3D Res (2017)8:26
DOI 10.1007/s13319-017-0135-x

3DR EXPRESS

A Novel Image Encryption Based on Algebraic S-box and Arnold Transform

Shabieh Farwa · Nazeer Muhammad · Tariq Shah · Sohail Ahmad

Received: 5 May 2017 / Revised: 22 June 2017 / Accepted: 12 July 2017

Abstract Recent study shows that substitution box (S-box) only cannot be reliably used in image encryption techniques. We, in this paper, propose a novel and secure image encryption scheme that utilizes the combined effect of an algebraic substitution box along with the scrambling effect of the Arnold transform. The underlying algorithm involves the application of S-box, which is the most imperative source to create confusion and diffusion in the data. The speciality of the proposed algorithm lies, firstly, in the high sensitivity of our S-box to the choice of the initial conditions which makes this S-box stronger than the chaos-based S-boxes as it saves computational labour by deploying a comparatively simple and direct approach based on the algebraic structure of the multiplicative cyclic group of the Galois field. Secondly the proposed method becomes more secure by considering a combination of S-box with certain number of iterations of the Arnold transform. The strength of the S-box is examined in terms of various performance indices such as nonlinearity, strict avalanche criterion, bit independence criterion, linear and differential approximation probabilities etc. We prove through the most significant techniques used for the statistical analyses of the encrypted image that our image encryption algorithm satisfies all the necessary criteria to be usefully and reliably implemented in image encryption applications.

Keywords S-box · Galois field $GF(2^8)$ · Primitive element · Arnold transform · Image encryption

1 Introduction

Increased traffic of confidential information over internet demands high level of security for safe communication. This has become the most challenging problem of the recent world to keep secret data protected from the adversaries.

Shannon [1] laid the foundation of modern cryptography. Cryptography is known as the science of changing the useful information into dummy data so that except for the intended recipient, nobody can access the secret information. Mainly there are two classes of cryptography; symmetric key cryptography and the asymmetric or public key cryptography. This

S. Farwa (✉) · N. Muhammad · S. Ahmad
Department of Mathematics, COMSATS Institute of Information Technology, Wah Campus, Wah Cantt, Pakistan
e-mail: drsfarwa@gmail.com

N. Muhammad
e-mail: nazeermuhammad@ciitwah.edu.pk

S. Ahmad
e-mail: sohailahmad@ciitwah.edu.pk

T. Shah
Department of Mathematics, Quaid-i-Azam University, Islamabad, Pakistan
e-mail: stariqshah@gmail.com

Published online: 19 July 2017

classification is based on the keys. In symmetric key cryptography same key is used on both the ends to encrypt and decrypt information. However in asymmetric key cryptography there are two different keys known as the private key and the public key.

It has been established in literature that the substitution box (S-box) is a standout in symmetric key cryptography and is a widely used mechanism in any substitution-permutation network as a source to produce nonlinearity [2, 3]. Due to indispensable involvement of the S-box, many algorithms have been presented for the construction of safer and more reliable S-boxes [2, 4–6]. In addition, applications of S-boxes in digital image encryption, steganography and watermarking have become quite popular and influential in recent years [7–9].

Zhang et al. [10] studied the S-box-only encryption algorithm and proved that S-box-only cipher is cryptographically vulnerable. Keeping this fact in view, we propose an image encryption algorithm that utilizes the composition of a particular S-box along with the scrambling effect of the Arnold transform. The algorithm used for S-box is associated with the structural properties of the Galois field. The design algorithm uses the iterative applications of exponent of the primitive element of the Galois field.

In recent literature, chaos has been extensively used in construction of stronger S-boxes [8, 10–13], because of its most dominating feature of sensitivity towards the initial conditions. Our proposed strategy is also highly sensitive to the choice of the initial conditions but in our case, we reach the same performance efficiency results by applying a comparatively simple and direct method that utilizes some prime properties of the Galois field structure. We determine the cryptographic significance of this S-box by several dominating performance indices used in literature such as bit independence, strict avalanche, nonlinearity, linear and differential approximation probability tests. We compare the performance of this S-box with some prevailing algorithms also. It is however true that even depicting outstanding performance indices, the S-box-only image encryption is not efficient. We in this paper present an image encryption algorithm using the application of a highly efficient substitution followed by 10 iterations of the Arnold transform. To the best of our knowledge, the presented idea is novel and not been discussed in the existing literature. The results obtained by this strategy are tested through highly significant measures used for this purpose and we conclude that the anticipated technique is potentially strong and can be reliably used for further encryption applications.

The material distribution is as follows. Section 2 deals with the properties of the used Galois field and their application in the construction of a substitution box. In Sect. 3 we discuss and compare the cryptographic significance of the newly synthesized S-box. The basic concepts regarding the Arnold transform are presented in Sect. 4. Section 5 presents the detailed algorithm used for the image encryption. In Sect. 6 we test the strength of the proposed scheme using statistical analyses and lastly Sect. 7 presents the conclusion.

2 Algorithm for S-box

The intent of this section is to presents the design principle of our S-box. In this regard, we prefer to give a view of some fundamental facts.

Galois field $GF(p^n)$: where p is a prime number, is expressed as a factor ring $\mathbb{F}_p[X]/(f(x))$ where $f(x) \in \mathbb{F}_p[X]$ is a degree n irreducible polynomial. For $GF(2^8)$ we choose a degree - 8 irreducible polynomial $f(x) = x^8 + x^6 + x^5 + x^4 + 1 \in \mathbb{F}_2[X]$. We know that the multiplicative group G of the resultant field $GF(2^8)$ is cyclic and hence each nonzero element of the field can be expressed as a power of the generator $g = 00000010$.

Now we state the construction process for the S-box where an 8×8 S-box is a vectorial Boolean function $S : GF(2^8) \rightarrow GF(2^8)$.

