An Effective S-Box Construction Based on Linear Recurrences With Constant Co-Efficient

wajeeha Iftikhar (wajeehaiftikhar993@gmail.com)
University of Engineering and Technology Taxila, Pakistan
NASIR SIDDIQUI
University of Engineering and Technology Taxila, Pakistan
Muhammad Ehtisham ul Haq
University of Engineering and Technology Taxila, Pakistan

Research Article

Keywords: Substitution-box, Symmetric Cryptography, Linear Recurrence Formula, Image Encryption

Posted Date: March 16th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-259399/v1

An effective S-box construction based on linear recurrences with constant co-efficient

Nasir Siddiqui[a] , Wajeeha Iftikhar [a] and Muhammad Ehtisham ul Haq[b]

Abstract

In this paper, we propose an algorithm for the construction of substitution-box through a linear recurrence relation. S-box is considered as the building block of block ciphers; here we present a technique to construct Substitution-boxes by using linear recurrence relation to comply with the standards of good quality S-boxes. We have witnessed that the latest research relies more on improving already existing techniques, rather than developing wholly new methods. We use linear recurrence in an entirely new way. Real initial and obtained values are concealed by converting it into new numbers to avoid any pattern to follow. The obtained S-boxes are analyzed through performance tests to check the strength and quality of our S-boxes. Later we will encrypt an image and also perform encryption and decryption in noise channels to make it more applicable in low profile applications.

Keywords Substitution-box, Symmetric Cryptography, Linear Recurrence Formula, Image Encryption

1 Introduction

The security of data has become a major necessity of our life in the present era. Fast and modern communication channels are being used around the globe, which demands the security of a transmitted data. In order to prevent the misuse of data by unauthorized people, many researchers are developing techniques to create confusion in the original data. As time progresses, the need

[a] Department of Basic Sciences, University of Engineering and Technology, Taxila, Pakistan

E-mail address: nasir.siddiqui@uettaxila.edu.pk (N. Siddiqui), wajeehaiftikhar993@gmail.com (W. Iftikhar)

[b] Department of Computer Engineering, University of Engineering and Technology, Taxila, Pakistan

E-mail address: ehatishamuet@gmail.com

for cryptographically secure systems is becoming very important as we are using them not only in military applications, but also in our daily life in our mobile phones, social media accounts; Banks, remote control car lock systems [1].

Substitution-box plays a significant role in ensuring the security of the system and is considered to be a major component of a symmetric block ciphers. Substitution-box creates confusion in data by establishing a unique relationship between plaintext and cipher text. Most secure block ciphers include both substitution and permutation [2]. The purpose of this paper is to construct S-boxes, which satisfy all the necessary conditions of a secure system. It is a known fact that in the last two decades; the academic study of construction of Substitution-boxes for safety of our data has been an attractive area of study for many researchers. AES is considered as the strongest systems and is widely used, but due to the high computational complexities, comparatively easy applicable algorithms are developed these days[3].

The proposed technique of our S-box construction is based on linearly recurrence relation. The idea of using linear recurrence may be perceived as outdated in this era. However, we will use it in a unique way along with the latest methods to get efficient results.

In section 1, the preliminaries will be discussed. In section 2, the method for the construction of our substitution-box will be explained. In section 3, the comparison with already existing techniques will be discussed. The strength of the constructed S-boxes is tested on the basis of non-linearity, BIC (Bit Independence criterion, SAC (Strict Avalanche Criterion, LP (Linear Probability) and DP (Differential probability) [4], [5].

2 Preliminaries

2.1 Linear recurrence formula:

In order to incorporate linear recurrence in this research, I will have to delve into its prior history, which can be classified as finite history and full history [6]. Finite history emphasizes on the dependence of fixed number of earlier values while an equation that depends on all the preceding terms has a full history. Similar to differential equation it can be classified into homogeneous and non-homogenous. Homogenous linear recurrence relations are easily distinguishable from non-homogenous relations due to the presence of an extra term $g(x)$ .The formula of linear recurrence is defined in equation (1).

$$c_0 x_n + c_1 x_{n-1} + \cdots + c_m x_{n-m} = g(x), \qquad n \geq m \tag{1}$$

If $g(x) = 0$,equation is homogenous, but when it is not equal to zero, then equation is non-homogenous. Here we have considered a homogenous equation with all coefficients zero except $c_0, c_1$and c_2.Here we take the values as $c_0 = 1, c_1 = -1$ and $c_2 = -1$.

3 Scheme of Proposed S-box:

3.1 Step 1

First we consider the Fibonacci number calculation formula [6]. We are using the following equation.

$$x_n = x_{n-1} + x_{n-2} \tag{2}$$

Consider two initial values randomly.

3.2 Step 2:

The values are calculated. But after many iterations maximum of 168 values are calculated. To calculate more values we apply the same formula with slight change in initial conditions. The process repeats until we get all required values. We get all values by using a formula three to four times with the change in initial conditions and using different variables. For example this time we use equation (3).

$$y_n = y_{n-1} + y_{n-2} \tag{3}$$

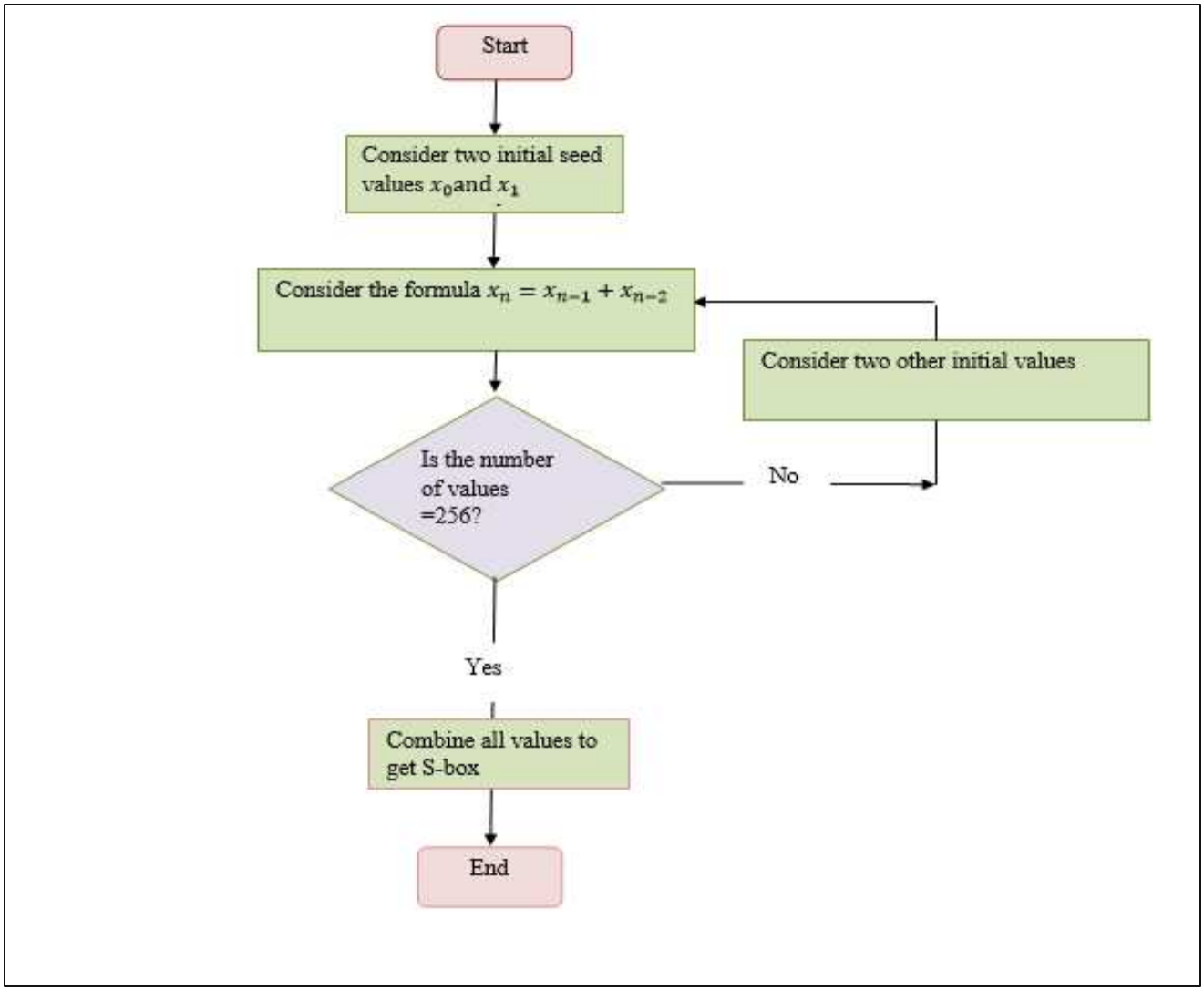
We can also change the formula as a product of preceding terms instead of summation to create more confusion.

