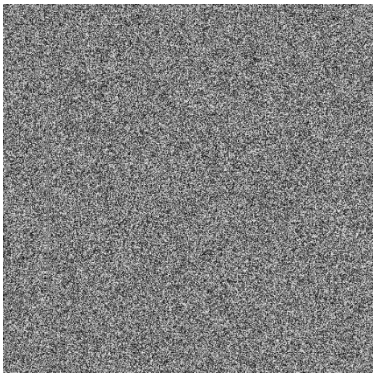
Med-Image 6-Org



Med-Image 4-Enc



Med-Image 5-Enc



Med-Image 6-Enc

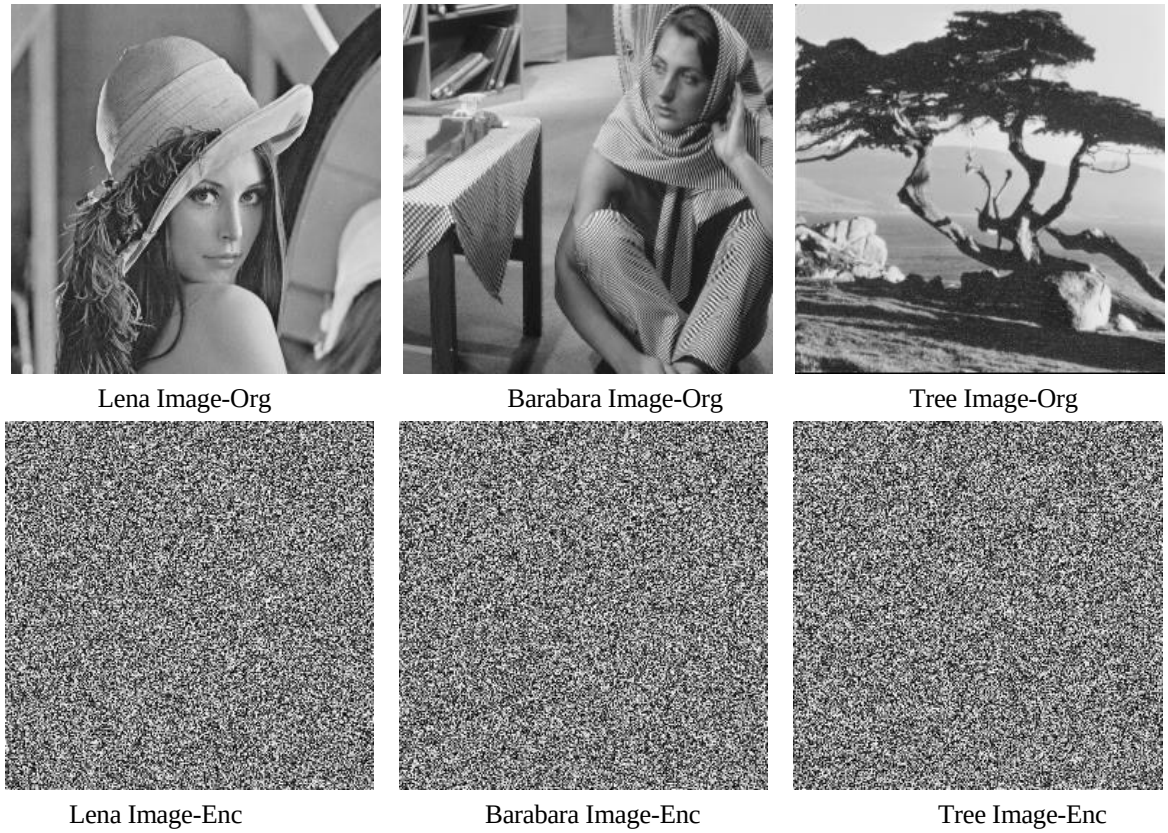


Figure 2. Initial and distorted versions of images selected for Image encryption.

5.1. Decryption process

A series of operations and functions are utilized during the decryption procedure in order to restore the encrypted image E to its original state P. To commence the decryption process, the 2D encrypted Image 1s converted into a 1D array denoted as C. Subsequently, a series of substitution operations are performed, which consist of bitwise XOR operations employing a pre-established substitution box (S), bitwise calculations, and intricate bit-level manipulations. The encrypted Image 1s then reshaped back into its original 2D matrix form. Reverse circular shifting operations are performed on the bitplanes of the image, driven by modular calculations derived from predetermined values. The original bitplanes are reconstructed through a reverse block-wise XOR operation that utilizes specific bitplanes and their relevant elements from the encryption hash (H). Decrypted Image variable P is ultimately produced by combining the reconstructed bitplanes. The intricate decryption process highlights the complexity and resilience of the proposed encryption scheme.

6. Experimental analyses

In this section, we have conducted many standard analyses to evaluate the reliability of the suggested encryption technique.

6.1. Majority logic criterion

The Majority Logic Criterion (MLC) [55] is a comprehensive framework consisting of contrast, energy, correlation, and homogeneity analyses. Its primary objective is the meticulous examination of the statistical properties inherent in image encryption algorithms.

6.1.1. Contrast

The degree of contrast within an image plays a crucial role During the image processing procedure, alterations are made to ensure optimum contrast and luminance viewing conditions. Contrast refers to the difference in luminance between objects within an image. The encryption procedure incorporates a non-linear S-box replacement, which establishes a connection between visual contrast and randomness. A standard unaltered image has very little contrast. The calculation of image contrast is determined by utilizing this formula:

$$C = \sum_{j,k=0}^{m-1,n-1} p(j,k)\,|k-j|^2. \tag{6.1}$$

In this equation, $p(j,k)$ represents the location of pixels in gray level co-occurrence matrices. Table 4 presents the contrast values for all nine images. The encrypted images show significantly greater contrast ratings than the original ones. This significant difference demonstrates that the proposed encryption technique effectively minimizes disclosure of data.

6.1.2. Energy

In energy analysis, the sum of squared gray level co-occurrence components is determined. The gray level co-occurrence matrix reveals that in a plain image, pixels with high values tend to cluster in specific regions, resulting in a higher energy value. The energy of the encoded Image 1s lower compared to the original image due to the distribution of energy values in the encoded image. The subsequent equation can be employed to compute it.

$$E = \sum_{j,k} p(j,k)^2. \tag{6.2}$$

6.1.3. Correlation

The correlation test is a widely utilized methodology for quantifying the resemblance between a plain image and its encrypted counterpart. It entails the examination of pixel values in the original image and their comparison with the corresponding values in the encrypted image. It serves as a metric for assessing the degree of association between neighboring pixel values in the two images. A lesser correlation value of the encrypted image confirms that it has been distorted more during encryption.

6.1.4. Homogeneity

Homogeneity is utilized as a quantitative measure to evaluate the proximity between the distributions of elements in the gray level co-occurrence matrix's diagonal and the gray level co-occurrence itself. This assessment involves the application of a mathematical procedure. The range of homogeneity lies in $[0,1]$, with the diagonal components of the gray level co-occurrence matrix determining its magnitude. Small homogeneity scores in encryption signify a stronger algorithm. The following equation is utilized to calculate homogeneity:

$$H = \sum_{j,k} \frac{p(j,k)}{1+|k-j|}. \tag{6.3}$$

The results of the MCL are shown in Table 4. The results demonstrate unequivocally that the proposed image encryption scheme is secure.

Table 4. Results of MLC.

Images	Contrast	Correlation	Energy	Homogeneity
Med-Image 1-Org	0.3607	0.9551	0.2086	0.9009
Med-Image 1-Enc	10.6963	-0.01783	0.0159	0.3889
Med-Image 1-Enc [56]	10.1802	0.00913	0.0334	0.4012
Med-Image 1-Enc [57]	10.0216	0.03001	0.0167	0.3916
Med-Image 1-Enc [58]	10.5286	0.00062	0.0194	0.4012
Med-Image 1-Enc [59]	10.2129	0.00381	0.0234	0.3930
Med-Image 2-Org	0.0964	0.9819	0.1944	0.9697
Med-Image 2-Enc	10.5078	0.00075	0.0156	0.3895
Med-Image 2-Enc [56]	10.2390	0.00093	0.0201	0.3898
Med-Image 2-Enc [57]	10.1904	0.00298	0.0177	0.3909
Med-Image 2-Enc [58]	10.3491	0.00081	0.0161	0.3891
Med-Image 2-Enc [59]	10.2145	0.00119	0.0209	0.3925
Med-Image 3-Org	0.0914	0.9503	0.2764	0.9617
Med-Image 3-Enc	10.5208	-0.00112	0.0156	0.3894
Med-Image 3-Enc [56]	10.4376	0.00121	0.0167	0.3912
Med-Image 3-Enc [57]	10.1903	0.00092	0.0183	0.3904
Med-Image 3-Enc [58]	10.2693	0.00032	0.0180	0.3944
Med-Image 3-Enc [59]	10.0061	0.00120	0.0163	0.4012
Med-Image 4 Org	0.2256	0.9776	0.4199	0.9405
Med-Image 4-Enc	10.4705	0.00101	0.0156	0.3891
Med-Image 4-Enc [56]	10.1283	0.00129	0.0159	0.3936
Med-Image 4-Enc [57]	10.1179	0.00213	0.0161	0.3962
Med-Image 4-Enc [58]	10.3810	0.00173	0.0188	0.4045
Med-Image 4-Enc [59]	10.2940	0.00122	0.0173	0.3981
Med-Image 5-Org	0.35963	0.9208	0.1981	0.9413
Med-Image 5-Enc	10.4583	0.00073	0.0156	0.3903
Med-Image 5-Enc [56]	10.2316	0.00214	0.0167	0.3956
Med-Image 5-Enc [57]	10.1132	0.00195	0.0179	0.3972
Med-Image 5-Enc [58]	10.3350	0.00094	0.0163	0.3982
Med-Image 5-Enc [59]	10.1543	0.00186	0.0193	0.3976
Med-Image 6-Org	0.2844	0.9394	0.3344	0.9188

