WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Color Image Encryption Through Linear Diophantine Equations

Saria Jahangir[1], Dania Saleem Malik[2]

[1,2]Department of Mathematics, Quaid-i-Azam University, Islamabad, Pakistan
[2]Department of Mathematics, HITEC University, Taxila, Pakistan
[1]saira156@gmail.com, [2]dania.saleem@hitecuni.edu.pk

ABSTRACT

In this new idea, we have anticipated an encryption technique to encrypt any kind of digital information. For this substitution-permutation created system, the polynomial based Linear Diophantine Equations is used for the substitution process. The substitution box is constructed by obtaining the infinite solutions of Linear Diophantine equation in two variables and then projected them to the Galois field. The proposed Substitution boxes have been characterized by some standard algebraic, statistical and texture analyses. A comparison of the anticipated and existing substitution boxes reveals that proposed boxes are comparatively better and can be used in well-known ciphers. One of the aims of this work is to suggest an encryption technique for RGB image based on permutation keys and triplet of newly generated S-boxes. The outcomes of security, statistical and differential analyses have approved that the foreseen scheme is remarkable for image encryption.

Key words: Linear Diophantine Equation; S-box; RGB image Encryption

1. Introduction

For last two decades, digital data has been exchanged enormously from one place to another due to development and advances in computer networking. During the communication of this data, one of the leading concerns is to avoid any kind of manipulation, unauthenticated form, repudiation and disintegration. Images are extensively used in numerous progressions. Hence, the fortification of image data from unlicensed entree is imperative. Image encryption and steganography play a substantial part in the field of information hiding. Swift development of network multimedia systems has been seen in recent years. This has led to cumulative alertness of how easy it is becoming to duplicate the data. The comfort with which flawless duplicates can be made may lead to large-scale unlicensed copying, which is a great alarm to the image, music, film, and book. Because of this unease over copyright concerns, a number of technologies are being developed to guard against illegitimate replication. There has been exponential development in the advancement of those frameworks which guarantee the security of this confidential information, alongside the private key. There are various encryption techniques accessible today. The elements that will figure out which one is the most proper include: the degree of security; the cost; the execution speed and execution issues. In this way, encryption algorithms adjust the information entropy by making new words or straightening out the probabilities of the current words for the situation the entire letter set is as of now utilized. These days, information encryption dependent on chaotic frameworks is valuable for advanced media encryption while showing the necessary upgraded sensitivity to initial conditions and framework parameters(sensitivity of the encryption key). While scrambling is significant, the encryption algorithms should meet some of the of the particular multimedia encryption prerequisites, for example the real-time constraint and high robustness against a wide range of known attacks. An opportunity to "break" or decrypt an algorithm by the attack is additionally a significant factor that must be thought about. The fundamental rule in the current symmetric ciphers comprises of rearranging the places of the image pixels and from that point diffusing the connection between the first and ciphered images. In any case, the distinction between these algorithms resides in the strategy utilized for the generation of the permutation and diffusion keys. On account of the chaotic stream ciphers, the confusion and diffusion forms are progressively refreshed as the dynamical framework is iterated. The generation of the permutation key in such a cipher is computationally of minimal effort and the confusion-diffusion step ought to be rehashed so as to achieve a more significant level of security. Despite the fact that chaos based encryption gives off an impression of being a promising innovation today, the long computational time required for the generation of the permutation and diffusion keys remains its principle confinement and henceforth of more extensive its selection. Performing at a similar high security level and quick encoding is then the genuine challenge in chaotic ciphering.

1.1 Related work

Currently, a common constituent which is used for attaining misperception in encrypted data is S-box, and it is the only nonlinear segment of a block cipher. Thus, the excellence of block cipher depends on S-box. Due to this cause, many researchers have shown their attention to design different and powerful S-boxes. Because of their strong cryptographic characteristics, S-boxes that are created on algebraic techniques have much consideration and which are robust to linear and differential cryptanalyses. So, a secure communication based on different types of S-boxes was designed, for instance in

AES, the affine power affine (APA) S-box is recommended to increase the algebraic complexity while keeping the anticipated encryption properties available in the new S-box [1]. By the action of symmetric group S_8 on the original S-box of AES, the S_8 AES S-boxes are proposed [2]. On applying additional transform based on binary Gray codes on the original S-box of AES, the Gray S-box is introduced [3]. The Gray S-box has a 255-term polynomial as compared to 9-term polynomial, which inherits almost all the properties and increases the security for AES. Consequently, it maintained the nonlinearity and algebraic complexity. Similarly, Xyi S-box, Residue Prime S-box and Skipjack S-box are commonly used S-boxes in the encryption and decryption methods [4, 5]. Whereas some of the authors keep the characteristics of these S-boxes as standard to determine the strength of newly constructed S-boxes by means of the criteria included Nonlinearity, strict avalanche criterion (SAC), bit independence criterion (BIC), linear approximation probability method (LP) and Differential approximation probability (DP) [6, 7].

The most S-boxes construction techniques in this regards are the composition of an inversion and bijection maps on the Galois field $GF(2^8)$. Other than it the most famous scheme of S-box construction is linear fractional transformations on Galois field $GF(2^8)$. So, for the fixed values of $a, b, c,$ and d of the Galois field $GF(2^8)$, the fractional transformation $x \longmapsto \frac{ax+b}{cx+d}$ design 8×8 S-boxes. In this new idea, we have anticipated an encryption technique to encrypt any kind of digital information. For this substitution-permutation created system, the polynomial based Linear Diophantine Equations is used for the substitution process. The substitution box is constructed by obtaining the infinite solutions of Linear Diophantine equation in two variables and then projected them to the Galois field. The proposed Substitution boxes have been characterized by some standard algebraic, statistical and texture analyses. A comparison of the anticipated and existing substitution boxes reveals that proposed boxes are comparatively better and can be used in well-known ciphers. One of the aims of this work is to suggest an encryption technique for RGB image based on permutation keys and triplet of newly generated S-boxes.

Recently there were proposed some quick encryption plans in literature. In these algorithms, the permutation and diffusion are as normal two independent and iterative stages and the two of them require filtering the image so as to get the pixel values. Along these lines, during the encryption procedure, the image is filtered twice per round of the permutation-diffusion activity. In [8], a one round chaos-based image encryption scheme based on the quick generation of enormous permutation and diffusion keys is proposed. In this plan, at the permutation step, chaotic numbers were created utilizing a calculated guide to rearrange the pixel positions without changing its value and at diffusion step, rearranged image is part in n sub-images and the mix of PWLCM (piecewise linear chaotic map) with arrangements of LDE (linear Diophantine equation) are produced to veil the pixels in each sub-image. Keeping in view the rising demands of digital security mechanisms, we have devised a novel technique of image encryption based on the polynomial type linear Diophantine equations to enrich existing information hiding schemes that relies on the Galois field.