3.3 Step 3:

The numbers are arranged in specific way that calculated values are picked in iterations in a respective manner. For example, the first value from x is used, then the first value of y and so on. This step will make all values more random. The program is designed in MATLAB software.

Table 1 Initial values

x_0	x_1	y_0	y_1	z_0	z_1	t_0	t_1
150	130	185	146	180	165	95	240



f ig 1 Flowchart Representation

The S-box obtained by following these steps is shown in table 2.All the values are obtained with x, y and z variables. But to create more confusion, in the last step we are using formula presented in equation (4)

$$t_n = t_{n-1} \times t_{n-2} \quad (4)$$

Table 2 Proposed S-box after three steps

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

It can be observed that the all our initial values are appearing in the first row, so overcome this problem we will have to move on to the next step.

3.4 Step 4

The actual obtained S-box is transformed by converting the values from decimal to binary and permuted in reverse order to get the new decimal numbers, which does not affect the non-linearity of the S-box; rather it helps us hide the initial values.

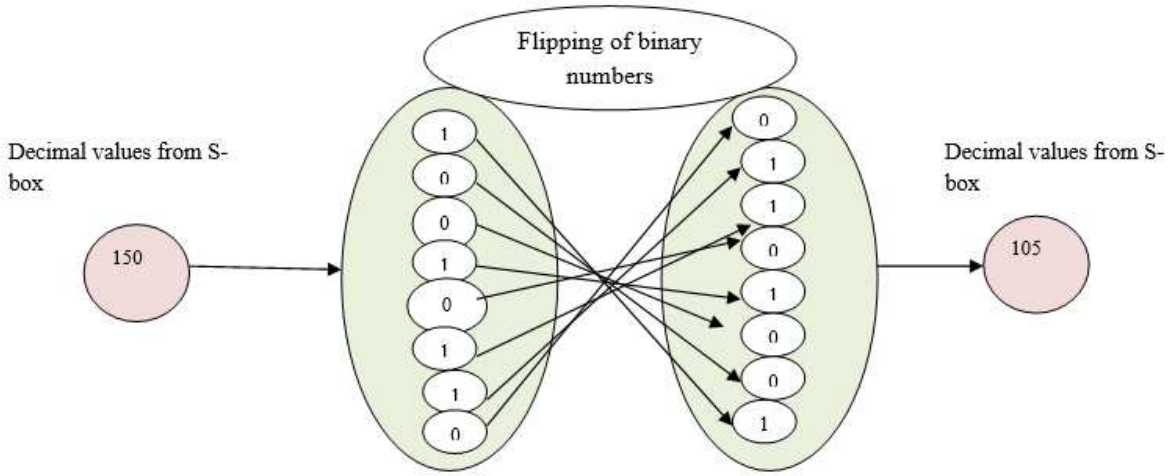


fig 2 Flipping of numbers

Similar process is applied to every value in the S-box to transform our S-box into a new S-box.

Table 3 Final Proposed S-box

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

4 Analysis criterion of S-boxes:

The In order to investigate the strength of our constructed S-box, we will have to test our substitution box according to the following criterions such as Non-Linearity, Strict Avalanche Criterion, Linear Probability, Differential probability and bit independence criterion as explained in [7], [8]. The values obtained are presented in the Table 4.

Table 4 Analysis of the constructed S-box

Analysis	Max Value	Min Value	Average value	LP	DP	Square deviation
Non linearity	108	104	106			
SAC	0.609375	0.406250	0.497070			0.046408
LP	160.0			0.125		
DP					0.039062	
BIC	103.571	98.000	2.1			

Table 5 Comparisons with different S-boxes

S-boxes	Non- linearity			SAC	LP	DP	BIC
	Maximum	Minimum	Average Value				
Proposed S-box	108	104	106	0.4970	160	0.039	103.57
AES S-box[9]	112	112	112	0.504	144	0.0156	112
APA S-box[10]	112	112	112	0.5	144	0.0156	112
Gray S-box[11]	112	112	112	0.499	144	0.0156	112
S_8 AES S-box[12]	112	112	112	0.504	144	0.0156	112
Skipjack S-box[13]	108	104	105.75	0.503	156	0.0468	104.14
Xyi S-box[14]	106	104	105	0.502	168	0.0468	103.78
Residue prime[15],[16]	104	94	99.5	0.516	162	0.281	101.71
[17]	108	102	104.5	0.4980	160	0.0469	104.64

4.1 Non-linearity:

S-box is designed in such a way that the relation between plaintext and cipher text is nonlinear in terms of mapping, otherwise it would be susceptible to linear cryptanalysis. Non-linearity is actually the distance between a Boolean function and the set of all the affine functions. The importance of non-linearity for the encryption process cannot be denied [8].

The calculated non-linearity of our S-box is 106, with minimum non-linearity as 104 and maximum non-linearity as 108.The comparison with the non-linearity of the known ciphers is presented in the table 6 and Figure 3.