Continued on next page

Images	Contrast	Correlation	Energy	Homogeneity
Med-Image 6-Enc	10.5157	0.00062	0.0156	0.3898
Med-Image 6-Enc [56]	10.1756	0.00109	0.0160	0.3987
Med-Image 6-Enc [57]	10.1382	0.00154	0.0195	0.4012
Med-Image 6-Enc [58]	10.3902	0.00071	0.0185	0.3917
Med-Image 6-Enc [59]	10.0185	0.00105	0.0176	0.4018
Lena Image-Org	0.4482	0.9024	0.1127	0.8622
Lena Image-Enc	10.4967	0.0011	0.0156	0.3899
Lena Image -Enc [56]	10.2814	0.0012	0.0163	0.4012
Lena Image-Enc [57]	10.2484	0.0014	0.0185	0.4083
Lena Image-Enc [58]	10.4129	0.0015	0.0191	0.3943
Lena Image-Enc [59]	10.3270	0.0017	0.0187	0.3982
Barabara Image-Org	1.0456	0.8246	0.0643	0.7695
Barabara Image-Enc	10.4456	0.0049	0.0156	0.3921
Barabara Image -Enc [56]	10.3184	0.0068	0.0166	0.3938
Barabara Image-Enc [57]	10.4290	0.0109	0.0182	0.3973
Barabara Image-Enc [58]	10.2283	0.0101	0.0174	0.4019
Barabara Image-Enc [59]	10.1840	0.0083	0.0162	0.3956
Tree Image-Org	0.3861	0.9572	0.1298	0.8697
Tree Image-Enc	10.5320	0.0010	0.0156	0.3904
Tree Image -Enc [56]	10.3754	0.0017	0.0174	0.3974
Tree Image-Enc [57]	10.2185	0.0034	0.0180	0.4095
Tree Image-Enc [58]	10.4493	0.0019	0.0159	0.4067
Tree Image-Enc [59]	10.5038	0.0071	0.0193	0.3949

6.2. Information entropy analysis

By means of entropy assessment, the degree of randomness of an encrypted Image 1s quantified. The mathematical formulation of entropy is as follows:

$$E = -\sum_{j=1}^{M-1} Q(X_j) log_2 Q(X_j), \tag{6.4}$$

where $Q(X_j)$ represents the likelihood that the given symbol (X_j) will be present. The gray value distribution of pixels is more uniform with more entropy. Predictability could compromise image security if encrypted image entropy is much less than 8.

Table 5. Results of information entropy analysis.

Images	Information Entropy Value
Med-Image 1-Org	5.538845468845064
Med-Image 1-Enc	7.995592352604773
Med-Image 2-Org	6.441629371127330
Med-Image 2-Enc	7.998595551509233
Med-Image 3-Org	6.528148444114600
Med-Image 3-Enc	7.999155836842628
Med-Image 4 Org	4.665262340281411
Med-Image 4-Enc	7.992226449459711
Med-Image 5-Org	7.178730739603131
Med-Image 5-Enc	7.999264746215498
Med-Image 6-Org	6.276306307901546
Med-Image 6-Enc	7.999096158086002
Lena Image-Org	7.443921390749898
Lena Image-Enc	7.997093894234909
Barabara Image-Org	7.630961729011966
Barabara Image-Enc	7.997428353585646
Tree Image-Org	7.310272448303230
Tree Image-Enc	7.997342743277636

6.3. Differential analysis

Two most common criteria, number of pixel change rate (NPCR) and unified average changing intensity (UACI), are used to quantitatively measure the influence of one pixel change on the encrypted image. Between the two encrypted images, the percentage of different pixel numbers is measured by NPCR and the average intensity of differences is measured by UACI. Let the difference in pixel of two original images is only one and their corresponding encrypted images are denoted by $C_1(i,j)$ and $C_2(i,j)$. The values of NPCR and UACI are calculated using the following formulas:

$$NCPR = \frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j) \times 100\% \tag{6.5}$$

$$UACI = \frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N} \frac{|C_1(i,j)-C_2(i,j)|}{255} \times 100\%, \tag{6.6}$$

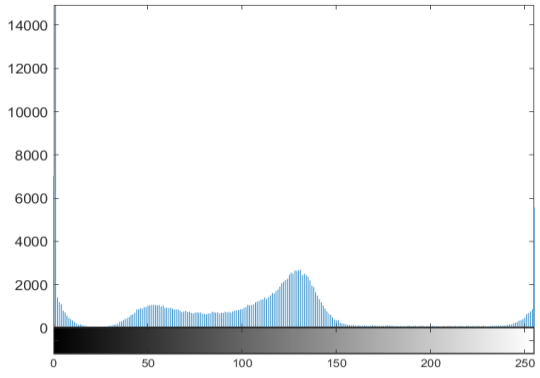
where $D(i,j)$ is zero if $C_1(i,j)$ and $C_2(i,j)$ are the same otherwise it is equal to one. Furthermore, M and N represent the image width and image height, respectively. Table 6 presents a comprehensive analysis of the UACI and NPCR metrics indicating the effectiveness and quality of the proposed image encryption scheme.

Table 6. UACI and NPCR scores of all selected images.

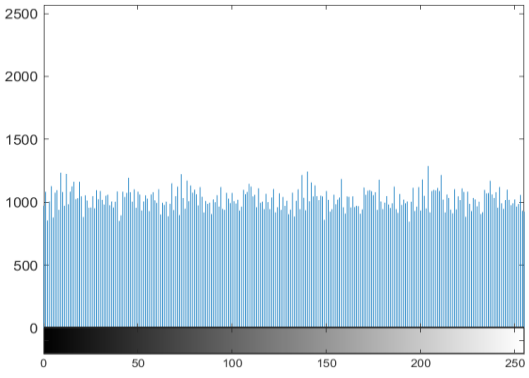
Image	*NCPR %*	*UACI %*
Med-Image 1	*99.618911743164063*	*33.417216282264860*
Med-Image 2	*99.628511372472786*	*33.505320066401367*
Med-Image 3	*99.592464826839830*	*33.440731169361683*
Med-Image 4	*99.657004888803684*	*33.486923718874053*
Med-Image 5	*99.608993530273438*	*33.334975897097117*
Med-Image 6	*99.582672119140625*	*33.547846476236977*
Lena	*99.5926*	*33.5699*
Barabara	*99.5789*	*33.3566*
Tree	*99.6170*	*33.3972*

6.4. Histogram analysis

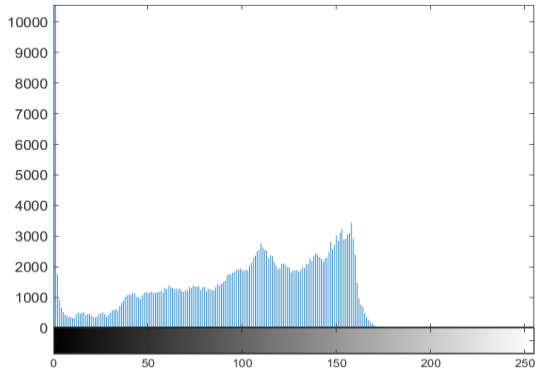
Histograms are representations of the distribution of pixel gray level intensities in an image. A cryptanalyst may utilize the information provided to perform histogram attacks if the distribution has a non-uniform nature. However, the approach has been designed to be resistant to histogram attacks, and information is unidentified if the histogram is uniform and flattened. By analyzing the histograms of both the encrypted and original images, we can observe the differences in color intensities between them. We conducted tests on the histograms of the original and encrypted images and found that the histogram distribution of the encrypted image, generated using the proposed S-box, significantly deviates from that of the original image. In Figure 3, histograms of the original and encrypted images of all nine images, chosen for encryption, are shown. The histogram of the encrypted image appears to be quite uniform, confirming the efficiency of the proposed mechanism. The correlation plots for vertical, horizontal and diagonal neighboring pixels in original and encrypted images are shown in Figure 4. This result indicates that it is exceedingly challenging to exploit the statistical characteristics of the encrypted image to reconstruct the original image.