1.2 Motivations

With the fast productions and after the broad investigation on the S- box construction and image encryption systems, the inspirations of this work are the accompanying:

1. Numerous S-box building techniques are accessible in the literature however some of them may not be a suitable choice in some of the applications because of high computational unpredictability and capacity to not endure any channel noise.
2. The image encryption algorithms for the most part do not have the security analysis of different attacks to survey the nature of these algorithms. Specifically, the cryptanalysis is not considered properly.
3. One of the fundamental highlights for a modern image encryption algorithm or any advanced encryption algorithm is to be resilient against robustness attack (cropping). Which revealed that if the in the cipher image a block of information is cropped the decryption algorithm can properly decipher the tainted cipher image with some changes. In the event that the cipher data is ruined even somewhat, the fame ciphers do not will in general effectively decipher that spoiled cipher data.

1.3 Contributions of this work

In this manuscript, we build up an economical S-box construction technique and a scheme for image encryption using Linear Diophantine equations (LDE). The proposed work is validated through different analysis and attacks. The contributions of this manuscript are summarized as follows:

1. We proposed a novel S-box construction technique, further an efficient S-box should satisfy some specific cryptographic criteria; objectiveness, nonlinearity, outputs bit independence, strict avalanche and linear approximation probability. We have done these analyses for the proposed S-boxes in order to test their strength and give a comparison with other famous S-boxes.
2. We have proposed an image encryption scheme. The encryption algorithm comprises of two phases: permutation and masking of pixels of the whole image. Permutation is achieved by and permutation using three different keys obtained by the solution of LDE and masking process is performed by the proposed S-boxes.
3. To survey the adequacy of the foreseen image encryption algorithm, we have performed diverse analysis alongside linear and differential cryptanalysis. The consequences of these analyses are compared with the current encryption algorithms representing the great performance of our foreseen encryption algorithm.

4. We have performed a robustness analysis (Cropping) which revealed that if the cipher image is tainted by the channel noise or by an illegal user, the decryption algorithm can properly decipher the tainted cipher image with some changes. For this analysis an information blocks with size 128×128 and 128×256 is removed from the cipher-image, decrypted images still contain the greater part of the first visual data. This shows the great robustness of the proposed encryption algorithm against cropping attacks.

1.4 GAP between existing and proposed technique

In this study, we proposed a novel scheme to assemble the S-boxes based on the solutions of linear Diophantine equations (LDE's), that is $ax + by=c$, where a, b, c are integers such that $\gcd(a,b) \mid c$. Once LDE possesses a solution, then it has infinite solutions, so the solution set of a LDE can generate infinite S-boxes. Also, this construction is more economical and convenient therefore can efficiently replace S-boxes in all those ciphers in which S-boxes construction is not economical such as S-boxes mentioned above. Proposed S-boxes also a good choice to replace chaos-based S-boxes, as chaos is used because of its randomness, LDE also fulfill this requirement as it has the whole set of integers for its randomness. Newly generated S-Boxes are better options to be used in standard ciphers because of its high-performance indices.

This paper is organized in six sections. Some basics of Linear Diophantine Equations are given in section II. Section III explains the procedure of the construction of the proposed S-boxes. Section IV presents the performance indices of proposed S-boxes. Section V deals with the application of introduced S-boxes in image encryption. Analyses based on image encryption application are performed and their details are deliberated in section VI. Finally, the concluding remarks are given in section VII.

2. Linear Diophantine Equation

A Diophantine equation named after the ancient Greek mathematician, Diophantus. It is a polynomial equation whose solutions are restricted to integers. This infers that Diophantine equations become harder (or even impossible) to solve than the equations that do not have this restriction. The following is a well-known result from Number Theory.

Theorem 1 [9] "*Given integers a and b, not both of which are zero, there exist integers x and y such that*

$\gcd(x,y) = ax + by$*."*

A linear Diophantine equation (LDE) (in two variables) is an equation of the form

$$ax + by = c,$$

where a, b, c, x, y are integers, at least one of a, and b is non-zero. A solution of this equation is a pair of integers x_0, y_0 satisfying the equation is called a solution; that is, $ax_0 + by_0 = c$. The condition for solvability is; the linear Diophantine equation (LDE) has a solution if and only if the greatest common divisor of a and b divides c, i.e. $d \mid c$, where $d = \gcd(a,b)$. If d is $\gcd(a,b)$, then there are integers r and s such that $a = dr$ and $b = ds$. If a solution x_0 and y_0 of LDE exists, so the equation $ax_0 + by_0 = c$ implies

$$ax_0 + by_0 = (dr)x_0 + (ds)y_0$$

$$= d(rx_0 + sy_0) = c$$

which means that $d \mid c$. Conversely, suppose that $d \mid c$, then $c = dt$. Using Theorem 1, integers x_0 and y_0 can be found satisfying $d = ax + by$. By taking the product with t, we develop

$$dt = (ax_0 + by_0)t$$

$$= a(tx_0) + b(ty_0) = c$$

Therefore, $x = tx_0$ and $y = ty_0$ is the particular solution the Diophantine equation $ax + by = c$. This discussion deduces the following Theorem.

Theorem 2 [9] "*The linear Diophantine equation* $ax + by = c$ *has a solution if and only if* $d \mid c$*, where If* (x_0, y_0) *is any particular solution of this equation, then all other solutions are given by*

$$x = x_0 + \left(\frac{b}{d}\right)t, y = y_0 - \left(\frac{a}{d}\right)t,$$

where t is an arbitrary integer."

4. S-boxes Construction Technique

Step I Take an LDE, which admits the solution. Once an equation has a solution, then it has an infinite number of solutions. For instance, let $43x + 5y = 250$, applying Euclidian's algorithm to the evaluation of $\gcd(43,5)$, we can find that their gcd is 1. Since $1 \mid 250$, a solution to this equation exists. To obtain the integer 1 as a linear combination of 43 and 20, backward steps of the Euclidian's Algorithm follows

$$1 = (2)43 + (-17)5.$$

Upon multiplying this relation by 250, we arrive at

$$250 = (500)43 + (-4250)5$$

It follows that $x_o = 500, y_0 = -4250$ serves as one solution.

Step II All other solutions of LDE are of the form

$$x = x_0 + \left(\frac{b}{d}\right)t, y = y_0 - \left(\frac{a}{d}\right)t, t \in \mathbb{Z}.$$

i.e. $x = 500 + 5t \; and \; y = -4250 - 43t$, where t is an integer.

Step III By step II we get infinite solutions of LDE in terms of x and y. to concatenate them and get a single term we join them through their average. As every solution of LDE is a multiple of greatest common divisor so there is a pattern in solution, to create the randomness we take average randomly, i.e. first we shuffle the solution sets to destroy the pattern in solutions. In other words, we didn't take an average of x_i with y_i. To remove the pattern from data, we take the average of x_i with y_j, where $i \neq j$. Since LDEs has infinite solutions, so their solution space is the whole set of integers, to confine them in desired space we take mod 256 of these solutions.