Table 6 Comparison of Non-Linearity of existing S-boxes

S-boxes	0	1	2	3	4	5	6	7	Average Non-linearity
Proposed S-box	104	106	106	104	108	106	108	106	106
AES S-box[9]	112	112	112	112	112	112	112	112	112
APA S-box[10]	112	112	112	112	112	112	112	112	112
Gray S-box[11]	112	112	112	112	112	112	112	112	112
S_8 AES S-box[12]	112	112	112	112	112	112	112	112	112
Skipjack S-box[13]	104	104	108	108	108	104	104	106	105.75
Xyi S-box[14]	106	104	104	106	104	106	104	106	105
Residue prime[15],[16]	94	100	104	104	102	100	98	94	99.5

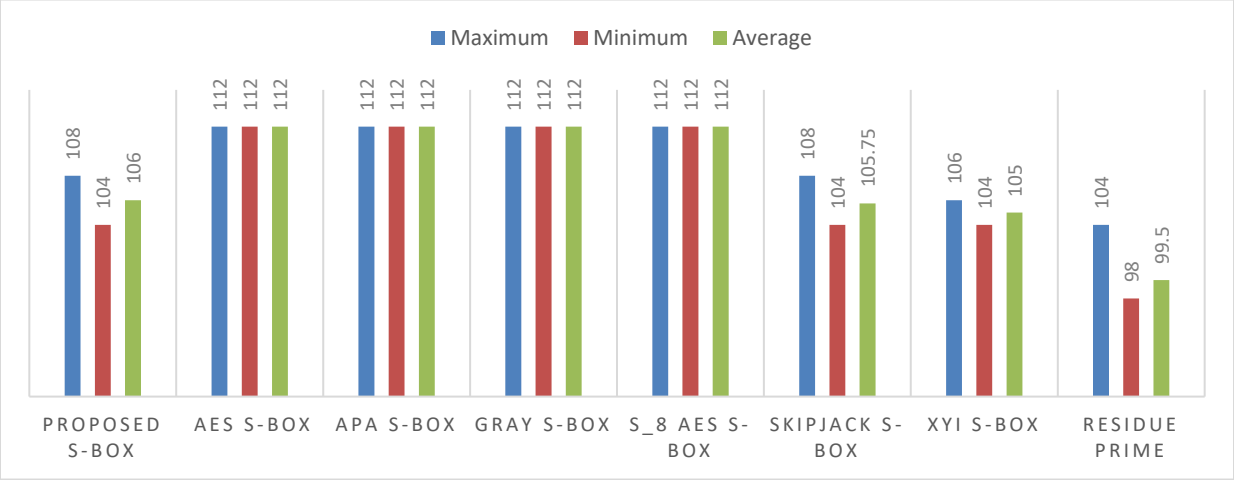


fig 3 Non linearity

4.2 Strict Avalanche Criterion:

According to the Strict Avalanche Criterion, if in the function that is forming the substitution box we change the single bit of input it is necessary that there is probability of 50% change in the output bits sequence. If the value is closer to AES, it becomes more reliable. The obtained strict avalanche value for our constructed S-Box is better than skipjack s-box and residue prime.

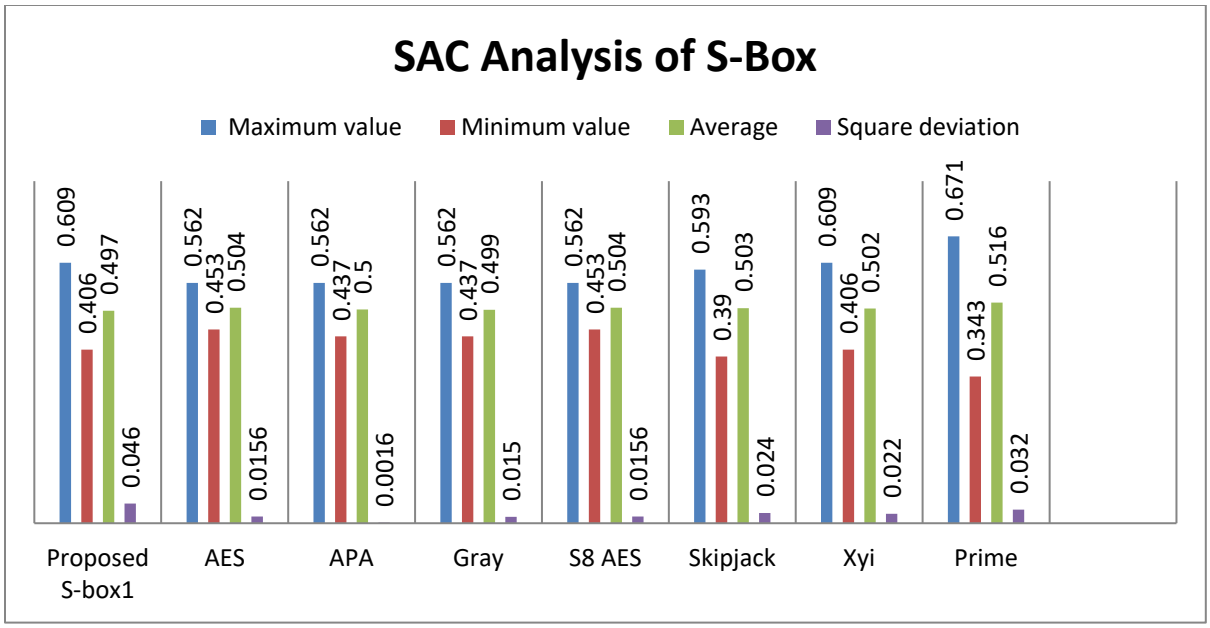


fig 4 Strict Avalanche criterions

4.3 Bit Independence Criterion:

The independent behavior of the pair of variables and the changes in input bits are considered as significant factors of bit independence criterion. According to this criterion, input bits are transformed completely, and then output bits are checked for their independence. Bit independence is one of the most important criterions of S-box strength.

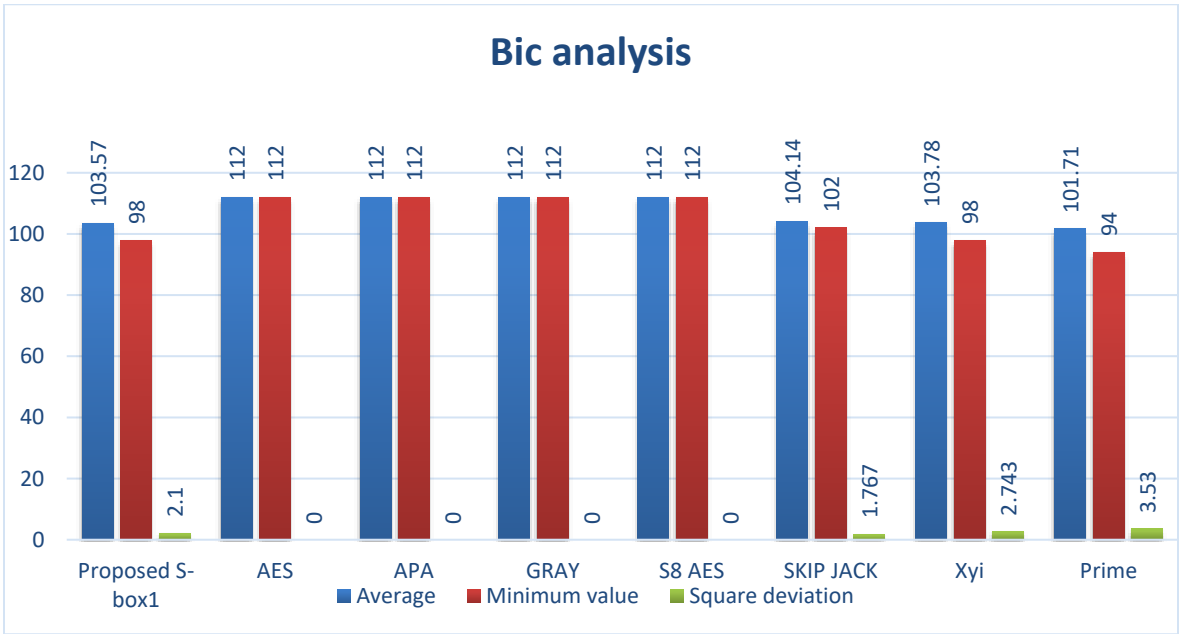


fig 5 Bit Independence Criterion

4.4 Differential probability and Linear Probability

To access the imbalance of an event, the linear probability of the constructed S-box is calculated. It is represented by the formula given in equation (5)

$$LP = \max_{\beta p, \beta q \neq 0} \left| \frac{\#\{ x \varepsilon GF(2^8) / x.\beta p = s(x).\beta q \}}{2^q} - \frac{1}{2} \right| \qquad (5)$$

In the given formula, p represents the input values of S-box. The input and output masks are expressed in the form of βp, βq respectively. We have compared our results with standard results. Our obtained value is 0.125, which is not too susceptible in terms of linear attacks [18].