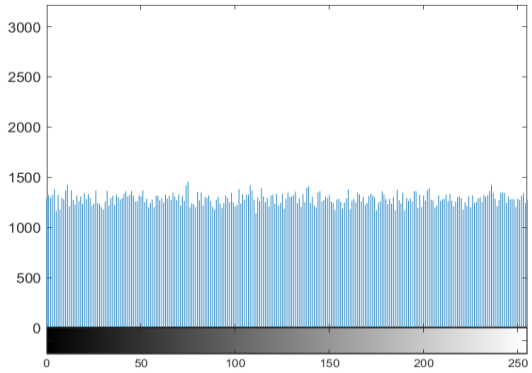
Histogram of Med-Image 1-Org



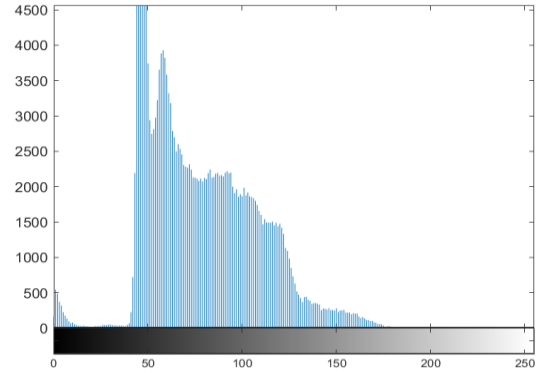
Histogram of Med-Image 1-Enc



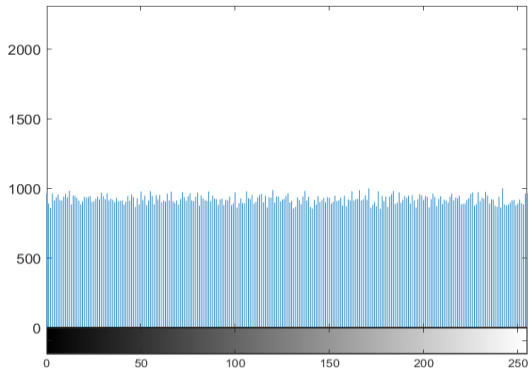
Histogram of Med-Image 2-Org



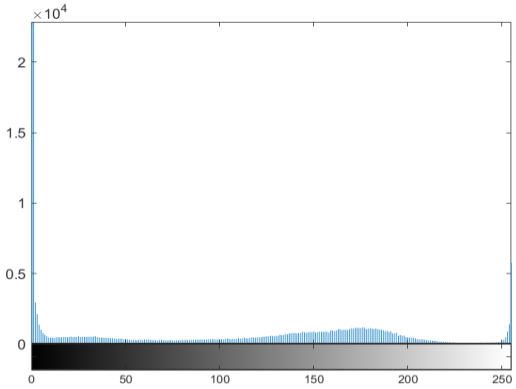
Histogram of Med-Image 2-Enc



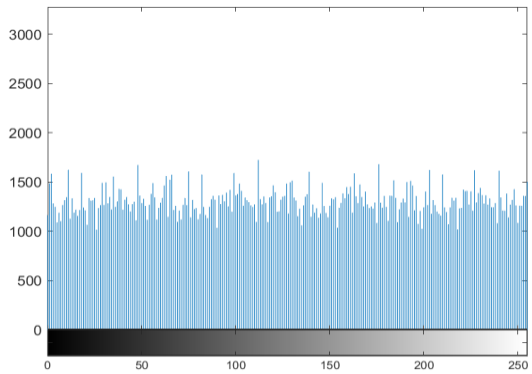
Histogram of Med-Image 3-Org



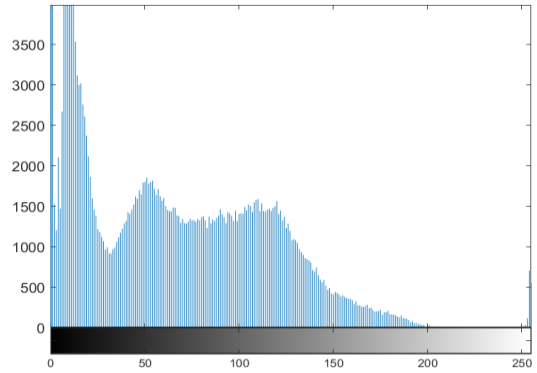
Histogram of Med-Image 3-Enc



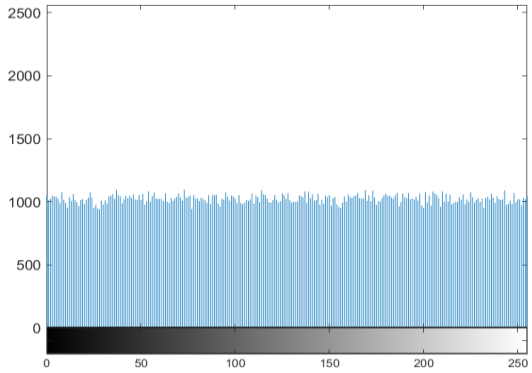
Histogram of Med-Image 4-Org



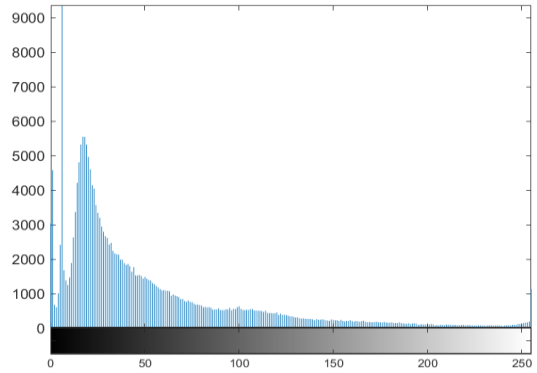
Histogram of Med-Image 4-Enc



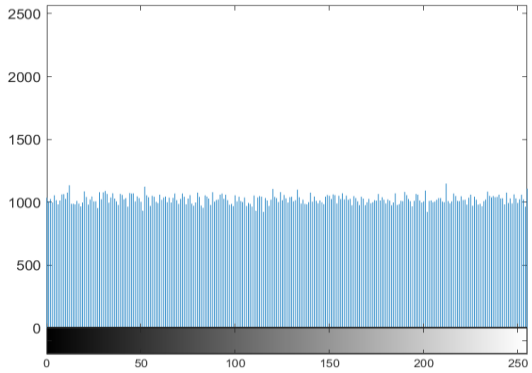
Histogram of Med-Image 5-Org



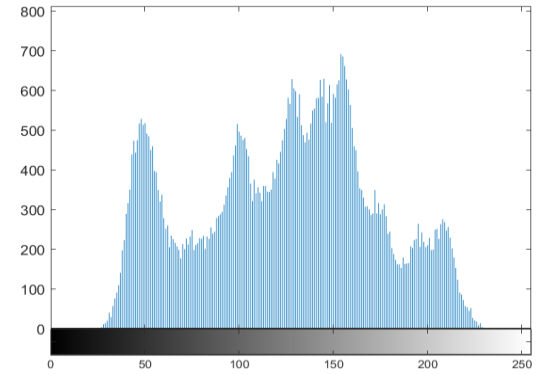
Histogram of Med-Image 5-Enc



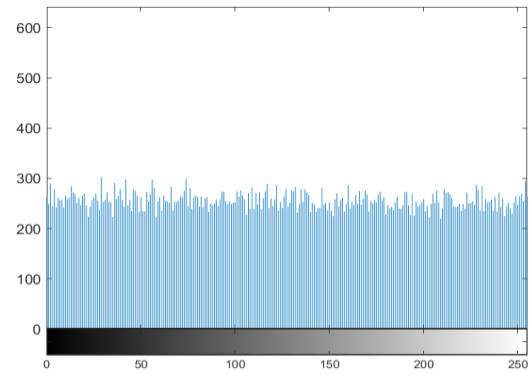
Histogram of Med-Image 6-Org



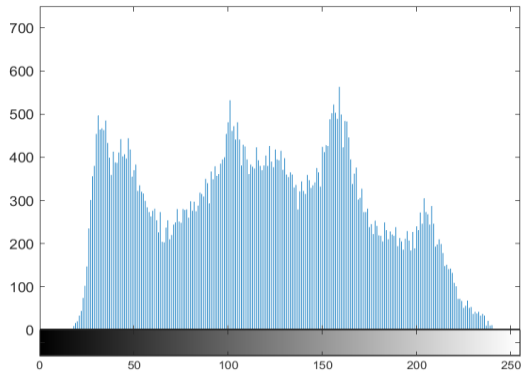
Histogram of Med-Image 6-Enc