In the proposed construction we use a specific nonlinear, iterative map ϕ defined on the $GF(2^8)$, given below:

$$\phi(x_j) : \begin{cases} g^{\phi(x_{j-1})} & : \ 1 \leq j \leq 254, \ j \neq 230, \ 234, \\ g^{\phi(x_{j-1})+12} & : \ j = 230, \\ g^{\phi(x_{j-1})+18} & : \ j = 234, \\ 0 & : \ j = 255. \end{cases} \tag{1}$$

The above expression shows that the outputs of this map depend upon the chosen initial condition. This sensitivity towards the change of initial conditions makes this map compatible with the chaotic maps, however, it is clear that this map is quite straightforward and easy with the implementation and

computation view point. In our calculations, we set the initial condition $\phi(x_0) = 1$. For the convenience, every element of the multiplicative cyclic group G of the associated Galois field is expressed in terms of exponents of the generator g in Table 1. Some calculations are explained below, which lead to the corresponding S-box elements (Table 2).

$$\phi(x_0) = 1 \quad \text{(the initial condition)},$$
$$\phi(x_1) = g^{\phi(x_0)} = g = 2,$$
$$\phi(x_2) = g^{\phi(x_1)} = g^2 = 4,$$
$$\phi(x_3) = g^{\phi(x_2)} = g^4 = 16,$$
$$\phi(x_4) = g^{\phi(x_3)} = g^{16} = 243.$$

It is an extremely desirable feature of an S-box to be invertible so that the process could be reverted accordingly. For invertibility property, the involved Boolean function is required to be bijective. It is evident from the expression of ϕ that our map is bijective and hence the S-box in invertible. The inverse S-box is shown in Table 3, which is extracted from Table 2. The values in Table 2 give the outputs $\phi(x) = y$, where $0 \le x \le 255$. Clearly, $\phi^{-1}(\phi(x)) = \phi^{-1}(y) = x$ shows that in the inverse S-box, the value at *yth* position should be x. Following this rule the inverse S-box values are obtained (Table 3).

Our next goal is to analyse the cryptographic performance of the new S-box. In the following section we discuss some well-known analysis techniques to figure out the strength of our S-box.

3 Performance Analysis of S-box

In this section, we analyze the newly synthesized S-box through some widely accepted parameters including nonlinearity, bit independence, strict avalanche, linear and differential approximation probabilities. We compare the results with the prevailing S-boxes i.e., AES S-box, Affine Power Affine (APA) S-box, Gray S-box, Skipjack S-box, Xyi S-box and Residue Prime S-box.

3.1 Nonlinearity

The nonlinearity measure [6] determines the smallest distance of the reference function from all the affine functions.

The numerical values are presented in Table 4, showing an average nonlinearity value 103.5. A comparison of the nonlinearity results with other S-boxes is shown in Table 6 and Fig. 1. Clearly, the nonlinearity of the proposed S-box lies in a highly acceptable range.

Generally chaos-based algorithms are employed to increase the complexity and nonlinearity of the S-box. In order to prove the forte of the newly synthesized S-box, we compare its nonlinearity with some chaos-based S-boxes as well to show the effectiveness of our model (see Table 5).

3.2 Strict Avalanche Criterion

According to SAC, a function $S : GF(2^n) \rightarrow GF(2^n)$ would be regarded as reliable if the probability of change in output-bits is 1 / 2 for a single input-bit change. The results are presented in Table 4, showing that our S-box fulfils the requirements of SAC. Table 6 and Fig. 2 compare these results with other S-boxes.

3.3 Linear and Differential Approximation Probabilities

Linear approximation probability is a measure that calculates the unevenness of an event. It is mathematically defined by:

$$LP = \max_{\Gamma_x, \Gamma_y \neq 0} \left| \frac{\#\{x | x.\Gamma_x = S(x).\Gamma_y\}}{2^n} - \frac{1}{2} \right|,$$

where x represents all possible inputs to the S-box and Γ_x and Γ_y give the parity of the input and output bits respectively.

The differential uniformity demonstrated by an S-box is determined through the differential approximation probability test [2]. The mathematical differential approximation probability is:

$$DP = \left[\frac{\#\{x \in X | S(x) \oplus S(x \oplus \Delta x) = \Delta y\}}{2^n} \right],$$

where Δx and Δy represent the input and output differentials respectively. The results of both LP and DP and their comparisons are given in Tables 4, 6 and Figs. 3, 4. It is evident that in the LP measure, our S-box is better than the Xyi S-box and is pretty similar to the Residue Prime S-box. However for differential approximation probability it is much better than the

Table 1 Exponential representation and the elements of G

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

Table 1 continued

$x \in G$	g^n	$x \in G$	g^n	$x \in G$	g^n	$x \in G$	g^n	$x \in G$	g^n
44	g^{156}	95	g^{18}	146	g^{110}	197	g^{171}	248	g^{149}
45	g^{242}	96	g^{236}	147	g^{239}	198	g^{99}	249	g^{216}
46	g^{252}	97	g^{163}	148	g^{115}	199	g^{86}	250	g^{198}
47	g^{32}	98	g^{214}	149	g^{127}	200	g^{248}	251	g^{172}
48	g^{235}	99	g^{98}	150	g^{204}	201	g^{143}	252	g^{96}
49	g^{213}	100	g^{247}	151	g^{17}	202	g^{56}	253	g^{100}
50	g^{246}	101	g^{55}	152	g^{69}	203	g^{180}	254	g^{175}
51	g^{135}	102	g^{136}	153	g^{194}	204	g^{137}	255	g^{87}

Table 2 S-box

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

Residue Prime S-box and pretty close to the Skipjack and Xyi S-boxes.

3.4 Bit Independence Criterion

The independent behavior of the pair of variables and the changes in input bits are considered as important factors of bit independence criterion [17]. According to this criterion, input bits are transformed exclusively, and then output bits are scrutinized for their independence. Bit independence is one of the most desirable properties in any cryptographic structure. The increasing independence between bits is of great worth to attain a high level of complexity and perplexity in a system.