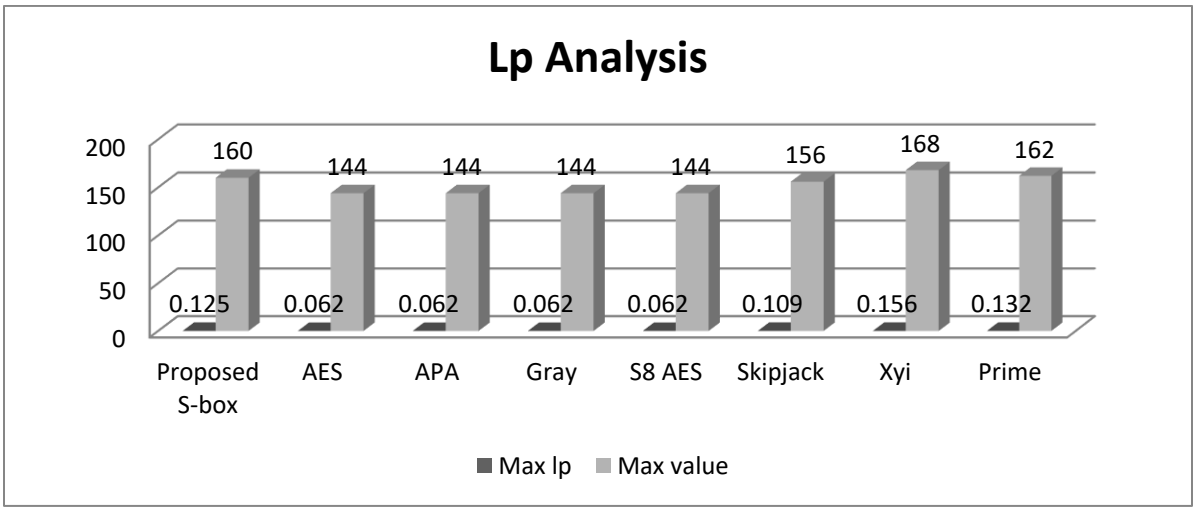


fig 6 Linear Probability

To measure the differential uniformity of the constructed S-box we will check the differential probability of the constructed S-box. The formula for the calculation of differential probability is expressed in the following form in equation (6)

$$DP = \left[\frac{\#\{x \epsilon\ X / S(x) \oplus S(y \oplus \Delta x = \Delta y\}}{2^p} \right] \qquad (6)$$

To represent the differentials we will use Δx andΔy . On the basis on comparative analysis, we can say that our results are better than Skipjack, X_{yi} and residue prime [18].

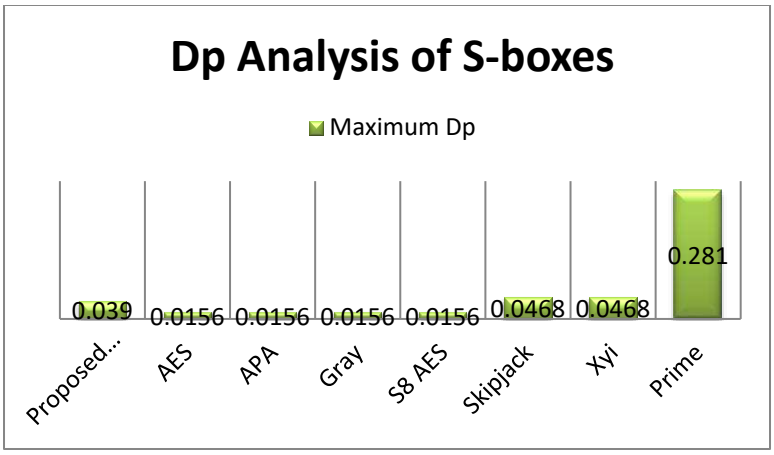


fig 7 Differential probability

5 Image Encryption:

Here we encrypt the image in order to test the strength of the constructed S-box. We are using capsicum image for the encryption process. The image from pixel value of 0 to 266 is considered for encryption and the S-box ranging from 0 to 256 constructed is applied on the image, which will replace values of the image according to the our S-box. The algorithm is applied twice to get the best encrypted image.

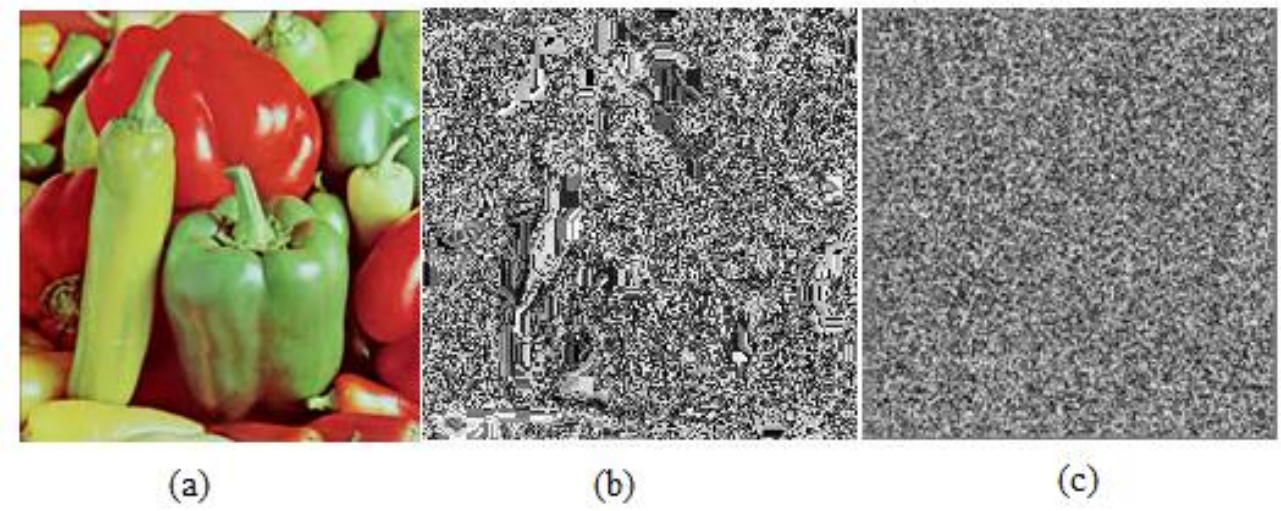


fig 8 Capsicum Image Encryption (a) Original Image (b) First Round Encrypted Image and(c) Final Encrypted image

Table 7 Image encryption using first algorithm

Image	Entropy	Correlation coefficient	Energy	Contrast	Homogeneity
Pepper Image	7.5846	0.1013	0.0178	9.2410	0.4663

6 Noise resistant property of the proposed Encryption Scheme:

As we know, that the intruder can add noise to any communication channel intentionally. This makes it necessary to develop an algorithm, which is noise resistant. The noise must be removed to reduce the effect of channel noise caused by unauthorized person [20], [21].