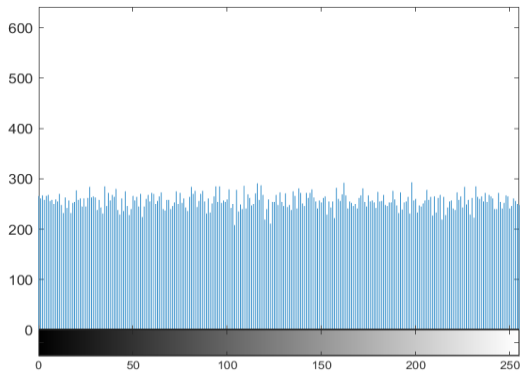
Histogram of Lena Image-Org



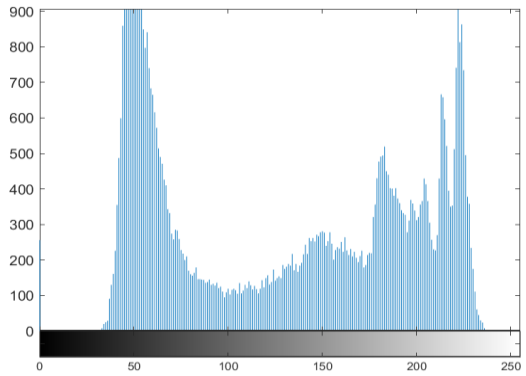
Histogram of Lena Image-Enc



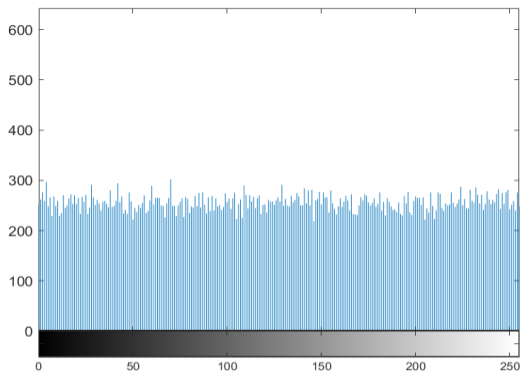
Histogram of Barabara Image-Org



Histogram of Barabara Image-Enc

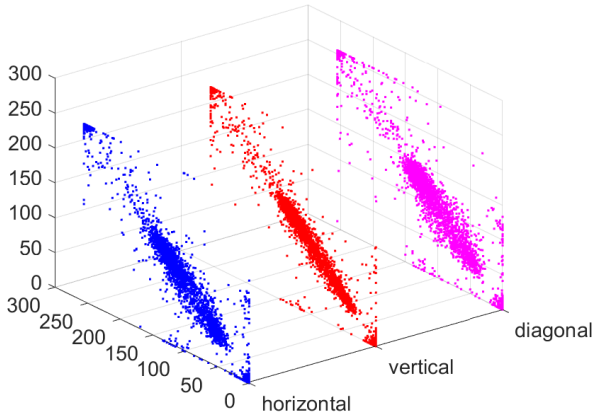


Histogram of Tree Image-Org

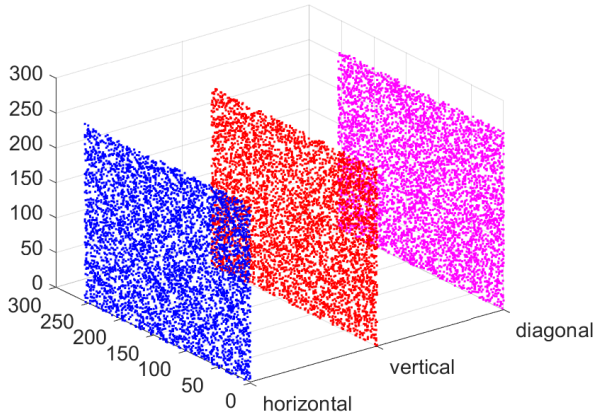


Histogram of Tree Image-Enc

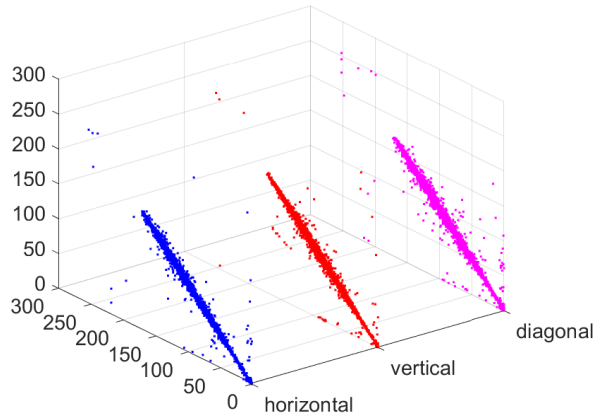
Figure 3. Histogram analysis.



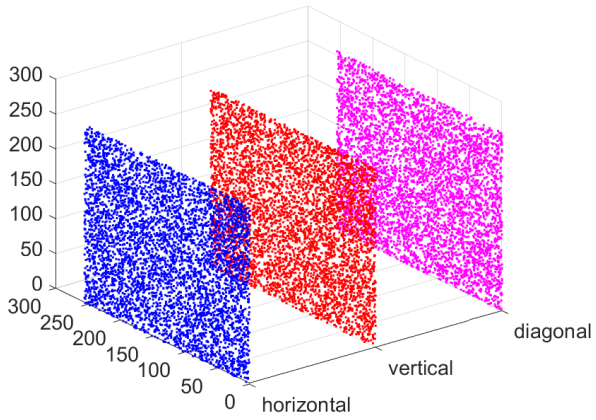
Correlation Coefficients of Med-Image 1-Org



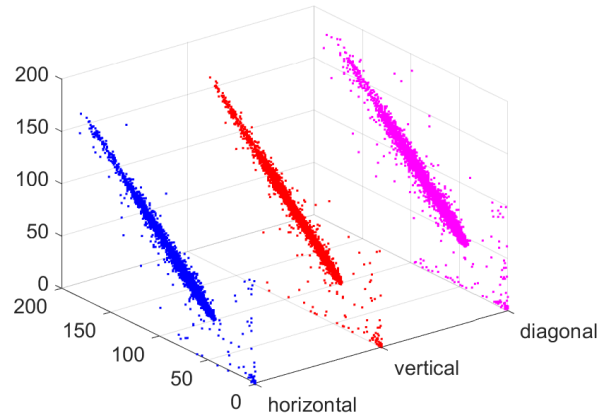
Correlation Coefficients of Med-Image 1-Enc



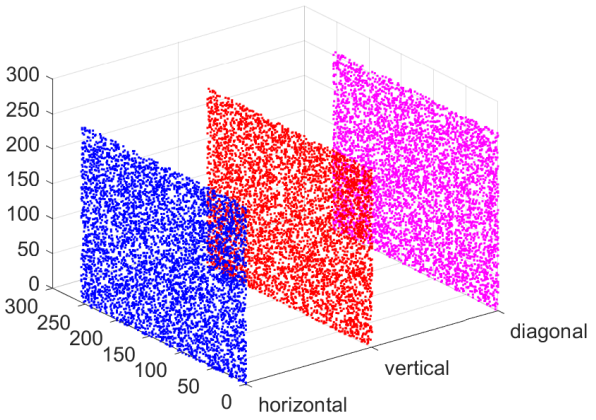
Correlation Coefficients of Med-Image 2-Org



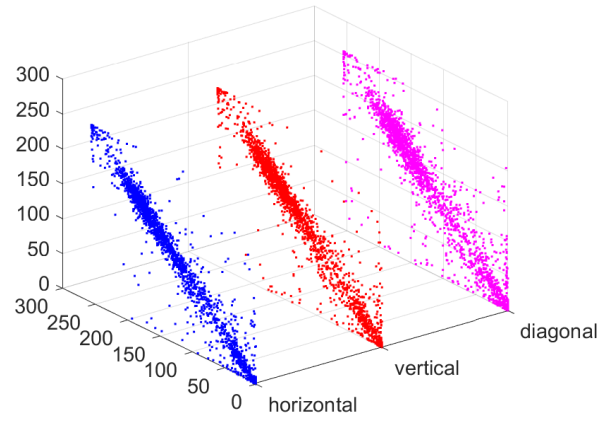
Correlation Coefficients of Med-Image 2-Enc



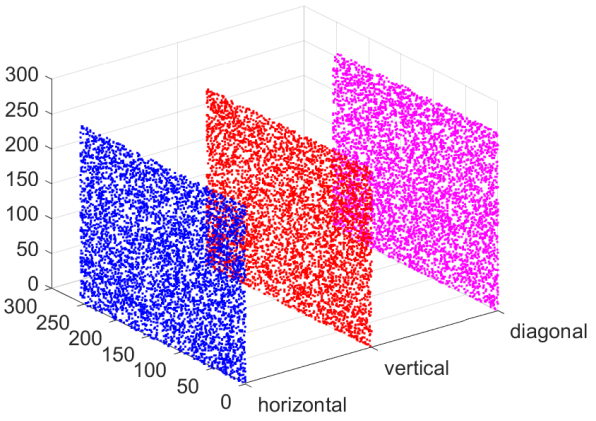
Correlation Coefficients of Med-Image 3-Org