Step IV Once space is confined, take unique elements of this space moving from left to right or any particular part of your choice and discard repeated elements. Create 8×8 S-box.

An overview of construction is given in the flow chart presented in fig. 1.

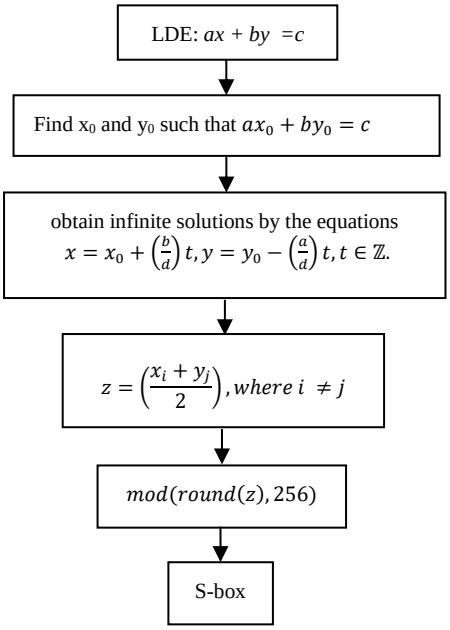

Fig. 1: Flow chart of S-box construction technique

Construction summary of S-box of order 16 is in Table 1.

Table 1: **The process to obtain 8×8 S-box over the solutions of LDE**

S. No	***X***	***Y***	$z = \left(\frac{x_i + y_j}{2}\right)$	**S-box entries** $mod(round(z), 256)$
1	29674	-82239	-2.6283e+04	85
2	30584	-84761	-2.7089e+04	47
3	33104	-91745	-2.9321e+04	119
⋮	⋮	⋮	⋮	⋮
255	26629	-73800	-2.3586e+04	222
256	34049	2540	-3.0158e+04	50

Above yield is arranged in 16×16 matrix to obtain the 8-by-8 S-box presented in Table 2.

Table 2: 8×8 S-box 1 over LDE

085	047	119	095	151	093	125	225	006	064	117	092	191	243	220	055
153	144	201	111	159	075	113	135	236	163	148	252	170	164	023	129
246	239	210	052	054	126	247	169	038	228	229	199	071	139	070	098
032	241	084	209	010	178	096	154	112	018	128	149	221	116	150	103
072	208	044	026	090	061	027	132	019	094	179	214	076	213	124	160
083	195	000	237	004	175	198	091	029	217	190	078	025	041	011	249
131	253	156	223	081	105	086	224	097	207	016	127	003	046	250	140
067	212	001	248	146	234	014	231	174	182	155	068	002	255	215	147
233	040	082	173	123	242	033	114	161	244	063	110	037	107	074	087
005	192	121	171	020	028	130	136	049	189	142	034	187	059	088	219
133	022	030	024	073	048	036	043	145	211	172	021	194	226	165	079
245	137	118	109	232	227	057	204	045	051	167	157	101	031	188	008
158	015	100	060	042	180	166	177	141	235	039	122	089	238	216	152
007	062	230	053	009	080	183	056	69	102	115	206	176	193	106	186
197	143	138	066	077	203	184	162	218	058	240	205	185	099	012	251
168	196	200	104	254	181	017	013	065	202	108	120	134	035	222	050

We take two more LDE's to get two more S-boxes, which are presented in Table 3 and Table 4.

Table 3: 8×8 S-box 2 over LDE

114	109	119	126	230	122	123	177	068	016	115	090	239	183	218	103
170	130	184	125	238	060	051	228	217	165	194	219	141	193	102	160
215	253	150	067	071	095	247	169	069	209	241	244	116	172	084	021
001	179	082	178	012	135	017	142	019	006	128	226	250	083	198	117
024	146	073	014	030	107	046	192	038	094	167	214	088	242	091	129
054	180	000	249	064	237	212	062	106	186	207	092	042	041	044	187
164	251	202	254	050	057	086	145	049	252	002	127	036	077	159	200
052	210	032	155	134	157	076	245	205	199	174	080	004	255	246	166
185	009	022	233	063	151	033	023	161	211	111	093	097	061	028	118
096	144	059	173	066	074	132	136	035	235	204	005	175	047	026	190
224	070	078	010	056	003	065	045	162	182	201	098	148	149	225	124
243	168	087	121	153	181	043	216	105	039	229	234	113	110	203	008
206	108	081	075	013	195	197	163	232	189	101	031	058	221	154	138
100	079	213	099	040	018	231	011	112	085	055	220	131	176	029	143
240	236	140	020	120	188	139	133	158	015	248	023	171	053	072	191
137	208	152	025	223	227	034	104	048	156	089	027	196	037	222	007

Table 4: 8×8 S-box 3 over LDE

212	061	245	221	087	220	252	166	017	128	244	216	127	231	218	117
078	066	142	189	095	141	228	023	186	039	082	250	043	050	085	006
243	191	195	112	113	249	247	046	049	178	182	151	149	015	145	161
032	230	208	198	009	099	160	075	224	065	002	086	222	240	083	181
136	194	056	073	201	124	077	018	069	217	103	211	152	214	248	034

197	135	000	190	016	063	147	205	092	206	123	153	076	044	013	238
007	254	090	223	196	172	209	162	164	159	064	253	005	057	235	026
133	210	004	234	067	171	025	183	059	115	079	144	001	255	215	071
174	040	193	062	237	227	036	225	038	242	125	185	052	173	137	213
020	130	236	047	080	088	003	010	100	126	027	033	111	109	200	207
022	081	089	072	140	096	048	045	070	199	058	084	131	163	054	157
246	014	241	188	170	167	108	154	060	101	055	094	180	093	122	008
091	029	176	120	041	114	051	102	030	175	053	233	204	187	202	074
021	121	179	116	012	192	119	104	148	177	229	155	098	134	169	107
150	031	011	129	156	143	106	035	203	105	158	225	110	165	024	239
042	146	138	168	251	118	068	028	132	139	184	232	019	037	219	097

4. Performance analyses of proposed S-boxes

An efficient S-box should satisfy some specific cryptographic criteria; objectiveness, nonlinearity, outputs bit independence, strict avalanche and linear approximation probability. We implement different analyses for the proposed S-boxes in order to test their strength and ranking with respect to some other famous S-boxes.

Nonlinearity: "The distance between the Boolean function f and the set of all affine linear functions is said to be nonlinearity of f." Simply the nonlinearity of a Boolean function "f" signifies the number of bits which transformed in the truth table of f to reach the adjacent affine function. Boolean functions on even number of input variables *n*, attaining the maximum nonlinearity of $(2^{n-1} - 2^{\frac{n}{2}-1})$ are called the bent functions [10]. Whereas for odd *n*, the nonlinearity value $(2^{n-1} - 2^{\frac{n-1}{2}})$ is known as the bent concatenation bound. Comparison of nonlinearity of proposed S-box with some existing S-boxes is presented in the table 5, given below. Readings of this analysis reveals that synthesized S-boxes can efficiently replace S-boxes based on algebraic construction because of its more appealing construction and chaos-based S-boxes due to its vast interval for randomness.