The next step is followed by the analysis of our constructed S-box on the basis of bit error rate (BER) which is actually a function of length of burst errors for multiple values of SNR in aggregation with the single error correction code. We will have to compare the performance of our constructed S-box with conventional random S-box, Algebraic S-box and Chaotic S-Box. The conventional S-box is available in MATLAB as RANDINTRLV function, which makes MATLAB software to be a necessary tool. The data to taken is in the 100 random blocks with the size N=256.To encode our data we are using linear hamming code. The length of the cord word is (7, 4) whereas the minimum value of the hamming distance will be 3 in order to rectify even a single error. WE will have to introduce the burst of errors with different lengths and then we will XOR it with modular data to analyze the performance against burst errors. Error rates are calculated and compared with the standard S-boxes error rates at different values of SNR. We will compare our results with the AES, Gray, Skipjack and Residue prime S-boxes. The values for known S-boxes are taken from research paper [22].

Table 8 SNR=5 Error rate

Proposed box	0.48836	0.5267 2	0.51432	0.49176	0.50002	0.51988
AES	0.51024	0.49726	0.50752	0.48836	0.50478	0.50342
Gray	0.50068	0.4726	0.49452	0.52324	0.49314	0.48764
skipjack	0.487	0.4997	0.4910	0.5232	0.4917	0.4883
residue	0.50134	0.50684	0.51574	0.4863	0.51988	0.51438

Table 9 SNR=10 Error rate

Proposed box	0.41966	0.4175	0.42868	0.4328	0.40998	0.44062
AES	0.42626	0.41104	0.42532	0.42826	0.41532	0.42396
Gray	0.41404	0.42832	0.4167	0.42144	0.41014	0.43382
skipjack	0.4184	0.4085	0.4079	0.429	0.4137	0.4226
residue	0.43694	0.4143	0.42026	0.41984	0.41216	0.43372

Table 10 SNR=15 Error rate

Proposed box	0.00668	0.01052	0.01866	0.02438	0.03308	0.04632
AES	0.00618	0.01294	0.02292	0.02988	0.03636	0.04592
Gray	0.00606	0.0125	0.0164	0.02808	0.03486	0.05184
skipjack	0.0183	0.0306	0.0389	0.0540	0.0562	0.0635
residue	0.0060	0.01578	0.02082	0.0273	0.03064	0.0379

7 Conclusion

In this work, we proposed a new scheme for the construction of S-boxes. We have established that linear recurrence relation can be used to construct efficient S-boxes in a simpler way. The technique presented for construction has better than some known algorithms. The strength of constructed S-boxes is analyzed by performance tests in order to cope up to the standards of good S-boxes. Furthermore, the constructed S-box is used for the encryption of an image and noise removal.

References:

[1] Paar, C., & Pelzl, J. (2009). *Understanding cryptography: a textbook for students and practitioners*. Springer Science & Business Media.

[2] Greene, D. H., & Knuth, D. E. (2007). *Mathematics for the Analysis of Algorithms*. Springer Science & Business Media

[3] Sarfraz, M., Hussain, I., Ali, F., & Rasheed, A. (2016). A Mobius Transformation Based Algorithm for the Construction of Cryptographically Strong 131028 S-Boxes Having Highly Nonlinear. *International Journal of Computer Science and Information Security*, *14*(5), 611.

[4] Ahmad, M., Haleem, H., & Khan, P. M. (2014, February). A new chaotic substitution box design for block ciphers. In *2014 International Conference on Signal Processing and Integrated Networks (SPIN)* (pp. 255-258). IEEE.

[5] Han, J. S., Kim, H. S., & Neggers, J. (2012). On Fibonacci functions with Fibonacci numbers. *Advances in Difference Equations*, *2012*(1), 126.

[6] Wilf, H. S. (2005). generatingfunctionology. CRC press.

[7] Zahid, A. H., & Arshad, M. J. (2019). An Innovative Design of Substitution-Boxes Using Cubic Polynomial Mapping. *Symmetry*, *11*(3), 437.

[8] Farwa, S., Muhammad, N., Shah, T., & Ahmad, S. (2017). A novel image encryption based on algebraic S-box and Arnold transform. *3D Research*, *8*(3), 26.

[9] Daemen, J., & Rijmen, V. (2013). *The design of Rijndael: AES-the advanced encryption standard*. Springer Science & Business Media.

[10] Cui, L., & Cao, Y. (2007). A new S-box structure named Affine-Power-Affine. *International Journal of Innovative Computing, Information and Control*, *3*(3), 751-759.

[11] 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.

[12] 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.

[13] Hussain, I., Shah, T., Gondal, M. A., & Wang, Y. (2011). Analyses of SKIPJACK S-box. *World Appl. Sci. J*, *13*(11), 2385-2388.

[14] 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.

[15] Abuelyamam, E. S. (2013, August). Residues of prime numbers as entries for the S-Box. In *2013 INTERNATIONAL CONFERENCE ON COMPUTING, ELECTRICAL AND ELECTRONIC ENGINEERING (ICCEEE)* (pp. 584-588). IEEE.

[16] Hussain, I., Shah, T., Mahmood, H., Gondal, M. A., & Bhatti, U. Y. (2011). Some analysis of S-box based on residue of prime number. *Proc Pak Acad Sci*, *48*(2), 111-115.

[17] 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.

[18] Khan, M., & Shah, T. (2015). An efficient construction of substitution box with fractional chaotic system. *Signal, Image and Video Processing*, *9*(6), 1335-1338.

[19] Cheung, J. M. (2010). *The design of S-boxes* (Doctoral dissertation, Sciences).

[20] Hussain, I., Anees, A., Aslam, M., Ahmed, R., & Siddiqui, N. (2018). A noise resistant symmetric key cryptosystem based on S 8 S-boxes and chaotic maps. *The European Physical Journal Plus*, *133*(4), 167.

[21] Hussain, I., Shah, T., Gondal, M. A., & Khan, W. A. (2011). Construction of cryptographically strong 8× 8 S-boxes. *World Applied Sciences Journal*, *13*(11), 2389-2395.

[22] Siddiqui, N., Naseer, A., & Ehatisham-ul-Haq, M. (2020). A Novel Scheme of Substitution-Box Design Based on Modified Pascal's Triangle and Elliptic Curve. *Wireless Personal Communications*, 1-16.