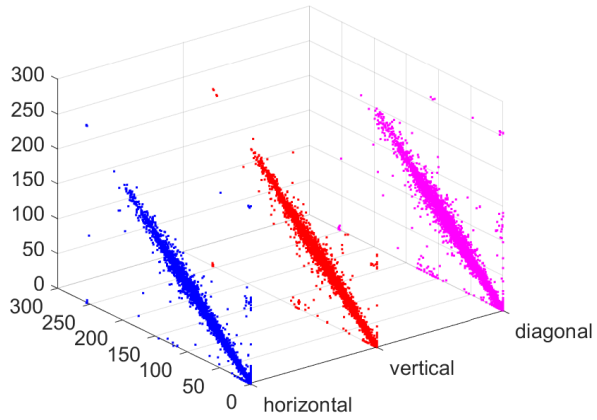
Correlation Coefficients of Med-Image 3-Enc



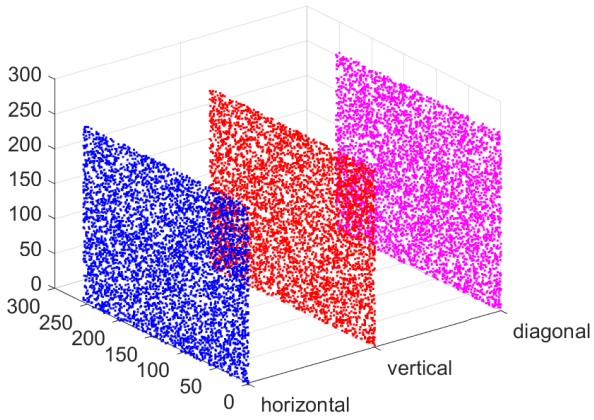
Correlation Coefficients of Med-Image 4-Org



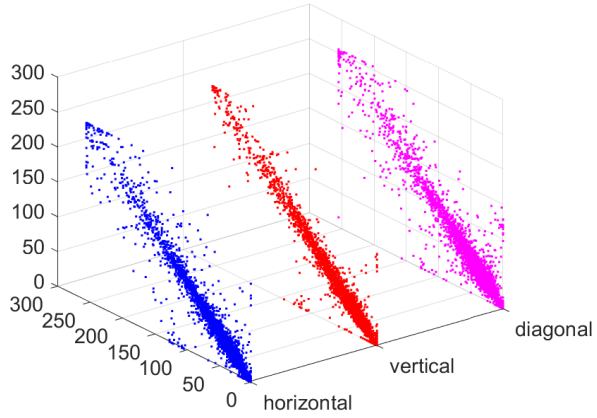
Correlation Coefficients of Med-Image 4-Enc



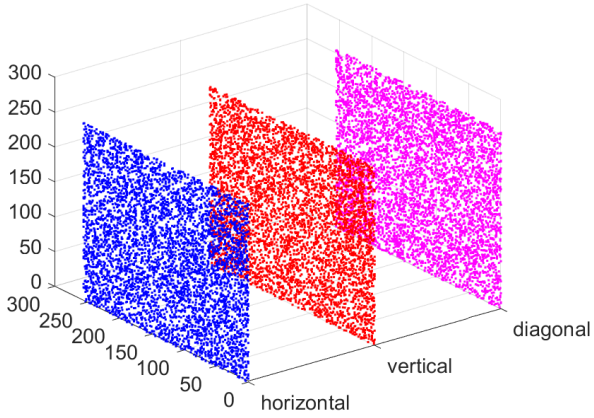
Correlation Coefficients of Med-Image 5-Org



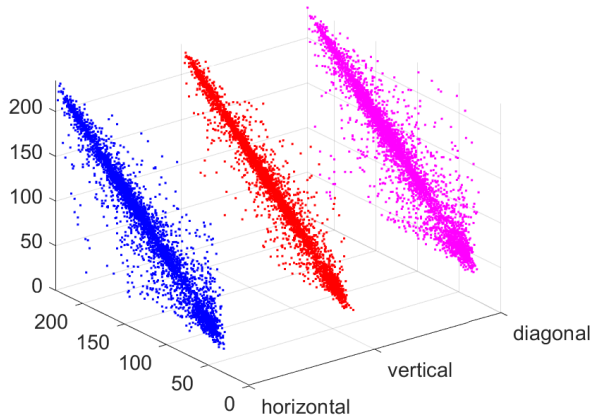
Correlation Coefficients of Med-Image 5-Enc



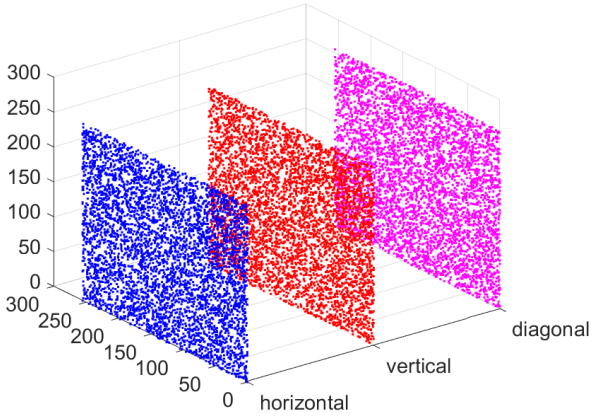
Correlation Coefficients of Med-Image 6-Org



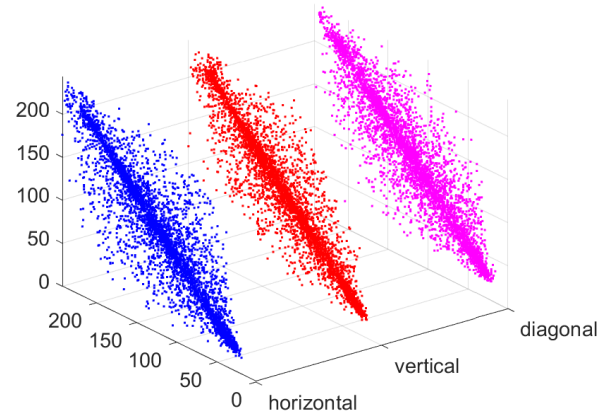
Correlation Coefficients of Med-Image 6-Enc



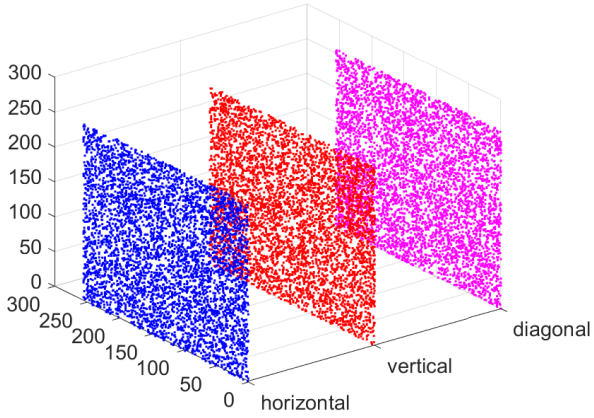
Correlation Coefficients of Lena Image-Org



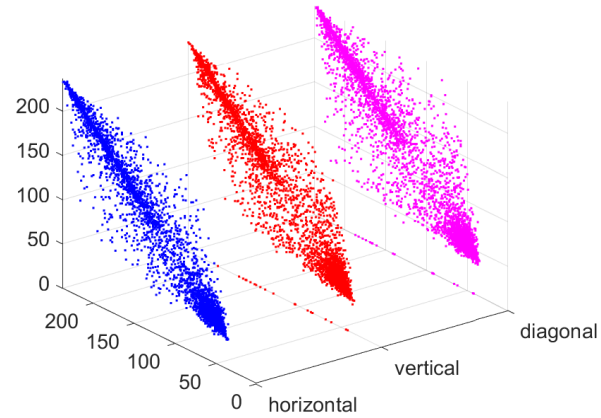
Correlation Coefficients of Lena Image-Enc



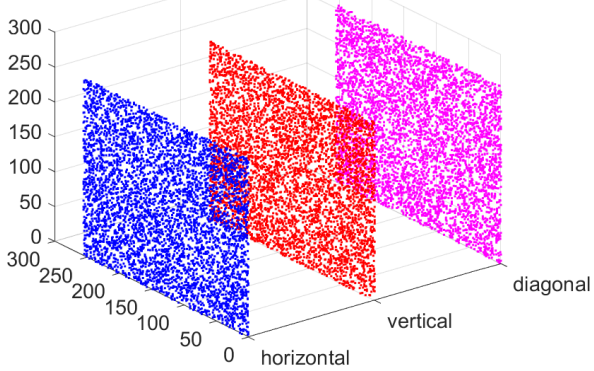
Correlation Coefficients of Barabara Image-Org



Correlation Coefficients of Barabara Image-Enc



Correlation Coefficients of Tree Image-Org



Correlation Coefficients of Tree Image-Enc

Figure 4. Pixel correlation plots.