Strict avalanche criteria (SAC): Feng and Wu [11] introduced SAC. This criterion analyzes that how output bits the cryptograph responds to the changes applied to input bits. It is required half of the output bits must be changed on the variation of a single input bit value. As the iteration progresses, an avalanche of change in output bits caused by alteration of a single input bit.

The unpredictability made by cipher will be maximum if a change only in a single input bit can make changes in output bit with a probability of 0.5. We can observe from Performance Indexes of S-boxes that the proposed S-boxes successfully satisfied SAC. The average value of SAC for proposed S-boxes is much closed to the optimal value.

Bit independent criterion (BIC): It is imperative to examine the deviation in the performance of output bits when input bits are changed. Several methodologies are introduced to quantify this change. Bit independent criterion (BIC) is a well-known method to measure the degree of dependent change in any pair of output bits when any input bit is retreated. This criterion was first introduced by Webster and Tavares [12]. Through Performance Indexes of suggested S-boxes we noticed that these proposed S-boxes satisfied BIC to the best possible value.

Linear approximation probability (LP): Linear approximation probability is the maximum value of the imbalance of an occurrence. The uniformity of the input bits designated by the cover G_a is equal to the uniformity of the output bits selected by the cover G_b. Conferring to Matsui's definition [6], "linear approximation probability of a given S-box is defined as:

$$LP = \max_{G_a, G_b \neq 0} \left| \frac{\#\{a \in X \mid a.G_a = S(a).G_b\}}{2^n} - \frac{1}{2} \right|$$

Where G_a and G_b are input and output covers, respectively, "X" the set of all possible inputs; and 2^n is the number of elements of X". From Performance Indexes of S-boxes, we observe that the average value of LP of the recommended S-boxes is 0.0625 which is suitable to resist linear attacks.

Differential Approximation Probability (DP) [13]**:** The tool used to measure the differential uniformity of an S-box is differential approximation probability (DP), which is defined as:

$$DP^s(\Delta a \rightarrow \Delta b) = \left[\frac{\#\{a \in X \mid S(a) \pm S(a \pm \Delta a) = \Delta b\}}{2^m} \right]$$

This means, an input discrepancy Δa_i should exclusively map to an output discrepancy Δb_i, so that certifying an even mapping probability for each i. The average value of differential approximation probability for recommended S-boxes is 0.015625, which is the same as AES, APA, Gray S-box.

Performance Indexes of S-boxes are given in Table 5 and Table 6 shows the comparison of suggested S-boxes with residue prime, Xyi, Skipjack, APA and AES S-boxes.

Table 5: Performance Indexes for proposed S-boxes

Analysis	Max.	Min.	Average	Square Deviation	The differential approximation probability (DP)	The linear approximation probability (LP)
Nonlinearity:						
S-box 1	112	112	**112**			
S-box 2	113	110	**111.75**			
S-box 3	113	110	**111.75**			
SAC:						
S-box 1	0.5625	0.453125	**0.504883**	0.0156783		
S-box 2	0.5625	0.4375	**0.502686**	0.0155672		
S-box 3	0.5625	0.4375	**0.502686**	0.0155672		
BIC:						
S-box 1		112	**112**	0		
S-box 2		110	**111.286**	0.699854		
S- box3		110	**111.286**	0.699854		
BIC- SAC:						
S-box 1		0.480469	**0.504604**	0.0102709		
S-box 2		0.480469	**0.504116**	0.0111387		
S-box 3		0.480469	**0.504116**	0.0114285		
DP:						
S-box 1					**0.015625**	
S-box 2					**0.015625**	
S-box 3					**0.015625**	
LP:						
S-box 1	144					**0.0625**
S-box 2	146					**0.0703125**
S-box 3	146					**0.0703125**

Table 6: Comparison of Performance indexes of proposed S-boxes

S-boxes	Nonlinearity	SAC	BIC–SAC	BIC	DP	LP
AES S-box	112	0.5058	0.504	112.0	0.0156	0.062
APA S-box	112	0.4987	0.499	112.0	0.0156	0.062
Gray S-box	112	0.5058	0.502	112.0	0.0156	0.062
Skipjack S-box	105.7	0.4980	0.499	104.1	0.0468	0.109
Xyi S-box	105	0.5048	0.503	103.7	0.0468	0.156
Residue Prime	99.5	0.5012	0.502	101.7	0.2810	0.132
Lui	105	0.499756	0.500698	104.071	0.0390625	0.128906
[14]	110.50	0.5031	----	109.21	0.0234	0.0860

[15]	106.5	0.507	----	103.9	0.140	0.054
[16]	104.5	0.498	----	104.6	0.047	0.125
[17]	106	0.0520	----	104.2	0.039	0.132
[18]	105.5	0.5000	----	103.78	0.0468	0.1250
[19]	106	0.5020	----	103.00	0.0469	0.1250
[20]	110.25	0.5000	----	104	10	0.125
proposed:						
S-box 1	**112**	**0.496582**	**0.50020**	**111.429**	**0.0234375**	**0.0703125**
S-box 2	**111.75**	**0.502197**	**0.50411**	**111**	**0.0234375**	**0.0703125**
S-box 3	**111.75**	**0.497314**	**0.503209**	**104.214**	**0.046875**	**0.0125**

The comparison of some well-known nonlinear constituent for block ciphers with suggested is given in Table 6. We can see that nonlinearity is accomplishing the higher worth, when the high estimation of any Walsh Hadamard esteem is limited. The less a limit f can be approximated by any immediate limit, the higher its nonlinearity. There are cutoff points to how adaptable a Boolean limit can be against straight estimate as displayed by Parseval. In this spin-off, the nonlinearity of our proposed S-boxes 1 and 2 is higher than Skipjack, Xyi, Residue prime, Lui and S-boxes presented in [14-20]. The SAC analyses of our suggested S-boxes are very close to previously existing S-boxes. The comparison of the BIC analyses of anticipated S-boxes and accessible nonlinear segment of block ciphers are given in Table 4. It very well may be observed that as indicated by these results of BIC-nonlinearity, our foreseen S-box scheme is very similar to the AES , APA and Gray S-boxes.

The differential approximation probabilities (DP) of our proposed S-box is very similar to AES , APA and Gray S-boxes and S-boxes presented [14-20]. The lower is the linear approximation esteem, the better is the S-box's resistance against linear cryptanalysis (see Table 6). Along these lines the values of LP is lower in case of our foreseen S-boxes which unmistakably mirror the resistance of our S-boxes against linear cryptanalysis. Linear cryptanalysis tries to abuse high probability events of linear expressions including plaintext bits, "ciphertext" bits (truly we may use bits from the second last round yield), and subkey bits. It is a known plaintext attack: that is, it is started on the assailant having data on a course of action of plaintexts and the contrasting ciphertexts. Regardless, the attacker has no genuine method to choose which plaintexts (and relating ciphertexts) are accessible. In numerous applications and situations it is sensible to acknowledge that the attacker knows about an unpredictable plan of plaintexts and the relating ciphertexts.