Figures

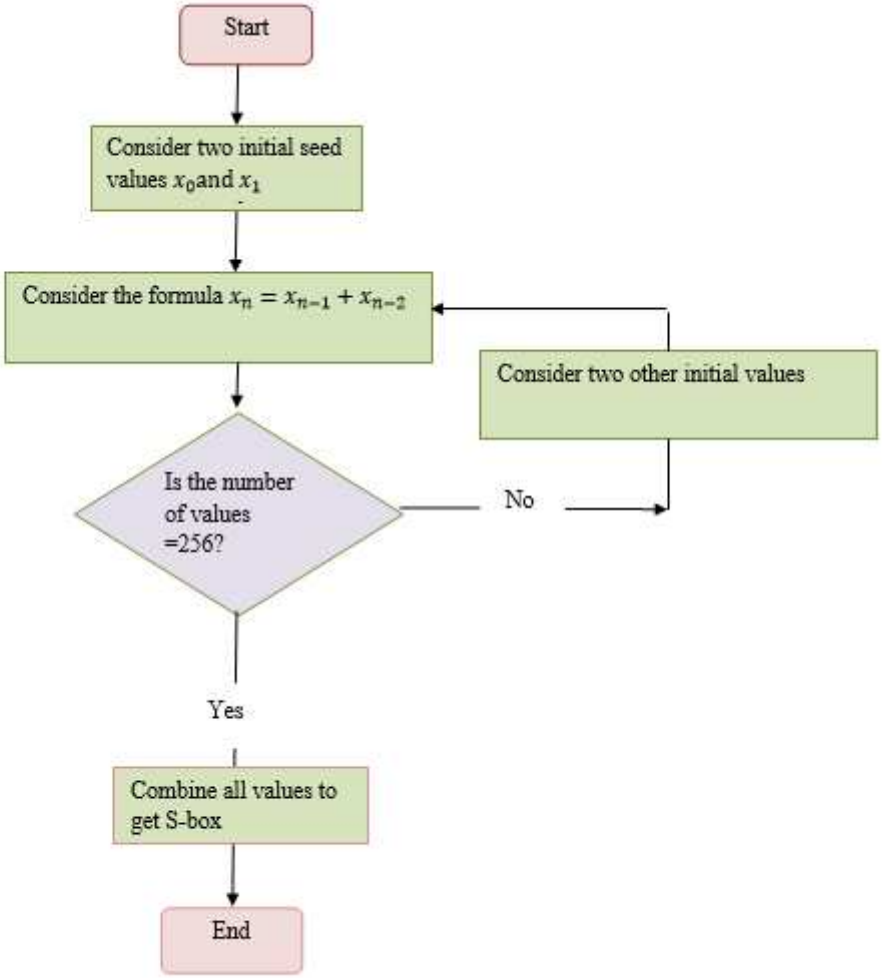


Figure 1

Flowchart Representation

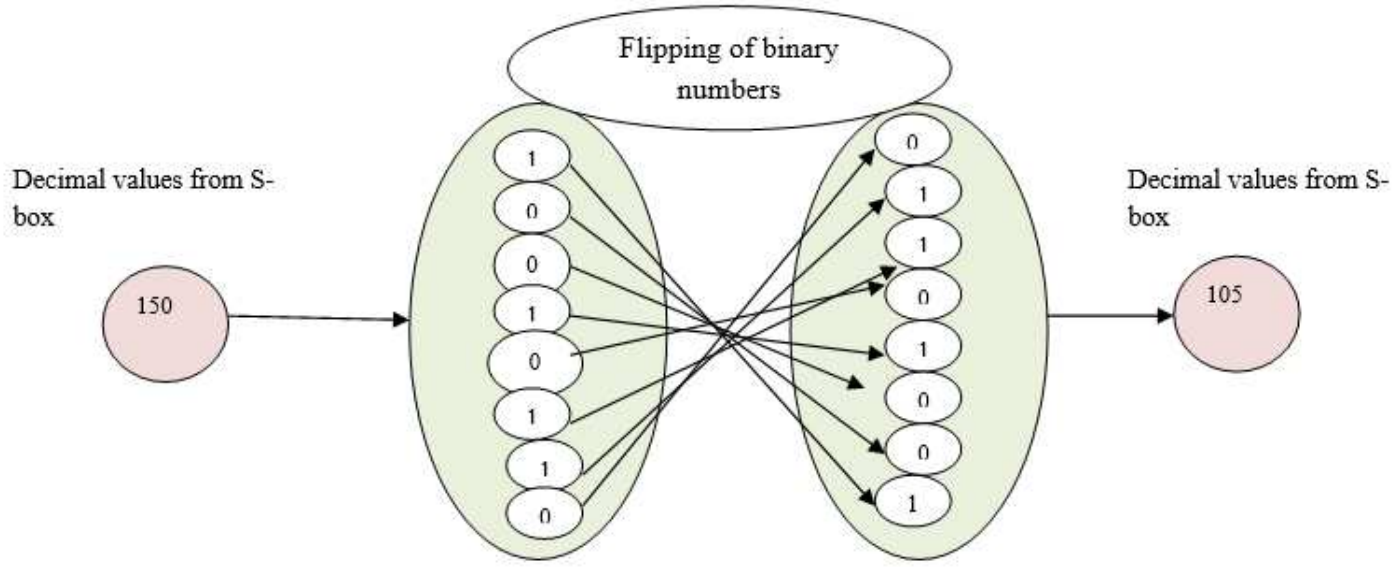


Figure 2

Flipping of numbers