The results of BIC are given in Table 4 and are compared in Table 6 and Fig. 5. It is evident that, in BIC, our S-box has similarity with the Xyi S-box. By analyzing the results presented in Table 4, it is quite clear that the proposed algebraic substitution box has upended cryptographic features and can be usefully implemented in encryption applications. Table 6 witnesses that when compared with AES, APA, Gray, Skipjack, Xyi and Residue prime S-boxes, our new S-box is wisely alike the formerly prevailing S-boxes.

4 Arnold Transform

Arnold transform is used for encryption of digital images to increase the spread of pixel intensities [18–20]. For any square image of size $M \times M$, encryption using the Arnold transform can be given as:

Table 3 The inverse S-box

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

Table 4 Performance Indices for S-box

Analysis	Max.	Min.	Average	Square deviation	DP	LP
Nonlinearity	106	99	**103.5**			
SAC	0.609375	0.421875	**0.506592**	0.0222178		
LP	162					**0.132813**
DP					**0.046875**	
BIC		99	**103.357**	2.14643		

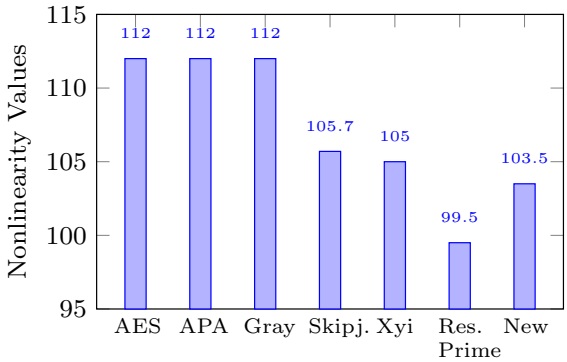


Fig. 1 Nonlinearity comparison

Table 5 Nonlinearity comparison with chaotic models

	Nonlinearity		
S-box	Max.	Min.	Avg.
Proposed	106	99	103.5
Chaotic [14]	106	98	103
Chaotic [15]	104	100	103.3
Chaotic [16]	108	98	103

$$\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \vartheta & \vartheta \\ \vartheta & \tau \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (modM), \tag{2}$$

where (x, y) and (α, β) are associated pixel coordinates of the input image and encrypted data, such that $(\vartheta, \tau) = (1, 2)$, as shown in Fig. 6.

The Arnold transform encryption is worked on periodic boundary treatment. The n number of iterations for encrypting the image may be written as:

$$I(\alpha, \beta)^k = \Lambda(x, y)^{k-1} (modM),$$

where Λ is the Arnold transform matrix given in (2) and I is an $M \times M$ encrypted image data for k number of iterations: $k = 1, 2, \ldots, n$, such that

Table 6 Performance comparison of different S-boxes

S-box	Nonlinearity	SAC	BIC	DP	LP
New	**103.5**	**0.506592**	**103.357**	**0.046875**	**0.132813**
AES	112	0.5058	112.0	0.0156	0.062
APA	112	0.4987	112.0	0.0156	0.062
Gray	112	0.5058	112.0	0.0156	0.062
Skipjack	105.7	0.4980	104.1	0.0468	0.109
Xyi	105	0.5048	103.7	0.0468	0.156
Residue prime	99.5	0.5012	101.7	0.2810	0.132

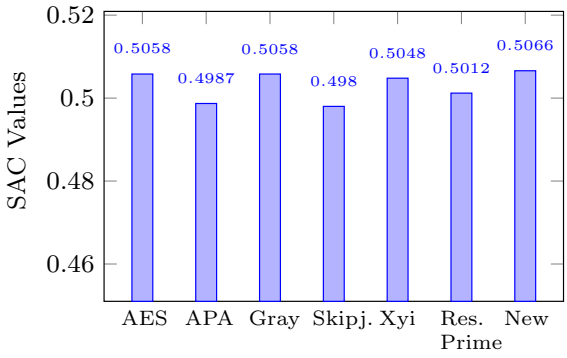


Fig. 2 SAC comparison

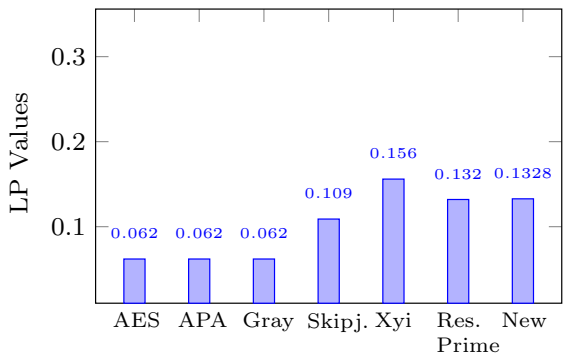


Fig. 3 LP comparison

$I(\alpha,\beta)^0 = I(x,y)$. Periodicity of encryption is dependent on the size of a given image. The encrypted image data can be reversed on application of the inverse Arnold transform to the I with same iterations k as follows:

$$I(x,y)^k = I\Lambda^{-1}(\alpha,\beta)^{k-1}(modM).$$

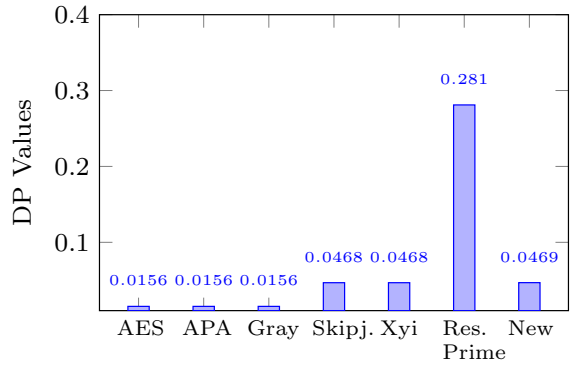


Fig. 4 DP comparison

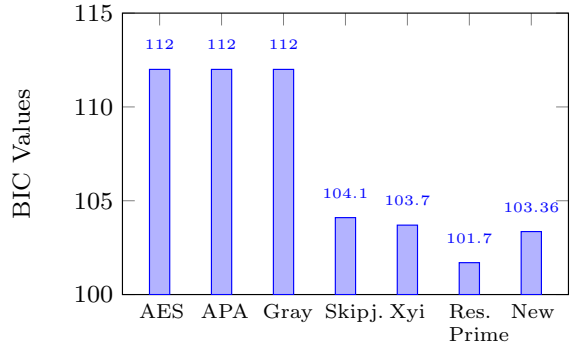


Fig. 5 BIC comparison

5 Image Encryption Scheme

Now we present the scheme used for the image encryption. It comprises of the following two steps.

- Use substitution box to partially encrypt the plain image.
- Apply 10 iterations of the Arnold transform on this partially encrypted image to obtain the fully encrypted image.

Algorithm 1 A novel image encryption

Input: Plain image $I(x, y)$
1: Initialize $\phi(x_0) = 1$.
2: **for** all $i = 0, 1, 2, ..., 255$ **do**
3: $\phi(x_i) = g^{\phi(x_{i-1})}$ using Eq.(1)
4: **for** each pixel $k = 1 : 10$ obtained from ϕ **do**
5: $I(\alpha, \beta)^k = \Lambda\phi(x, y)^{k-1}(modM)$ using Eq.(2)
6: **end for**
7: **end for**
Output: Encrypted image $I(\alpha, \beta)$ is obtained.

5.1 Encryption Algorithm

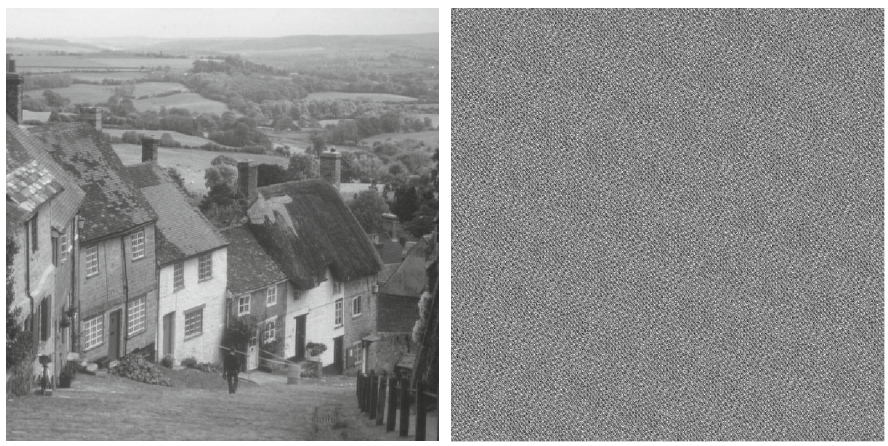
We selected three 512×512 benchmark images of hill, peppers and Barbara respectively. By following the above stated scheme the images are encrypted. We obtain the decrypted images by applying the inverse Arnold transform and inverse S-box respectively. Figures 7, 8, 9 and 10 show the plain images, the S-box-only encrypted images, the fully encrypted images and the decrypted images respectively. One can observe that the visual results of S-box-only encryption are not completely unintelligible however the combined effect of the S-box and Arnold transform is much better. We further examine the proposed encryption strategy through some statistical analysis.

6 Statistical Analysis of the Proposed Method

The statistical analysis of the proposed method includes the most significant measures such as entropy, contrast, correlation, homogeneity, number of pixels change rate and unified average change intensity. We discuss these security parameters one by one and present the numerical results also.

6.1 Histogram Analysis

Histogram is a graphical representation of image-pixels distribution at each intensity level. A good encryption technique requires significant difference in the histogram of the plain and encrypted image so that the original content could not be extracted. Figures 11, 12, 13 show the respective histograms of plain, encrypted and the decrypted images. The histograms of the encrypted images, though not very uniformly distributed, but are evidently better than those, obtained by applying the encryption schemes proposed in [21, 22] and are pretty alike to [8]. The visual results obtained for histograms prove that the proposed method is stable against the histogram based attacks.



(a) **(b)**

Fig. 6 Effect of 10 iterations of Arnold transform. (**a**) (Plain image (*Hill*). (**b**) Arnold encryption