5. Application of synthesized S-boxes in Image Encryption

We take an image of dimensions *256*, split it into three layers; red layer, green layer and blue layer. Each layer of the image is encrypted in two steps. In the first step we scramble the each of image through a permutation key generated by solutions of LDE and in the second step each layer is again vailed through S-boxes synthesized in section 3.

5.1 Pixels permutation

In this phase, the location of the pixels is mixed-up of the whole image without altering their values and the image becomes distorted. The determination of confusion is to diminish the high correlation between end-to-end pixels in the plain image. To boost the degree of unpredictability and the level of security, we take the solutions of three different LDEs in terms of x and y, calculate their average as described in the construction of S-box step-III. Hence, we get three sequences which will serve as permutation keys. After the generation of the required length of keys, shuffled them to create randomness and then we use the aforementioned three different keys for the pixel scrambling of each layer of the image. Suppose $I(i, j)$ be the plain image of dimension 256×256. Here i signifies the location of pixel on X-axis and j signifies the location of pixel on Y-axis. After permutation, we get the image $I'(i, j)$. Figures; 10, 11, 12, and 13 depict the results after applying permutation keys on each channel of an input image.5.2 **Pixels mixing**

After permutation, we have the image $I'(i, j)$. In the Pixels mixing process, we use trio cohort S-boxes; generated in section 3. For pixels mixing XOR operation is used. In each layer of permuted image, different S-box is XORed to achieve a high level of security and complexity. The process summarized in the figure below. $R'(i, j)$, $G'(i, j)$ and $B'(i, j)$ are splits layers of permuted image, $R_e(i, j)$, $G_e(i, j)$, $B_e(i, j)$ are encrypted layers and $I_e(i, j)$ is recombined layers. Which is the final encrypted image.

The whole encryption scheme is summarized in the flow chart given in Fig. *2*.

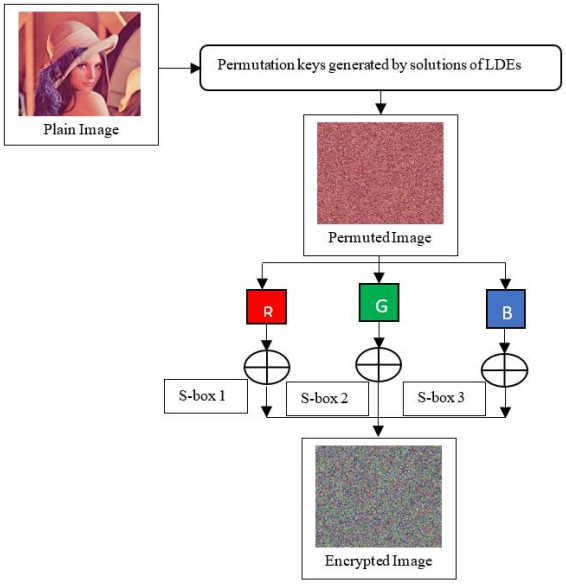

Fig. 2: Flow chart of Image encryption technique

Encryption and decryption processes are applied on Lena image through a given procedure. Figure 2 and 6 are original and encrypted images of Lena respectively. Figures; 3, 4, 5, 6 show red, green and blue layers of the original image whereas figures; 7, 8, 9, 10 permuted layers, and figures; 11, 12, 13, 14 are their layer-wise encryptions. By viewing these figures, one can analyze the efficiency of the given algorithm.

Fig. 3: Original image

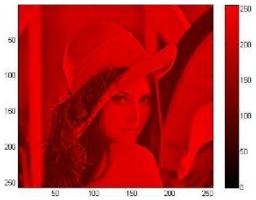

Fig. 4: Red layer

Fig. 5: Green layer

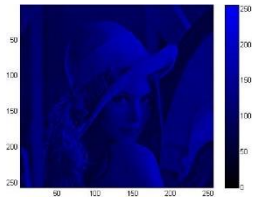

Fig. 6: Blue layer

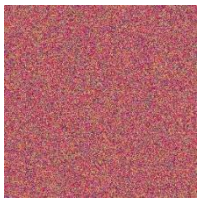

Fig. 7: Permuted image

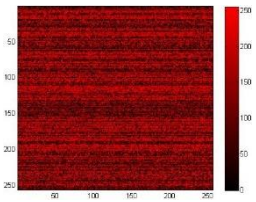

Fig. 8: Permuted red layer

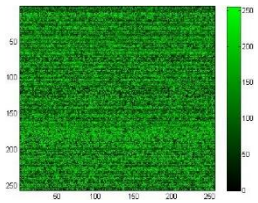

Fig. 9: Permuted green layer

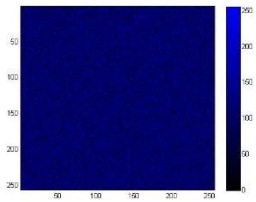

Fig. 10: Permuted blue layer

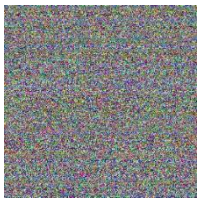

Fig. 11: Encrypted image

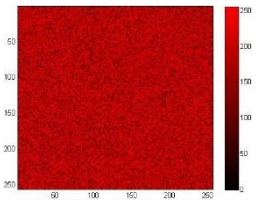

Fig12: Encrypted red layer

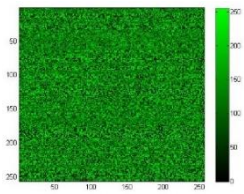

Fig13: Encrypted green layer

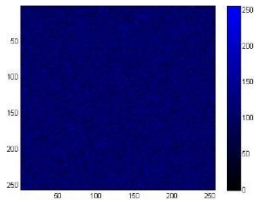

Fig14: Encrypted blue layer

6. Security Analysis

To determine the strength of the proposed encryption scheme, we perform an image encryption experiment on the “Lena” image of dimensions 256 and examine the encrypted image through some standard analyses like histogram, texture, robustness and differential analysis.

6.1 Histogram analysis

The 3D layer wise histogram of the plain-image and cipher image are in figures from 15 to 22. We found that the histograms of the ciphered image have a uniform distribution which highlights the usefulness of the algorithm, as all the 256 RGB channels present the same prospect.