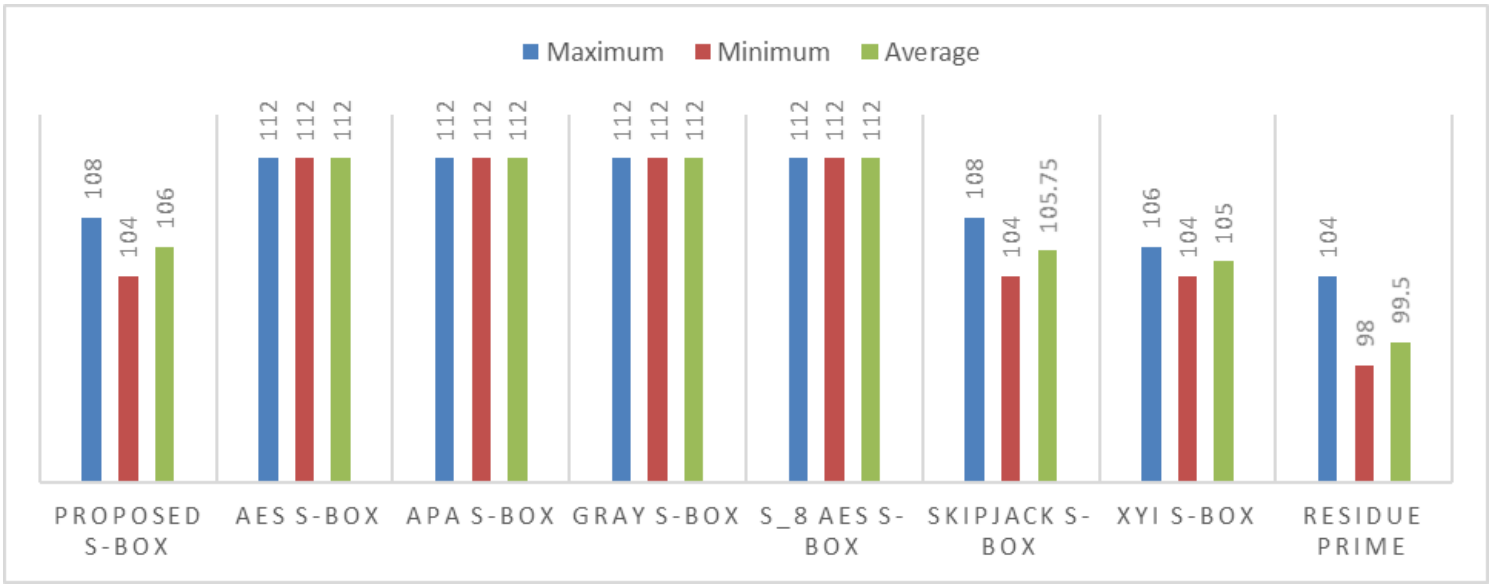


Figure 3

Non linearity

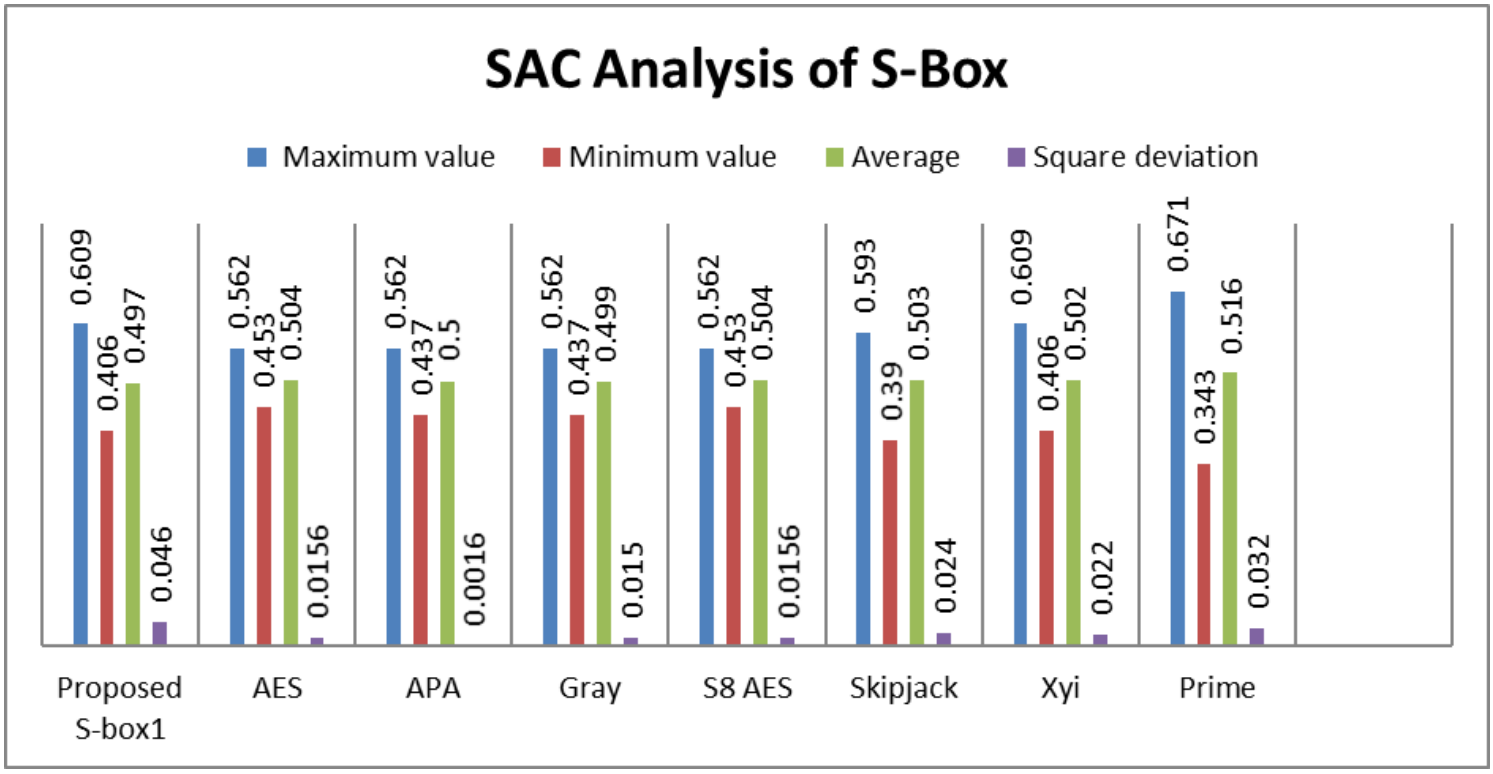


Figure 4

Strict Avalanche criterions

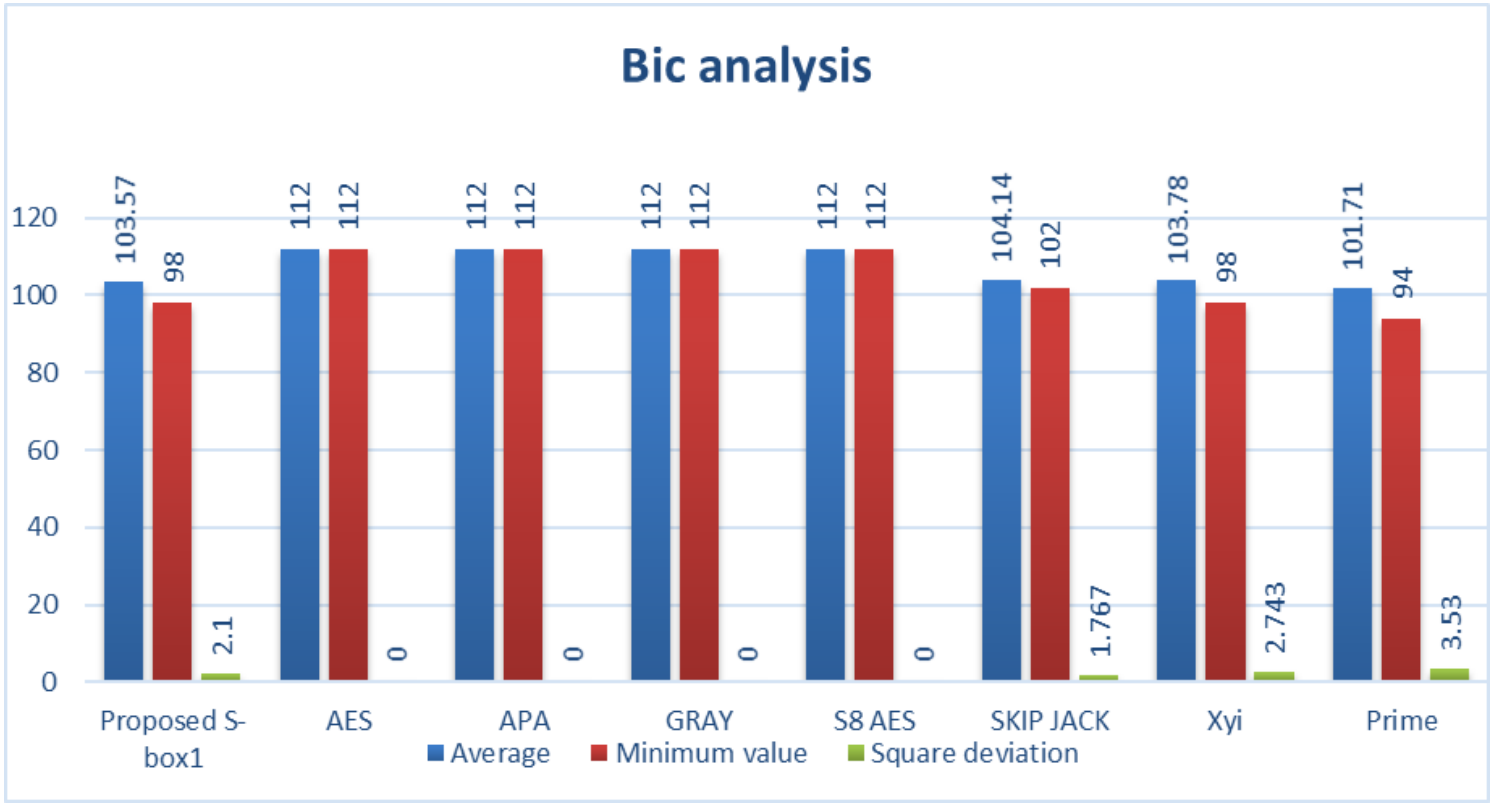


Figure 5