6.5. Measures of encrypted image quality

In this section, the effectiveness of the presented encryption algorithm is evaluated experimentally. The nine original multiple images, as well as each of their encrypted counterparts, are analyzed here. These ciphered images were produced following the proposed encryption algorithm. The purpose is to evaluate the robustness and dependability of the proposed encryption technique.

6.5.1. Mean squared error

The MSE is used to determine the cumulative squared difference between plain image and cipher image [60]. The statistical formula used to calculate MSE is given below:

$$MSE = \frac{1}{M \times N} \sum_{j=1}^{M} \sum_{i=1}^{N} \big(\alpha(i,j) - \beta(i,j)\big)^2, \tag{6.7}$$

where $\alpha(i,j)$ is the original image and $\beta(i,j)$ is the encrypted image. Moreover, M and N represent the image width and image height, respectively.

6.5.2. Root mean squared error

This criterion [61] provides the discrepancy between the original and encoded images. In order to determine its value, the following relation is applied:

$$RMSE = \sqrt{\frac{1}{M\times N}\sum_{j=1}^{M}\sum_{i=1}^{N}\big(\alpha(i,j)-\beta(i,j)\big)^2}. \tag{6.8}$$

6.5.3. Peak signal to noise ratio

The peak signal-to-noise ratio, abbreviated PSNR [62], is the metric used to determine the fidelity of the encrypted image. The formulas listed below define PSNR:

$$PSNR = 10log_2\left(\frac{Y_{max}^2}{MSE}\right), \tag{6.9}$$

where Y_{max} is the highest possible pixel value in the image.

6.5.4. Maximum and average difference (MD & AD)

Researchers utilized the MD and AD test [62] to calculate the maximum and mean variations between the original $\alpha(i,j)$ and concealed $\beta(i,j)$ images. Formulas for calculating MD and AD scores are as follows:

$$MD = max|\alpha(i,j)-\beta(i,j)| \tag{6.10}$$

$$AD = \frac{1}{M\times N}\sum_{j=1}^{M}\sum_{i=1}^{N}|\alpha(i,j)-\beta(i,j)|. \tag{6.11}$$

6.5.5. Mutual information (MI)

According to [63], MI quantifies the quantity of original image data that can be reconstructed from the encrypted version. Applying the following formula, the value of MI can be calculated:

$$MI = \sum_{i\in\alpha}\sum_{j\in\beta}\rho(i,j)\,log_2\frac{\rho(i,j)}{\rho(i)\rho(j)}. \tag{6.12}$$

Here $\rho(i,j)$ represents joint probability function of α and β.

6.5.6. Universal quality index (UQI)

According to reference [63], the UQI technique breaks down assessments of picture distortion into three distinct categories: Brightness, structural similarity, and contrast. In order to determine the value of the UQI, the following statistical equation is used.

$$UQI = \frac{4\rho_\alpha\rho_\beta\rho_{\alpha\beta}}{\left(\rho_\alpha^2-\rho_\beta^2\right)\left(\partial_\alpha^2-\partial_\beta^2\right)}. \tag{6.13}$$

The symbols ρ_α and ρ_β represent the mean scores of the actual and altered images, respectively. In a similar way, ∂_α and ∂_β represent the standard deviation of the source and altered images, respectively.

6.5.7. Structural similarity (SSIM)

SSIM [63] is a refined variant of the UQI that is used to determine how similar the two images are to one another. For this purpose, SSIM assumes that the other Image 1s error-free before evaluating the precision of the first image. The SSIM score is calculated by applying the following equation to an image's (R, S) window pairs:

$$SSIM = \frac{(2\theta_R\theta_S+b_1)(2\pi_R\pi_S+b_2)}{(\theta_R^2+\theta_S^2+b_1)(\pi_R^2+\pi_S^2+b_2)}, \tag{6.14}$$

where π_R and π_S are the standard deviations of R and S, whereas θ_R and θ_S are the means of R and S. The possible value range of the SSIM index is [-1,1]. When the two images are alike, the SSIM $= 1$.

6.5.8. Normalized cross correlation (NCC)

According to [64], the resemblance between both images is derived through the use of the correlation function. NCC finds the relationship between the initial and ciphered images. NCC is determined by the following equation:

$$NCC = \sum_{j=1}^{M}\sum_{i=1}^{N}\left(\frac{\alpha(i,j)\times\beta(i,j)}{\sum_{j=1}^{M}\sum_{i=1}^{N}|\alpha(i,j)|^2}\right). \tag{6.15}$$

6.5.9. Normalized absolute error (NAE)

The NAE [60] is utilized to evaluate the effectiveness of an image encryption procedure by assessing each of the pixels in the initial image and those in the scrambled image. To determine the NAE between both images (unencrypted and encrypted), the following formula is used:

$$NAE = \frac{\sum_{j=1}^{M}\sum_{i=1}^{N}|\alpha(i,j)-\beta(i,j)|}{\sum_{j=1}^{M}\sum_{i=1}^{N}\alpha(i,j)}. \tag{6.16}$$

6.5.10. Structural content (SC)

The connection between both images (plain and ciphered) is analyzed using SC, which is a correlation-based metric. The score of SC [64] is calculated using the following formula:

$$SC = \frac{\sum_{j=1}^{M}\sum_{i=1}^{N}|\alpha(i,j)|^2}{\sum_{j=1}^{M}\sum_{i=1}^{N}|\beta(i,j)|^2}. \tag{6.17}$$

Table 7 presents a comprehensive analysis of the aforementioned image quality metrics.

Table 7. Results of different image quality metrics.

Images	MSE	RMSC	PSNR	MD	AD	MI	UQI	SSIM	NCC	NAE	SC
Med-Image 1	13728	117.1696	27.4426	255.0	-57.5962	-1.01389	0.0054	-0.000049	0.9030	1.3832	0.4538
Med-Image 2	11149	105.5917	27.8945	253.0	-48.3941	-1.0077	0.0021	-0.000096	1.0517	1.0906	0.4407
Med-Image 3	8964	94.6823	26.0824	180.0	-51.1355	-1.0093	0.0012	-0.000064	1.4499	1.0203	0.3084
Med-Image 4	17077	130.6791	26.9687	255.0	-73.6196	-1.0127	0.0016	-0.000043	0.7550	2.0285	0.4189
Med-Image 5	12124	110.1127	27.7124	255.0	-64.3602	-1.0102	0.0009	-0.000085	1.2329	1.4249	0.3011
Med-Image 6	15057	122.7096	27.2420	255.0	-83.8400	-1.0132	0.0003	0.000195	1.2466	2.3282	0.2051
Lena Image	7777	88.1901	28.2221	230.0	-2.6871	-1.0415	0.0595	0.000502	0.8890	0.5890	0.8211
Barabara Image	8529	92.3570	28.1286	237.0	-9.9577	-1.0415	0.0175	0.000251	0.8919	0.6479	0.7732
Tree Image	10001	100.0072	27.4946	232.0	1.5429	-1.0420	-0.2945	-0.000455	0.7770	0.6322	0.9755

6.6. NIST test

The NIST STS800 test suite is applicable for the first six images shown in Figure 2. The reason being that all six images have number bits higher than 10^6, and the NIST tool has the prerequisite, is that the candidate sequence under examination for the randomness test should have at least 10^6 bits, whereas the size of the other 3 benchmark images is 256×256, the total bits are less than 10^6. The outcomes of these analysis are given in Table 8.

Table 8. Outcomes of NIST Test.

Test type	**Image-1**	**Image-2**	**Image-3**	**Image-4**	**Image-5**	**Image-6**
Monobit Test	0.43903	0.47770	0.35340	0.69731	0.88392	0.77641
Block Frequency Test	0.99997	0.14594	0.96356	0.82187	0.40998	0.08800
Runs Test	0.47271	0.58403	0.38273	0.23048	0.88078	0.13415
Longest Runs Test	0.18970	0.45625	0.07606	0.16298	0.18540	0.21418
Rank Test	0.43982	0.55657	0.94818	1.4328e-10	0.42273	0.88511
DFT Test	0.50274	0.11032	0.56317	0.39283	0.34926	0.60732

Continued on next page

Test type	Image-1	Image-2	Image-3	Image-4	Image-5	Image-6
Non-Overlap Template	0.12903	0.04168	0.21012	0.001338	0.80155	0.04310
Overlapping Template	0.075307	0.00450	0.60909	0.002588	0.79531	0.57313
Maurer's Universal	0.70728	0.49828	0.89436	0.068614	0.75774	0.56219
Linear Complexity Test	0.90873	0.25357	0.79977	0.967248	0.45090	0.63855
Serial Test	0.29041	0.42942	0.34673	0.48921	0.08615	0.013220
ApEn Entropy	0.84024	0.42091	0.08957	0.76294	0.21730	0.91937
Cumulative Sums	0.00123	0.82715	0.44668	0.46938	0.52637	0.53563
Excursion Test	0.58931	0.26336	0.26599	0.29880	0.33396	0.34847
Random Excursion Variant	0.76302	0.53474	0.88917	0.55629	0.43098	0.67804

7. Conclusions

This research presents a significant contribution to the field of medical image encryption by introducing a novel algorithm that addresses the security requirements of e-Healthcare systems. A novel methodology is developed to generate substitution-boxes through the combination of a multiplicative cyclic group and a permutation group. To assess the efficacy of the suggested S-box, several benchmark algebraic parameters are performed. The outcomes obtained from these assessment mechanisms provide evidence for the reliability and robustness of the proposed S-box in mitigating numerous attacks. An algorithm for robust medical image encryption is devised that is based on the generated substitution box. In order to evaluate the quality of the encryption scheme, benchmark assessments that are specifically tailored for image encryption techniques are employed. The outcomes demonstrate that the proposed encryption method can successfully encrypt medical images. In the future, we plan on using these resilient S-boxes, created by the suggested approach, in multimedia security applications beyond only image encryption. This includes video and audio steganography as well as watermarking.