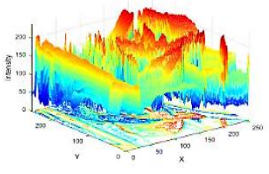

Fig. 15: Histogram of original image

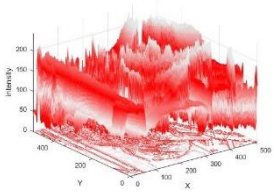

Fig. 16: Histogram of original red layer

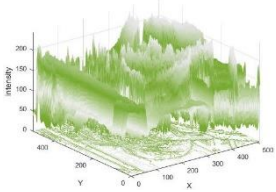

Fig. 17: Histogram of original green layer

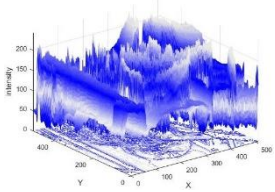

Fig. 18: Histogram of original blue layer

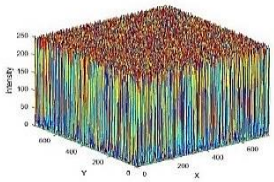

Fig. 19: Histogram of encrypted image

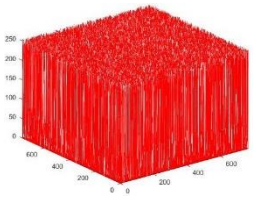

Fig. 20: Histogram of encrypted red layer

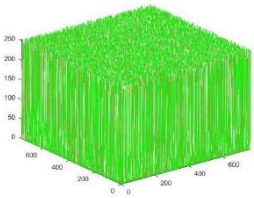

Fig. 21: Histogram of encrypted green layer

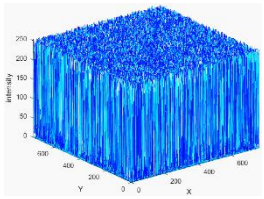

Fig. 22: Histogram of encrypted blue layer

6.2 Texture analysis of the image

One of the most significant features of a substantial defining the appearance of its exterior is the texture along with color. There are varies techniques to aspect the analysis of surfaces. Wavelet approach and Fourier approach are examples of such ways. However, the modest investigation is motivating as linked to the human optical system identifies texture, which is the very first method to texture analysis designed by Haralik [21], and it is still commonly used in image dissection. By this method, following five features are computed; energy, contrast, homogeneity, correlation, and Entropy, which are proposed to describe the texture.

6.2.1 Contrast

The extent of the difference in an image assists the observer to detect the entities in an image intensely. A lucid quantity of contrast intensities in the image also saturates the units which ease the identification of the image more precisely. The number of randomness increases during the encryption of an image, which promotes the contrast rank to a much higher value. The entities in the image entirely blur because of the nonlinear mapping from the replacement of the image file. One can infer that a higher level of contrast in the encoded image portrays robust encryption as it associates with the quantity of misperception molded by the S-box in the simple image. The illustration of this analysis is such as under

$$C = \sum_{i,j} (i-j)^2 p(i,j),$$

here i and j are the pixels in the image, and the number of gray-level co-occurrences matrices is represented by $p(i,j)$. Contrast is 0 for a constant image.

6.2.2 Correlation

The correlation analysis is partitioned into three different categories. It executes on upright, horizontal, and slanting formats. The association of a pixel to its neighbor is measured by this analysis. During this analysis, the texture of the whole image kept into consideration. The mathematical formulation of this analysis is the equation

$$K = \sum_{i,j} \frac{(i-\mu i)(j-\mu j)p(i,j)}{\sigma_i \sigma_j}.$$

Correlation is 1 or -1 for a dreamily positively or negatively associated image.

Figures from 23 to 30 expressed the correlation of adjacent pixels in the horizontal, vertical, diagonal and antidiagonal directions of the original and encrypted image respectively. The correlation between the original image pixel rendering evident linear relationship and encryption image pixels of random correspondent relations are visible.

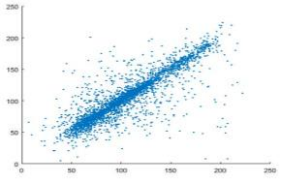

Fig.23: Horizontal correlation of original image

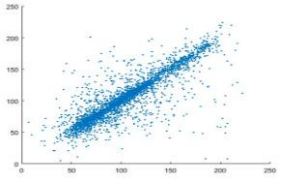

Fig.24: Vertical correlation of original image

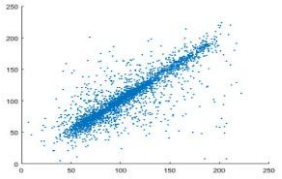

Fig.25: Diagonal correlation of original image

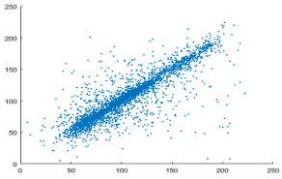

Fig.26: Antidiagonal correlation of original image

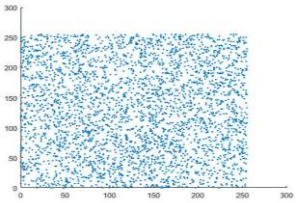

Fig.27: Horizontal correlation of encrypted image

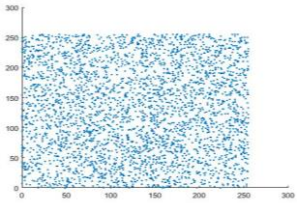

Fig.28: Vertical correlation of encrypted image

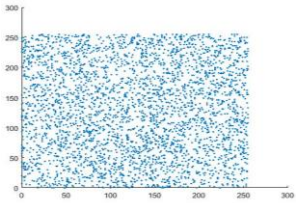

Fig.29: Diagonal correlation of encrypted image

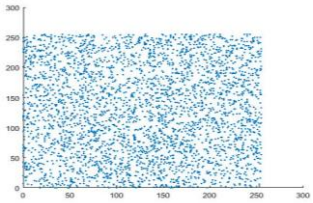

Fig.30: antidiagonal correlation of encrypted image

Table 7: Correlation coefficients of proposed scheme and its comparison

		Original image	Proposed image	[22]	[23]	[24]	[25]
Red	**Horizontal**	0.9387	0.0009	-0.0080	0.0818	0.0238	−0.0042
	Vertical	0.9688	0.00025	0.000029	0.0738	0.0163	−0.0036
	Diagonal	0.9083	-0.00009	-0.0086	0.0669	0.0172	0.0072
	Anti-Diagonal	0.9317	-0.0003	0.0076	0.0647	--	--
Green	**Horizontal**	0.9384	-0.00055	0.0039	0.0853	0.0218	0.0022
	Vertical	0.97564	0.00073	-0.0034	0.0789	0.0331	0.0026
	Diagonal	0.9210	-0.00006	-0.0044	0.0621	0.0186	0.0027
	Anti-Diagonal	0.9321	-0.0027	0.0018	0.0624	--	--
Blue	**Horizontal**	0.8922	-0.00026	0.0013	0.0804	0.0198	−0.0034
	Vertical	0.9418	-0.0007	-0.0005	0.0737	0.0123	0.0020
	Diagonal	0.9143	-0.000078	0.0027	0.0696	0.0148	0.0029
	Anti-Diagonal	0.8885	0.000072	0.0040	0.0699	--	--

The upshots of the correlation analysis are accessible in the Table 7. For a best encryption scheme, the correlation results must be equal to zero or approaches to zero. This table indicates the correlation of original image is almost close to 1 and the correlation of encrypted image is closer to 0.