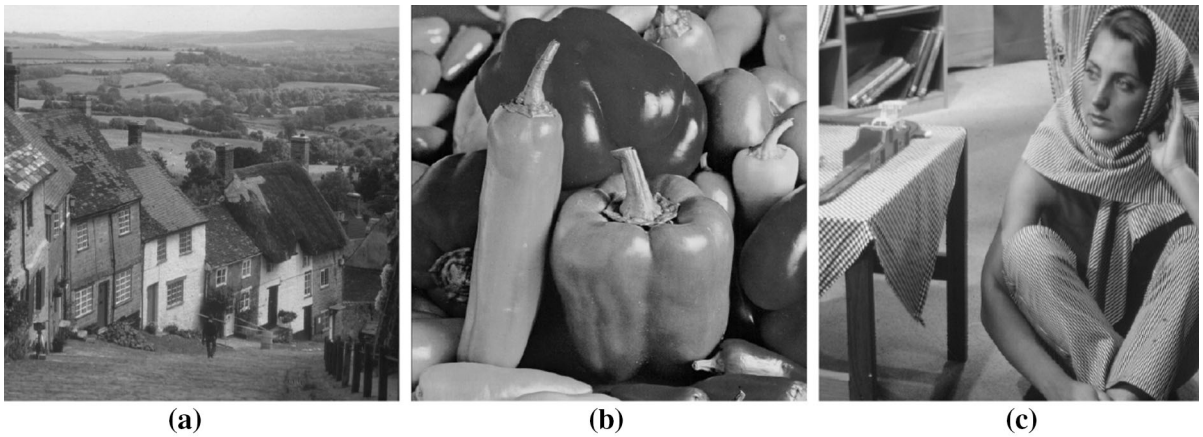


Fig. 7 Plain Images: (**a**) Hill, (**b**) Peppers and (**c**) Barbara

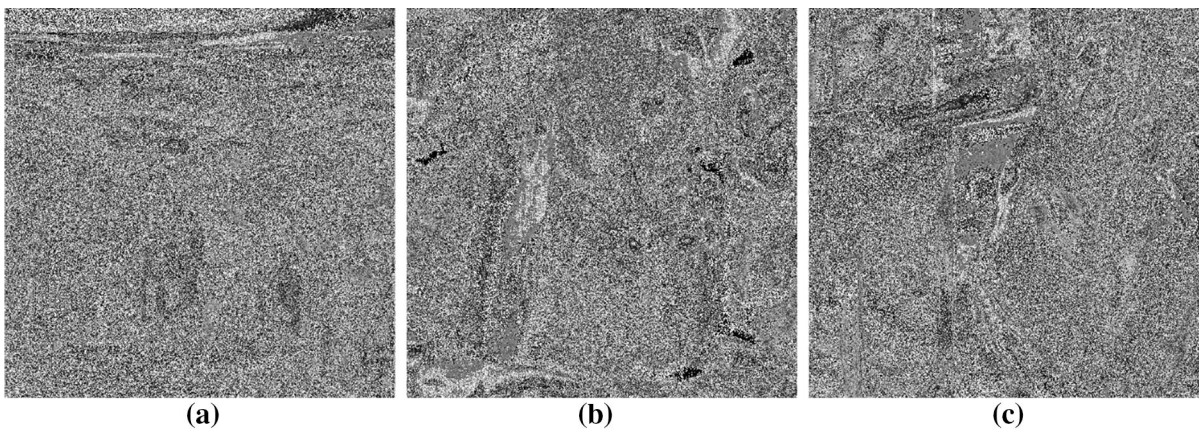


Fig. 8 S-box encryption: (**a**) Hill, (**b**) Peppers and (**c**) Barbara

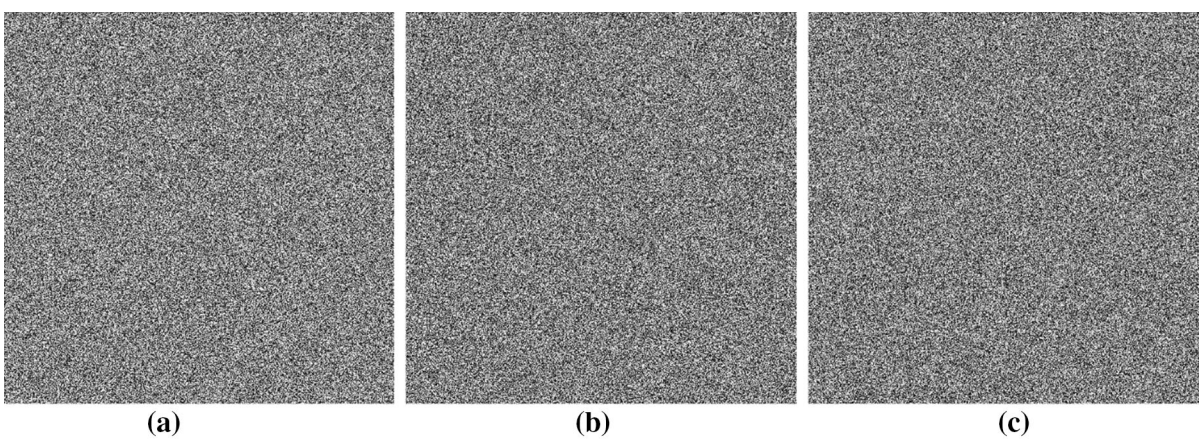


Fig. 9 Full encryption: (**a**) Hill, (**b**) Peppers and (**c**) Barbara

Fig. 10 Full decryption: (**a**) Hill, (**b**) Peppers and (**c**) Barbara

6.2 Deviation from Uniform Histogram

An ideal encryption algorithm produces uniform histogram distribution. In order to determine the encryption quality of the proposed scheme we examine the deviation from the uniform histogram. The smaller the deviation, the better is encryption algorithm. The mathematical expression for the ideally uniform histogram is given by:

$$H(C_i) : \begin{cases} \dfrac{M \times N}{256} & : \ 0 \le C_i \le 255 \\ 0 & : \ \text{elsewhere} \end{cases} \tag{3}$$

The deviation from the ideality can be expressed as:

$$D = \frac{\sum_{C_i=0}^{255} |H_{C_i} - H_C|}{M \times N},$$

where H_C represents the histogram of the encrypted image, H_{C_i} is the uniform histogram and $M \times N$ represents the image size. We calculate the deviation values for 512×512 images of hill, peppers and Barbara and the results are shown below in Table 7. It is quite clear that our scheme is in a good comparison with the scheme of [8], however, it is much better than [21].