Use of AI tools declaration

The authors declare that they have not used Artificial Intelligence (AI) tools in the creation of this article.

Conflict of interest

The authors declare no conflicts of interest.

References

1. Y. Dai, H. Z. Wang, Z. X. Zhou, Z. Y. Jin, Research on medical image encryption in telemedicine systems, *Technol. Health Care*, **24** (2016), S435–S442. http://dx.doi.org/10.3233/THC-161166
2. V. Pavithra, J. Chandrasekaran, *Developing security solutions for telemedicine applications: Medical image encryption and watermarking*, In: Research anthology on telemedicine efficacy, adoption, and impact on healthcare delivery. http://dx.doi.org/10.4018/978-1-7998-8052-3.ch032
3. W. J. Cao, Y. C. Zhou, C. L. P. Chen, L. M. Xia, Medical image encryption using edge maps, *Signal Process.*, **132** (2017), 96–109. https://doi.org/10.1016/j.sigpro.2016.10.003
4. Z. Y. Hua, S. Yi, Y. C. Zhou, Medical image encryption using high-speed scrambling and pixel adaptive diffusion, *Signal Process.*, **144** (2018), 134–144. https://doi.org/10.1016/j.sigpro.2017.10.004
5. D. S. Laiphrakpam, M. S. Khumanthem, Medical image encryption based on improved ElGamal encryption technique, *Optik*, **147** (2017), 88–102. https://doi.org/10.1016/j.ijleo.2017.08.028
6. S. T. Kamal, K. M. Hosny, T. M. Elgindy, M. M. Darwish, M. M. Fouda, A new image encryption algorithm for grey and color medical images, *IEEE Access*, **9** (2021), 37855–37865. https://doi.org/10.1109/ACCESS.2021.3063237
7. K. Jain, A. Aji, P. Krishnan, Medical image encryption scheme using multiple chaotic maps, *Pattern Recogn. Lett.*, **152** (2021), 356–364. https://doi.org/10.1016/j.patrec.2021.10.033
8. M. Ş. Açkkapi, F. Özkaynak, A. B. Özer, Side-channel analysis of chaos-based substitution box structures, *IEEE Access*, **7** (2019), 79030–79043. https://doi.org/10.1109/ACCESS.2019.2921708
9. N. Mouha, Q. J. Wang, D. W. Gu, B. Preneel, *Differential and linear cryptanalysis using mixed-integer linear programming*, In: Information security and cryptology: 7th International Conference, Inscrypt 2011, Beijing, China, November 30-December 3, 2011.
10. H. M. Heys, A tutorial on linear and differential cryptanalysis, *Cryptologia*, **26** (2002), 189–221. https://doi.org/10.1080/0161-110291890885
11. A. Shafique, K. H. Khan, M. M. Hazzazi, I. Bahkali, Z. Bassfar, M. U. Rehman, Chaos and cellular automata-based substitution box and its application in cryptography, *Mathematics*, **11** (2023), 2322. https://doi.org/10.3390/math11102322
12. A. H. Zahid, M. J. Arshad, M. Ahmad, N. F. Soliman, W. El-Shafai, Dynamic S-box generation using novel chaotic map with nonlinearity tweaking, *Comput. Mater. Con.*, **75** (2023), 3011–3026. https://doi.org/10.32604/cmc.2023.037516
13. A. Razaq, G. Alhamzi, S. Abbas, M. Ahmad, A. Razzaque, Secure communication through reliable S-box design: A proposed approach using coset graphs and matrix operations, *Heliyon*, **9** (2023), e15902. https://doi.org/10.1016/j.heliyon.2023.e15902
14. A. Alkhayyat, M. Ahmad, N. Tsafack, M. Tanveer, D. H. Jiang, A. A. Abd El-Latif, A novel 4D hyperchaotic system assisted josephus permutation for secure substitution-box generation, *J. Sign. Process. Syst.*, **94** (2022), 315–328. https://doi.org/10.1007/s11265-022-01744-9
15. N. A. Azam, U. Hayat, M. Ayub, A substitution box generator, its analysis, and applications in image encryption, *Signal Process.*, **187** (2021), 108144. https://doi.org/10.1016/j.sigpro.2021.108144

16. A. A. A. El-Latif, B. Abd-El-Atty, A. Belazi, A. M. Iliyasu, Efficient chaos-based substitution-box and its application to image encryption, *Electronics*, **10** (2021), 1392. https://doi.org/10.3390/electronics10121392
17. N. Siddiqui, A. Naseer, M. Ehatisham-ul-Haq, A novel scheme of substitution-box design based on modified Pascal's triangle and elliptic curve, *Wireless Pers. Commun.*, **116** (2021), 3015–3030. https://doi.org/10.1007/s11277-020-07832-y
18. A. Sarkar, J. Dey, S. Karforma, Musically modified substitution-box for clinical signals ciphering in wireless telecare medical communicating systems, *Wireless Pers. Commun.*, **117** (2021), 727–745. https://doi.org/10.1007/s11277-020-07894-y
19. S. Ibrahim, H. Alhumyani, M. Masud, S. S. Alshamrani, O. Cheikhrouhou, G. Muhammad, et al., Framework for efficient medical image encryption using dynamic S-boxes and chaotic maps, *IEEE Access*, **8** (2020), 160433–160449. https://doi.org/10.1109/ACCESS.2020.3020746
20. C. R. Zhang, J. X. Chen, D. M. Chen, W. Wang, Y. S. Zhang, Y. C. Zhou, Exploiting substitution box for cryptanalyzing image encryption schemes with DNA coding and nonlinear dynamics, *IEEE T. Multimedia*, **26** (2024), 1114–1128. https://doi.org/10.1109/TMM.2023.3276504
21. X. L. Liu, X. J Tong, Z. Wang, M. Zhang, A new n-dimensional conservative chaos based on generalized Hamiltonian system and its' applications in image encryption, *Chaos Soliton. Fract.*, **154** (2022), 111693. https://doi.org/10.1016/j.chaos.2021.111693
22. H. Nematzadeh, R. Enayatifar, H. Motameni, F. G. Guimarães, V. N. Coelho, Medical image encryption using a hybrid model of modified genetic algorithm and coupled map lattices, *Opt. Laser. Eng.*, **110** (2018), 24–32. https://doi.org/10.1016/j.optlaseng.2018.05.009
23. Z. Mishra, B. Acharya, High throughput and low area architectures of secure IoT algorithm for medical image encryption, *J. Inf. Secur. Appl.*, **53** (2020), 102533. https://doi.org/10.1016/j.jisa.2020.102533
24. X. L. Liu, X. J. Tong, Z. Wang, M. Wang, A novel hyperchaotic encryption algorithm for color image utilizing DNA dynamic encoding and self-adapting permutation, *Multimed. Tools Appl.*, **81** (2022), 21779–21810. https://doi.org/10.1007/s11042-022-12472-4
25. A. T. Hashim, A. K. Jabbar, Q. F. Hassan, Medical image encryption based on hybrid AES with chaotic map, *J. Phys.: Conf. Ser.*, 1973, 012037. https://doi.org/10.1088/1742-6596/1973/1/012037
26. W. El-Shafai, F. Khallaf, E. S. M. El-Rabaie, F. E. A. El-Samie, Robust medical image encryption based on DNA-chaos cryptosystem for secure telemedicine and healthcare applications, *J. Ambient Intell. Human. Comput.*, **12** (2021), 9007–9035. https://doi.org/10.1007/s12652-020-02597-5
27. M. F. Khan, K. Saleem, M. A. Alshara, S. Bashir, Multilevel information fusion for cryptographic substitution box construction based on inevitable random noise in medical imaging, *Sci. Rep.*, **11** (2021), 14282. https://doi.org/10.1038/s41598-021-93344-z
28. K. C. P. Shankar, S. P. Shyry, A novel hybrid encryption method using S-box and Henon maps for multidimensional 3D medical images, *Soft Comput.*, 2023. https://doi.org/10.1007/s00500-023-08006-1
29. U. Hayat, N. A. Azam, H. R. Gallegos-Ruiz, S. Naz, L. Batool, A truly dynamic substitution box generator for block ciphers based on elliptic curves over finite rings, *Arab. J. Sci. Eng.*, **46** (2021), 8887–8899. https://doi.org/10.1007/s13369-021-05666-9