6.2.3 Entropy

In an image, the amount of entropy is accompanying to the arrangement of objects which assist the humans to recognize the image. The process of replacement of nonlinear constituent in cryptosystem induced uncertainty in the image. The level of unpredictability brought by encryption is highly related to the fact that the human eye can identify the consistency in the image. The deficiency of unpredictability may consequence in recognition of the encrypted/processed image. Therefore, the extent of entropy can deliver essential evidence about the encryption asset and is measured as

$$= \sum_{i=0}^{n} p(x_i) log_b p(x_i),$$

where (x_{iH}) indicates the histogram counts. Table 8 enlist the values of entropy analysis.

Table 8: Comparison of Entropy Analysis

Images	Entropy
Proposed	7.9996
[21]	7.9985
[23]	7.9997

[24]	7.9993
[25]	7.9972

6.2.4 Energy

During the execution of energy analysis, the gray-level co-occurrence matrix is used. "Energy is the addition of squared elements in the GLCM. The mathematical demonstration of this analysis is such as

$$E = \sum_i \sum_j p^2(i,j).$$

For a continuous image, energy is 1".

6.2.5 Homogeneity

The data of an image connected to its contents have a natural distribution. To measure the closeness of the distributed text in the GLCM to GLCM diagonal we implement the homogeneity analysis. The GLCM illustrates the indicators of groupings of gray pixel levels in tabular form. The scrutiny additionally prolonged by treating entries from the GLCM table. The mathematical interpretation of this analysis given as

$$H = \sum_i \sum_j \frac{p(i,j)}{1+|i-j|}.$$

In Table 9, the texture analyses of encrypted and plain image are shown.

Table 9: Second order texture analyses for plain and encrypted Lena image

	Plain color components of image			**Cipher color components of image**		
	Red	**Green**	**Blue**	**Red**	**Green**	**Blue**
Contrast	0.407797	0.415518	0.399096	10.6173	10.5931	10.6341
Homogeneity	0.865153	0.866101	0.866035	0.38712	0.387554	0.38741
Entropy	7.32778	7.60503	7.13246	7.9985	7.9986	7.9985
Correlation	0.917715	0.926071	0.84887	-0.00096577	-0.000645	-0.000241
Energy	0.135304	0.0973005	0.159384	0.015638	0.0156366	0.0156396

6.3 NPCR and UACI analysis

For the strong cryptosystem of images, the universal stipulation is that the original image is completely stashed in its encrypted image. To estimate the strength of an encrypted image against the differential attack, there are two most probable techniques; a number of pixels change rate (NPCR) and unified average changing (UACI).

The NPCR (Number of pixels changing rate) [26] consider two encrypted images only differ by one pixel, If the first image is represented by $C_1(i, j)$ and the second by $C_2(i, j)$, then NPCR is evaluated as;

$$NPCR(C_1, C_2) = \frac{\sum_{i,j} D(i,j)}{T} \times 100\%,$$

Where T is the total number of pixels and $D(i, j)$ is defined as

$$D(i,j) = \begin{cases} 0, & if\ C_1(i,j) = C_2(i,j) \\ 1, & if\ C_1(i,j) \neq C_2(i,j) \end{cases}.$$

The UACI (Unified average changed intensity) [26] is designed to test the number of changing pixels and the number of averaged changed intensity between cipher text images, respectively, when the difference between plaintext images is subtle (usually a single pixel). Mathematically this analysis is represented by the formula,

$$UACI(C_1, C_2) = \frac{1}{MXN} \sum_{i=0}^{M-1} \sum_{j=0}^{N} \frac{|D(i,j) - P(i,j)|}{F \times T} \times 100\%,$$

Where F denotes the largest supported pixel value compatible with the cipher text image format and $D(i, j)$ is defined as:

$$D(i,j) = \begin{cases} 0, & if\ C_1(i,j) = C_2(i,j) \\ 1, & if\ C_1(i,j) \neq C_2(i,j) \end{cases}.$$

To get the strong encryption algorithm for images, the values of NPCR should be substantial than 99% and UACI values should be closer to 33%. Results of NPCR and UACI are given in Table 10.

Table 10: NPCR and UACI analysis of Lena image and its comparison

		Red	*Green*	*Blue*
Proposed Algorithm	**NPCR**	99.596	99.643	99.654
	UACI	33.097	30.57	33.0964
[27]	**NPCR**	99.6510	99.6267	99.5868
	UACI	26.169	28.4922	28.0849
[22]	**NPCR**	99.5148	99.5224	99.5018
	UACI	32.6698	29.8269	31.5435
[28]	**NPCR**	94.6836	95.6835	98.6810
	UACI	33.4647	34.5048	35.4999
[29]	**NPCR**	86.6846	86.6801	86.6807
	UACI	32.5103	32.4382	32.4340

The results shown in Table 10, offered that the proposed technique for image encryption has raised NPCR and pertinent UACI values. Higher NPCR values have shown that each pixel position is randomized exaggeratedly. And the pertinent UACI values presented that nearly every level of a grey pixel in the proposed encrypted algorithm are altered. For each RGB channel, NPCR values of proposed encrypted scheme are greater than the other referred schemes and UACI values are greater than the schemes presented in reference [28,29]. So, the comparison depicts that the proposed encryption algorithm has competent diffusion properties, which indicate its high resistance against algebraic attacks.

6.4 Robustness Analysis

Here, we center around the robustness of the proposed image encryption algorithm against the image processing operation, geometrical twists (for example, cropping). For accommodation, we take the encoded Lena image in Figure 11 as the test image in the accompanying simulations. Cropping is usually utilized in genuine applications. It is a lossy activity. In Figure 31 and 32 an information blocks with size 128×128 and 128×256 is removed from the cipher-image respectively. Figures 33 and 34 show the relating decrypted images. As can be seen, the decrypted images still contain the greater part of the first visual data. This shows the great robustness of the proposed encryption algorithm against cropping attacks.