6.3 Information Entropy

Entropy analysis measures the randomness of system. The information entropy is given by,

$$H(M) = \sum P(m_i) \log_2 \frac{1}{\mathrm{P(m_i)}};$$

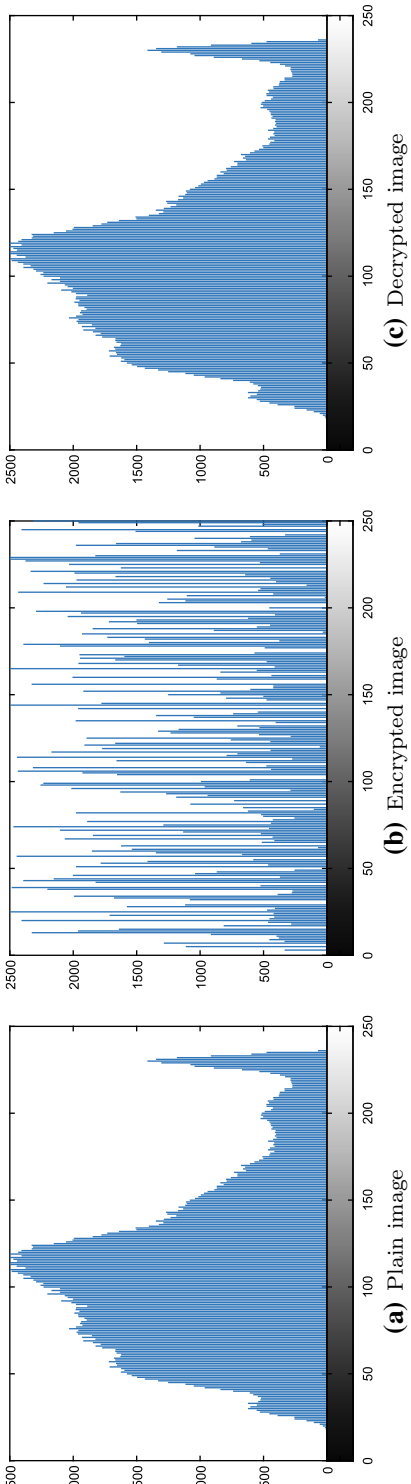
where $M = m_i$ represents the values of discrete random variable and $P(m_i)$ is the probability at m_i. For an image with 256 gray levels, the ideal value of entropy measure is 8 and a strong cryptosystem attains entropy close to the ideal value in order to resist the entropy attacks. It has been established that the true randomness could be captured by using *local entropy* [23, 24]. In this regard, we select some randomly chosen, non-overlapping blocks of the encrypted images, calculate the average of the entropy measures of these blocks. For the proposed method, the numerical results for both the local and global entropy of images of hill, peppers and Barbara are shown in Table 8.

6.4 Contrast

Contrast is a measure used to identify objects in an image. A strong encryption technique produces high level of contrast. Table 9 shows that our encryption scheme fulfills this criterion and the results obtained by the combined effect of S-box and Arnold transform are comparatively better than the individual effect of the S-box or the Arnold transform only. One can see that the proposed scheme offers a high level of contrast when compared with [25].

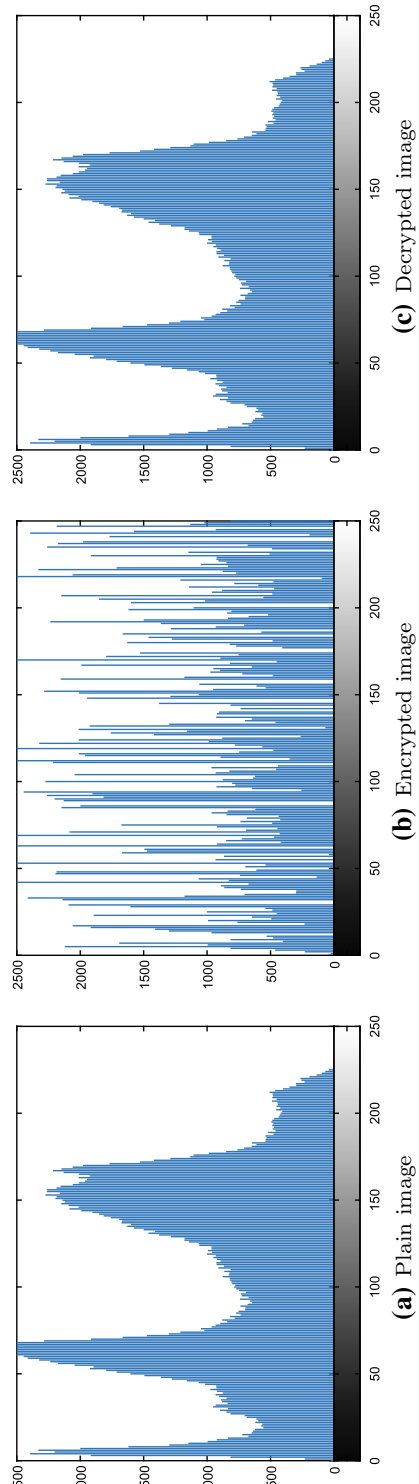
6.5 Correlation

In order to examine the encryption effect of the proposed method we perform correlation analysis on both the plain and the encrypted images. It is quite clear that for an efficient encryption, the correlation