30. K. Z. Zamli, F. Din, H. S. Alhadawi, Exploring a Q-learning-based chaotic naked mole rat algorithm for S-box construction and optimization, *Neural Comput. Applic.*, **35** (2023), 10449–10471. https://doi.org/10.1007/s00521-023-08243-3
31. A. A. Alzaidi, M. Ahmad, H. S. Ahmed, E. A. Solami, Sine-cosine optimization-based bijective substitution-boxes construction using enhanced dynamics of chaotic map, *Complexity*, **2018** (2018), 1–16. https://doi.org/10.1155/2018/9389065
32. A. Razaq, M. Ahmad, A.Yousaf, M. Alawida, A. Ullah, U. Shuaib, A group theoretic construction of large number of AES-like substitution-boxes, *Wireless Pers. Commun.*, **122** (2022), 2057–2080. https://doi.org/10.1007/s11277-021-08981-4
33. S. Ibrahim, A. M. Abbas, Efficient key-dependent dynamic S-boxes based on permutated elliptic curves, *Inform. Sciences*, **558** (2021), 246–264. https://doi.org/10.1016/j.ins.2021.01.014
34. B. M. Alshammari, R. Guesmi, T. Guesmi, H. Alsaif, A. Alzamil, Implementing a symmetric lightweight cryptosystem in highly constrained IoT devices by using a chaotic S-box, *Symmetry*, **13** (2021), 129. https://doi.org/10.3390/sym13010129
35. H. S. Alhadawi, M. A. Majid, D. Lambić, M. Ahmad, A novel method of S-box design based on discrete chaotic maps and cuckoo search algorithm, *Multimed. Tools Appl.*, **80** (2021), 7333–7350. https://doi.org/10.1007/s11042-020-10048-8
36. M. Khan, T. Shah, M. A. Gondal, An efficient technique for the construction of substitution box with chaotic partial differential equation, *Nonlinear Dyn.*, **73** (2013), 1795–1801. https://doi.org/10.1007/s11071-013-0904-x
37. M. Khan, T. Shah, An efficient construction of substitution box with fractional chaotic system, *Signal Image Video P.*, **9** (2015), 1335–1338. https://doi.org/10.1007/s11760-013-0577-4
38. M. Long, L. L. Wang, S-box design based on discrete chaotic map and improved artificial bee colony algorithm, *IEEE Access*, **9** (2021), 86144–86154. https://doi.org/10.1109/ACCESS.2021.3069965
39. R. Soto, B. Crawford, F. G. Gonzáez, R. Olivares, Human behaviour based optimization supported with self-organizing maps for solving the S-box design Problem, *IEEE Access*, **9** (2021), 84605–84618. https://doi.org/10.1109/ACCESS.2021.3087139
40. W. H. Yan, Q. Ding, A novel S-box dynamic design based on nonlinear-transform of 1D chaotic maps, *Electronics*, **10** (2021), 1313. https://doi.org/10.3390/electronics10111313
41. P. Z Zhou, J. X. Du, K. Zhou, S. F.Wei, 2D mixed pseudo-random coupling PS map lattice and its application in S-box generation, *Nonlinear Dyn.*, **103** (2021), 1151–1166. https://doi.org/10.1007/s11071-020-06098-0
42. S. Yang, X. J. Tong, Z. Wang, M. Zhang, S-box generation algorithm based on hyperchaotic system and its application in image encryption, *Multimed. Tools Appl.*, **82** (2023), 25559–25583. https://doi.org/10.1007/s11042-023-14394-1
43. D. Lambić, A novel method of S-box design based on discrete chaotic map, *Nonlinear Dyn.*, **87** (2017), 2407–2413. https://doi.org/10.1007/s11071-016-3199-x
44. G. J Liu, W. W. Yang, W. W. Liu, Y. W. Dai, Designing S-boxes based on 3-D four-wing autonomous chaotic system, *Nonlinear Dyn.*, **82** (2015), 1867–1877. https://doi.org/10.1007/s11071-015-2283-y
45. L. Y. Liu, Y. Q. Zhang, X. Y. Wang, A novel method for constructing the S-box based on spatiotemporal chaotic dynamics, *Appl. Sci.*, **8** (2018), 2650. https://doi.org/10.3390/app8122650

46. X. Y. Wang, J. J. Yang, A novel image encryption scheme of dynamic S-boxes and random blocks based on spatiotemporal chaotic system, *Optik*, **217** (2020), 164884. https://doi.org/10.1016/j.ijleo.2020.164884
47. A. Razaq, Iqra, M. Ahmad, M. A. Yousaf, S. Masood, A novel finite rings based algebraic scheme of evolving secure S-boxes for images encryption, *Multimed. Tools. Appl.*, **80** (2021), 20191–20215. https://doi.org/10.1007/s11042-021-10587-8
48. S. Saeed, M. S. Umar, M. A. Ali, M. Ahmad, Fisher-yates chaotic shuffling based image encryption, *arXiv preprint*, 2014. https://doi.org/10.48550/arXiv.1410.7540
49. A. Manzoor, A. H. Zahid, M. T. Hassan, A new dynamic substitution box for data security using an innovative chaotic map, *IEEE Access*, **10** (2022), 74164–74174. https://doi.org/10.1109/ACCESS.2022.3184012
50. X. L. Liu, X. J. Tong, M. Zhang, Z. Wang, A highly secure image encryption algorithm based on conservative hyperchaotic system and dynamic biogenetic gene algorithms, *Chaos Soliton. Fract.*, **171** (2023), 113450. https://doi.org/10.1016/j.chaos.2023.113450
51. J. Pieprzyk, G. Finkelstein, Towards effective nonlinear cryptosystem design, *IEE P. Comput. Dig. T.*, **135** (1988), 325–335.
52. E. Biham, A. Shamir, Differential cryptanalysis of DES-like cryptosystems, *J. Cryptology*, **4** (1991), 3–72. https://doi.org/10.1007/BF00630563
53. M. Matsui, *Linear cryptanalysis method for DES cipher*, In: Workshop on the theory and application of of cryptographic techniques Lofthus, Norway, May 23–27, 1993 Proceedings, Springer, **765** (2003).
54. A. F. Webster, S. E. Tavares, *On the design of S-boxes.* In: Conference on the theory and application of cryptographic techniques, Heidelberg: Springer Berlin, 1985, 523–534. https://doi.org/10.1007/3-540-39799-X_41
55. I. Hussain, T. Shah, M. A. Gondal, H. Mahmood, Generalized majority logic criterion to analyze the statistical strength of S-boxes, *Z. Naturforsch. A*, **67** (2012), 282–288. https://doi.org/10.5560/zna.2012-0022
56. I. Hussain, A. Anees, T. A. Al-Maadeed, A novel encryption algorithm using multiple semifield S-boxes based on permutation of symmetric group, *Comp. Appl. Math.*, **42** (2023), 80. https://doi.org/10.1007/s40314-023-02208-x
57. A. Razzaque, A. Razaq, S. M. Farooq, I. Masmali, M. I. Faraz, An efficient S-box design scheme for image encryption based on the combination of a coset graph and a matrix transformer, *Electron. Res. Arch.*, **31** (2023), 2708–2732. https://doi.org/10.3934/era.2023137
58. S. L Zhu, X. H. Deng, W. D. Zhang, C. X. Zhu, Secure image encryption scheme based on a new robust chaotic map and strong S-box, *Math. Comput. Simulat.*, **207** (2023), 322–346. https://doi.org/10.1016/j.matcom.2022.12.025
59. Y. Y. Su, X. J. Tong, M. Zhang, Z. Wang, Efficient image encryption algorithm based on dynamic high-performance S-box and hyperchaotic system, *Phys. Scripta*, **98** (2003), 065215. https://doi.org/10.1088/1402-4896/acd1c3
60. A. M. Eskicioglu, P. S. Fisher, Image quality measures and their performance, *IEEE T. Commu.*, **43** (1995), 2959–2965. https://doi.org/10.1109/26.477498
61. N. F. F. Areed, S. S. A. Obayy, Novel design of symmetric photonic bandgap based image encryption system, *Prog. Electroma. Res. C*, **30** (2012), 225–239. https://doi.org/10.2528/PIERC12050205

62. Q. Huynh-Thu, M. Ghanbari, Scope of validity of PSNR in image/video quality assessment, *Electron. Lett.*, **44** (2008), 800–801. https://doi.org/10.1049/el:20080522
63. Z. Wang, A. C. Bovik, H. R. Sheikh, E. P. Simoncelli, Image quality assessment: From error visibility to structural similarity, *IEEE T. Image Process.*, **13** (2004), 600–612. https://doi.org/10.1109/TIP.2003.819861
64. Z. Wang, A. C. Bovik, A universal image quality index, *IEEE Signal Proc. Let.*, **9** (2002), 81–84. https://doi.org/10.1109/97.995823

AIMS Press