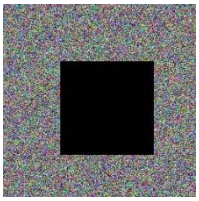

Fig. 31: encrypted image with a 128 × 128 data cut

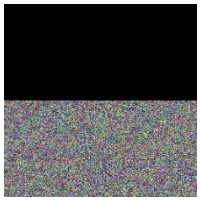

Fig. 32: encrypted image with a 128 × 256 data cut

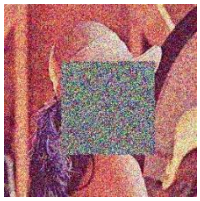

Fig. 33: decrypted image from (31)

Fig. 34: decrypted image from (32)

7. Conclusion

In the presented work, an innovative technique for the construction of S-boxes through the solutions of the Linear Diophantine equation is introduced. These S-boxes are used in image encryption together with the permutation keys, which are also obtained by solutions of LDEs. The application of the projected S-boxes, during the encryption process, increases the randomness in the plaintext, as chaos does. Chaos has a specific interval for its randomness, but solutions of LDE have the whole set of integers for its randomness, thus making it tremendously hard for the cryptanalyst to decipher secure data. To check the effectiveness of the proposed S-boxes and image encryption quality, we apply different types of analysis. The readings of these analyses in case of image encryption are much closed to optimal values that depict the validation of our construction method. Since this technique is more economical, also it can generate as many as S-boxes as chaos-based techniques could generate, therefore it is a brilliant choice to replace the nonlinear component in chaos-based ciphers and in some other renowned ciphers, for instance in AES. On the basis of the solution of one LDE infinite number of S-Boxes can be constructed. In future, we will obtain more S-boxes and classify them on the basis of some renowned analysis to use them in cryptographic contents more competently.

References

1. Chen, G., Chen, Y., & Liao, X. (2007). An extended method for obtaining S-boxes based on three-dimensional chaotic Baker maps. *Chaos, Solitons & Fractals*, *31*(3), 571-579.
2. Hussain, I., Shah, T., & Mahmood, H. (2010). A new algorithm to construct secure keys for AES. *International Journal of Contemporary Mathematical Sciences*, *5*(26), 1263-1270.
3. Tran, M. T., Bui, D. K., & Duong, A. D. (2008, December). Gray S-box for advanced encryption standard. In *2008 International Conference on Computational Intelligence and Security* (Vol. 1, pp. 253-258). IEEE.
4. Yi, X., Cheng, S. X., You, X. H., & Lam, K. Y. (1997, November). A method for obtaining cryptographically strong 8 X 8 S-boxes. In *GLOBECOM 97. IEEE Global Telecommunications Conference. Conference Record* (Vol. 2, pp. 689-693). IEEE.
5. Webster, A. F., & Tavares, S. E. (1985, August). On the design of S-boxes. In *Conference on the theory and application of cryptographic techniques* (pp. 523-534). Springer, Berlin, Heidelberg.
6. Matsui, M. (1993, May). Linear cryptanalysis method for DES cipher. In *Workshop on the Theory and Application of Cryptographic Techniques* (pp. 386-397). Springer, Berlin, Heidelberg.
7. Kim, J., & Phan, R. C. W. (2009). Advanced differential-style cryptanalysis of the NSA's skipjack block cipher. *Cryptologia*, *33*(3), 246-270.
8. Nkapkop, J. D. D., Effa, J. Y., Fouda, J. S. A. E., Alidou, M., Bitjoka, L., & Borda, M. (2014). A fast image encryption algorithm based on chaotic maps and the linear diophantine equation. *Computer science and applications*, *1*(4), 232-243.
9. Burton, D. M. (2006). *Elementary number theory*. Tata McGraw-Hill Education.
10. Dobbertin, H., Leander, G., Canteaut, A., Carlet, C., Felke, P., & Gaborit, P. (2006). Construction of bent functions via Niho power functions. *Journal of Combinatorial Theory, Series A*, *113*(5), 779-798.
11. Feng, D., & Wu, W. (2000). Design and analysis of block ciphers.
12. Dawson, M. H., & Tavares, S. E. (1991, April). An expanded set of S-box design criteria based on information theory and its relation to differential-like attacks. In *Workshop on the Theory and Application of of Cryptographic Techniques* (pp. 352-367). Springer, Berlin, Heidelberg.
13. Biham, E., & Shamir, A. (1991). Differential cryptanalysis of DES-like cryptosystems. *Journal of CRYPTOLOGY*, *4*(1), 3-72.
14. Shahzad, I., Mushtaq, Q., & Razaq, A. (2019). Construction of New S-Box Using Action of Quotient of the Modular Group for Multimedia Security. *Security and Communication Networks*, *2019*.
15. Zahid, A. H., & Arshad, M. J. (2019). An Innovative Design of Substitution-Boxes Using Cubic Polynomial Mapping. *Symmetry*, *11*(3), 437.
16. Liu, L., Zhang, Y., & Wang, X. (2018). A novel method for constructing the S-box based on spatiotemporal chaotic dynamics. *Applied Sciences*, *8*(12), 2650.
17. Wang, X., Akgul, A., Cavusoglu, U., Pham, V. T., Vo Hoang, D., & Nguyen, X. (2018). A chaotic system with infinite equilibria and its S-box constructing application. *Applied Sciences*, *8*(11), 2132.
18. Belazi, A., & El-Latif, A. A. A. (2017). A simple yet efficient S-box method based on chaotic sine map. *Optik*, *130*, 1438-1444.
19. Ullah, A., Jamal, S. S., & Shah, T. (2017). A novel construction of substitution box using a combination of chaotic maps with improved chaotic range. *Nonlinear Dynamics*, *88*(4), 2757-2769.
20. Wang, Y., Lei, P., & Wong, K. W. (2015). A method for constructing bijective S-box with high nonlinearity based on chaos and optimization. *International Journal of Bifurcation and Chaos*, *25*(10), 1550127.
21. Haralick, R. M., Shanmugam, K., & Dinstein, I. H. (1973). Textural features for image classification. *IEEE Transactions on systems, man, and cybernetics*, (6), 610-621.
22. Alabaichi, A. M. (2016). Color Image Encryption using 3D Chaotic Map with AES key Dependent S-Box. *International Journal of Computer Science and Network Security (IJCSNS)*, *16*(10), 105-115.
23. Alabaichi, A. (2018). True Color Image Encryption Based on Dna Sequence, 3D Chaotic Map, And Key-Dependent Dna S-Box Of Aes. *Journal of Theoretical & Applied Information Technology*, *96*(2).
24. Silva-García, V. M., Flores-Carapia, R., Rentería-Márquez, C., Luna-Benoso, B., & Aldape-Pérez, M. (2018). Substitution box generation using Chaos: An image encryption application. *Applied Mathematics and Computation*, *332*, 123-135.

25. Liu, H., Kadir, A., & Niu, Y. (2014). Chaos-based color image block encryption scheme using S-box. *AEU-international Journal of Electronics and Communications*, *68*(7), 676-686.

26. Khan, M. (2015). A novel image encryption scheme based on multiple chaotic S-boxes. *Nonlinear Dynamics*, *82*(1-2), 527-533.

27. Wu, Y., Noonan, J. P., & Agaian, S. (2011). NPCR and UACI randomness tests for image encryption. *Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT)*, *1*(2), 31-38.

28. Hussain, I., Shah, T., & Gondal, M. A. (2012). An efficient image encryption algorithm based on S8 S-box transformation and NCA map. *Optics Communications*, *285*(24), 4887-4890.

29. Hussain, I., Shah, T., & Gondal, M. A. (2014). Image encryption algorithm based on total shuffling scheme and chaotic S-box transformation. *Journal of Vibration and Control*, *20*(14), 2133-2136.