(a) Plain image **(b)** Encrypted image **(c)** Decrypted image

Fig. 11 Histogram of Hill's plain, encrypted and decrypted images



(a) Plain image **(b)** Encrypted image **(c)** Decrypted image

Fig. 12 Histogram of Peppers' plain, encrypted and decrypted images

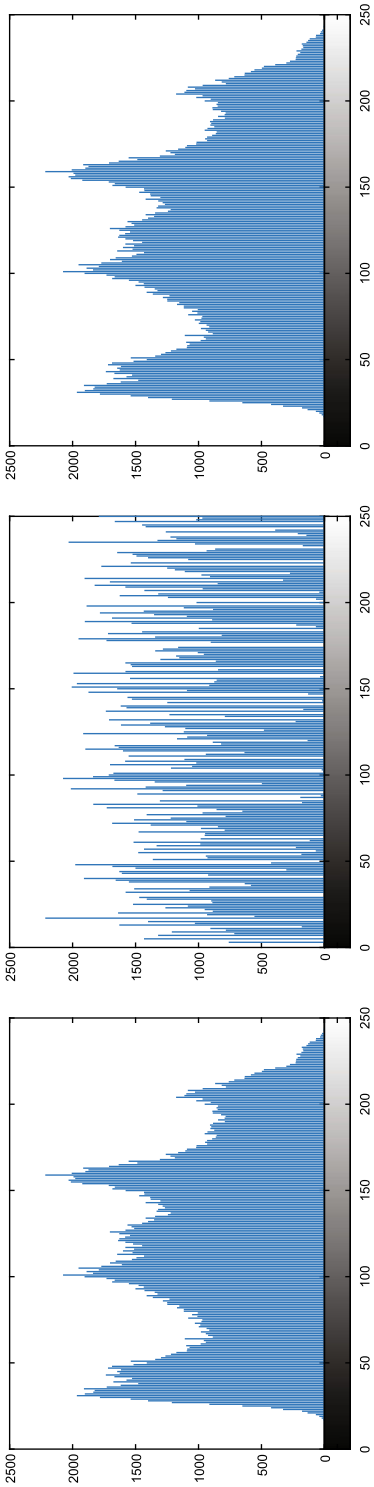


Fig. 13 Histogram of Barbara's plain, encrypted and decrypted images

Table 7 Deviation from uniform histogram

	Deviation from uniform histogram		
Images	Proposed	Ref.[8]	Ref.[21]
Hill	0.9147	0.2179	27
Peppers	0.9961	0.1998	34
Barbara	0.8954	0.1718	23

Table 8 Entropy analysis

	Entropy		
Images	Local	Global	Ref.[25]
Hill	7.4651	7.4802	7.6528
Peppers	7.5728	7.5714	7.7317
Barbara	7.6105	7.6321	7.7539

Table 9 Contrast analysis

	Contrast			
Images	S-box	Arnold	Comb.	Ref. [25]
Hill	10.0101	5.7534	10.3795	8.7905
Peppers	9.7141	6.3182	10.2218	8.5381
Barbara	9.5166	5.7368	9.9306	8.1451

Table 10 Correlation analysis

	Correlation			
Images	S-box	Arnold	Comb.	Ref.[25]
Hill	0.0360	−0.1305	0.0002	0.0105
Peppers	0.0498	0.0183	0.0003	0.0114
Barbara	0.0403	0.0378	−0.0013	0.0101

between the adjacent pixels of the encrypted image should be reduced as compared to the plain image. The coefficient is given by,

$$r_{xy} = \frac{E((x-\mu_x)(y-\mu_y))}{\sqrt{\delta_x \delta_y}},$$

where μ and δ represent the expected value and variance. The value of correlation coefficient close to zero guarantees better encryption quality. The analysis is performed on three images, hill, peppers and Barbara. The results arranged in Table 10 witness

the effectiveness of the proposed method in comparison with [25].

6.6 Homogeneity

Gray level co-occurrence matrix (GLCM) depicts the ability of combinations of pixel brightness results in tabular form. The closeness of the distribution in the (GLCM) to its diagonal is measured through the homogeneity analysis. The smaller is the homogeneity measure, the better is encryption. The numerical results shown in Table 11 go in favor of the proposed strategy.

6.7 Differential Analysis

A desirable feature of a cryptosystem is to show high sensitivity to single-bit change in the plain image. For this purpose two measures, NPCR and UACI, are commonly used. NPCR stands for the number of pixels change rate of encrypted image as a result of one pixel change in the plain image. NPCR can be defined as the variance rate of pixels in the encrypted image that occurs through the change of a single pixel in original image. However UACI means unified average intensity of differences between the plain and encrypted images. The percentage values for both these measures are given by the following formulae.

$$NPCR = \frac{\sum_{i,j} D_{ij}}{W \times H} \times 100, \tag{4}$$

$$UACI = \frac{1}{W \times H}\left[\frac{\sum_{i,j} C_{ij} - \acute{C}_{ij}}{255}\right] \times 100. \tag{5}$$

In above C and $\acute{C}$ represent the encrypted images obtained as a result of single bit change in the original image. In Eqs. (4) and (5), W and H represent the width and the height of the images C and $\acute{C}$.

An efficient encryption scheme is one that produces higher values of both NPCR and UACI. The results obtained in our case are shown in Tables 12 and 13 respectively which prove that our technique is quite efficient as compared to some recent methods.

6.8 Time Analysis

The time complexity of the proposed algorithm depends linearly on the size of the input image. The action per pixel is proportional to $N^2 \times M^2 + S_b + I_A$, where N and M are length and width of the given image, S_b represent the size o S-box, and I_A shows the iteration number of the Arnold transform, respectively.

The major focus of the proposed framework is the complexity of an encryption process. The computational speed of the proposed method is also reasonable. Although our scheme takes more time than [12] and [8] but offers increased security. The results presented in Table 14 show that the proposed algorithm is much faster than some recently presented chaos-based encryption techniques [21, 26], (see Table 2 of [8]). The computational cost results are obtained on three

Table 11 Homogeneity analysis

	Homogeneity			
Images	S-box	Arnold	Comb.	Ref. [25]
Hill	0.4233	0.4599	0.3915	0.4217
Peppers	0.4329	0.4317	0.3918	0.4365
Barbara	0.4285	0.4465	0.3944	0.4209

Table 12 NPCR comparison

	NPCR				
Images	S-box	Arnold	Comb.	Ref.[12]	Ref.[8]
Hill	1	0.9936	0.9960	0.9959	0.9899
Peppers	1	0.9943	0.9959	0.9960	0.9918
Barbara	1	0.9946	0.9959	0.9957	0.9941

Table 13 UACI comparison

	UACI				
Images	S-box	Arnold	Comb.	Ref.[12]	Ref.[8]
Hill	0.2990	0.2629	0.3313	0.3352	0.3311
Peppers	0.3120	0.2884	0.3384	0.3356	0.3326
Barbara	0.3072	0.2858	0.3320	0.3351	0.3297

Table 14 Computational cost comparison (in seconds)

Test images	Proposed	Ref.[21]	Ref.[26]
Hill	10.56	11.42	34.62
Peppers	10.81	12.13	35.11
Barbara	10.47	11.45	34.81

different gray test images of size 512×512. The listed methods implementation are performed on processor: Intel(R) Core(TM) i5-2520M CPU @ 2.5, RAM: 8.00 GB; the run times of each method are obtained using Matlab 2015a.

7 Conclusion

In this work we propose an image encryption scheme that is extremely simple and highly effective. It has been established in some recent research work that the S-box-only encryption techniques are not secured enough for confidential communications therefore we introduce the combination of the S-box with certain number of iterations of the Arnold transform. The strength of the proposed method is then analyzed through several metric measurements. Moreover, the proposed method test evaluation for confusion creating capability is self-evident in terms of visual randomness and better values as compared to some recently presented algorithms.

References

1. Shannon, C. E. (1949). Communication theory of secrecy systems. *Bell Systems Technical Journal*, *28*, 656–715.
2. Biham, E., & Shamir, A. (1991). Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, *4*(1), 3–72.
3. Matsui, M. (1998). Linear cryptanalysis method for DES cipher. *Proceedings of EUROCRYPT'93* (pp. 386–397). Berlin: Springer.
4. Kim, J., & Phan, R. C. W. (2009). Advanced differential-style crypt-analysis of the NSA's skipjack block cipher. *Cryptologia*, *33*(3), 246–270.
5. Hussain, I., Shah, T., Gondal, M. A., Khan, W. A., & Mahmood, H. (2013). A group theoretic approach to construct cryptographically strong substitution boxes. *Neural Computing and Applications*, *23*(1), 97–104.
6. Farwa, S., Shah, T., & Idrees, L. (2016). A highly nonlinear S-box based on a fractional linear transformation. *SpringerPlus*, *5*, 1658.
7. Xu, Z. H., Shen, G., & Lin, S. (2011). Image encryption algorithm based on chaos and S-boxes scrambling. *Advance Materials Research*, *171172*, 299304.
8. Rehman, A. U., Khan, J. S., & Ahmad, J. (2016). A New Image Encryption Scheme Based on Dynamic S-Boxes and Chaotic Maps. *3D Research*, *7*, 7.
9. Jamal, S. S., Khan, M. U., & Shah, T. (2016). A watermarking technique with chaotic fractional S-box transformation. *Wireless Personal Communications*, *90*(4), 2033–2049.
10. Zhang, Y., & Xiao, D. (2013). Cryptanalysis of S-box-only chaotic image ciphers against chosen plaintext attack. *Nonlinear Dynamics*, *72*(4), 751756.
11. Ahmad, M., Chugh, H., & Goel, A. (2013). A chaos based method for efficient cryptographic S-box design. *International Symposium on Security in Computing and Communications.*, *377*, 130–137.
12. Ahmad, J., & Hwang, S. O. (2016). A secure image encryption scheme based on chaotic maps and affine transformation. *Multimedia Tools and Applications*, *75*(21), 13951–13976.
13. Ahmad, J., Hwang, S. O., & Ali, A. (2015). An experimental comparison of chaotic and non-chaotic image encryption schemes. *Wireless Personal Communications*, *84*(2), 118.
14. Gondal, M. A., Raheem, A., & Hussain, I. A. (2014). Scheme for obtaining secure S-boxes based on chaotic Bakers map. *3D Research*, *5*, 17.
15. Ozkayanak, F., & Ozer, A. B. (2010). A method for designing stron S-boxes based on chaotic Lorenz system. *Physics Letters A*, *374*(36), 3733–3738.
16. Khan, M., Shah, T., Mahmood, H., & Gondal, M. A. (2013). An efficient method for the construction of block cipher with multi-chaotic systems. *Nonlinear Dynamics*, *71*(3), 489–492.
17. Webster, A. F., & Tavares, S. E. (1986). *Proceedings of CRYPTO'85*., On the design of s-boxes, advances in cryptology Berlin: Springer.
18. Muhammad, N., Bibi, N., & Kim, D. G. (2013). A fresnelet-based encryption of medical images using Arnold transform. *International Journal of Advanced Computer Science and Applications*, *A 1*(1), 131140.
19. Liu, Z., Xu, L., Liu, T., Chen, H., Li, P., Lin, C., et al. (2011). Color image encryption by using Arnold transform and color-blend operation in discrete cosine transform domains. *Optics Communications*, *284*, 123–128.
20. Liu, Z., Chen, H., Liu, T., Li, P., Xu, L., Dai, J., et al. (2011). Image encryption by using gyrator transform and Arnold transfom. *Journal of Electronic Imaging*, *20*(1), 013020.
21. Anees, A., Siddiqui, A. M., & Ahmed, F. (2014). Chaotic substitution for highly autocorrelated data in encryption algorithm. *Communications in Nonlinear Science and Numerical Simulation*, *19*(9), 31063118.
22. Wang, D., & Zhang, Y. B. (2009). Image encryption algorithm based on S-box sustitution and chaose random sequence, In: International Conference on Computer aided Modeling and Simulation. (pp. 110–113) Guangzhou, China.
23. Ravichandran, D., Praveenkumar, P., Rayappan, J. B. B., & Amirtharajan, R. (2016). Chaos based crossover and mutation for securing. *DICOM Image*, *72*, 170–184.
24. Wu, Y., Zhou, Y., Saveriades, G., Agaian, S., Noonan, J. P., & Natarajan, P. (2013). Local Shannon entropy measure with statistical tests for image randomness. *Information Sciences*, *222*, 323–342.
25. Hussain, I., Azam, N., & Shah, T. (2014). Stego optical encryption based on chaotic S-box transformation. *Optics and Laser Technology*, *61*, 50–56.
26. Wang, Y., Wong, K. W., Liao, X., & Chen, G. (2011). A new chaos-based fast image encryption algorithm. *Applied Soft Computing*, *11*(1), 514522.