Bit Independence Criterion

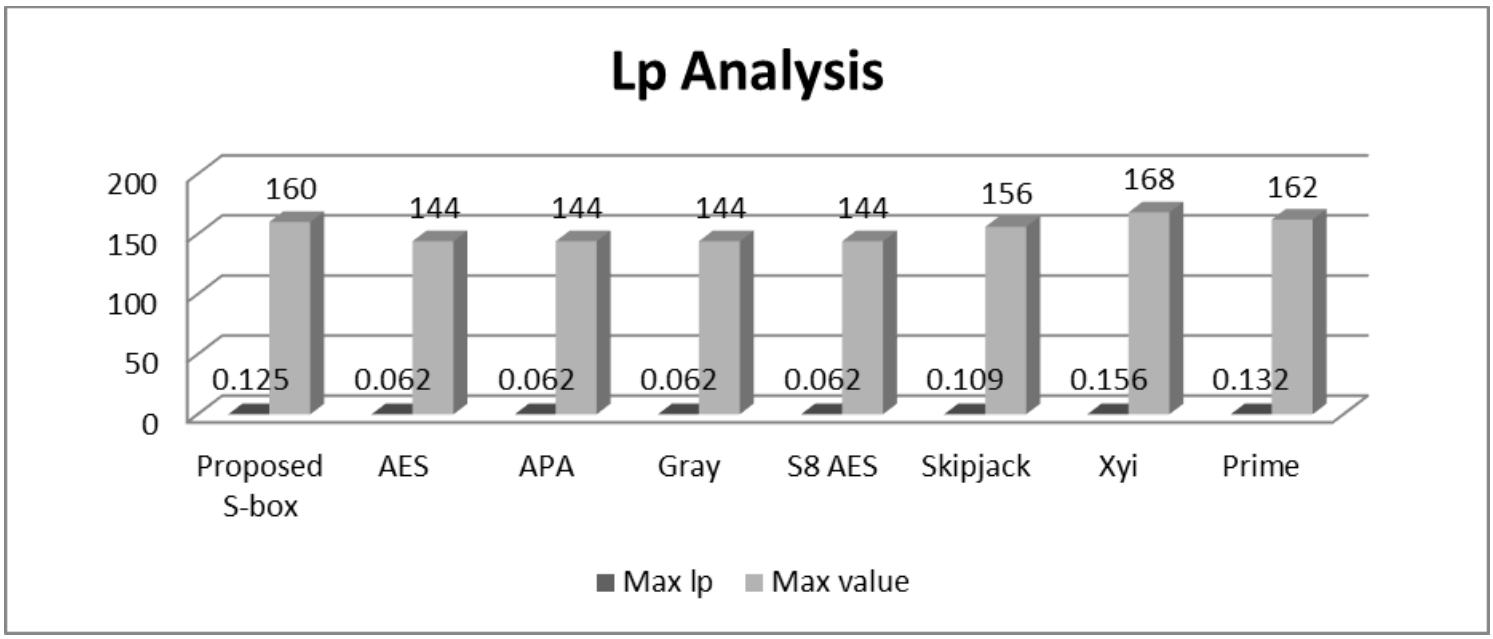


Figure 6

Linear Probability

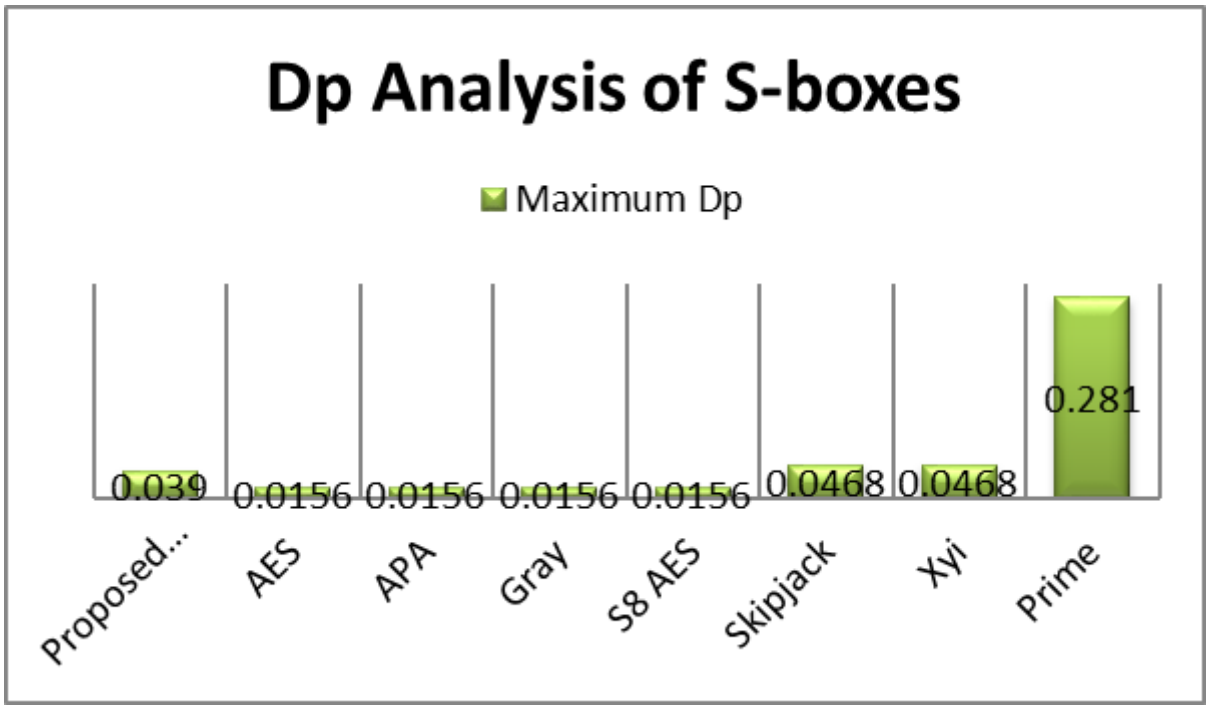


Figure 7

Differential probability

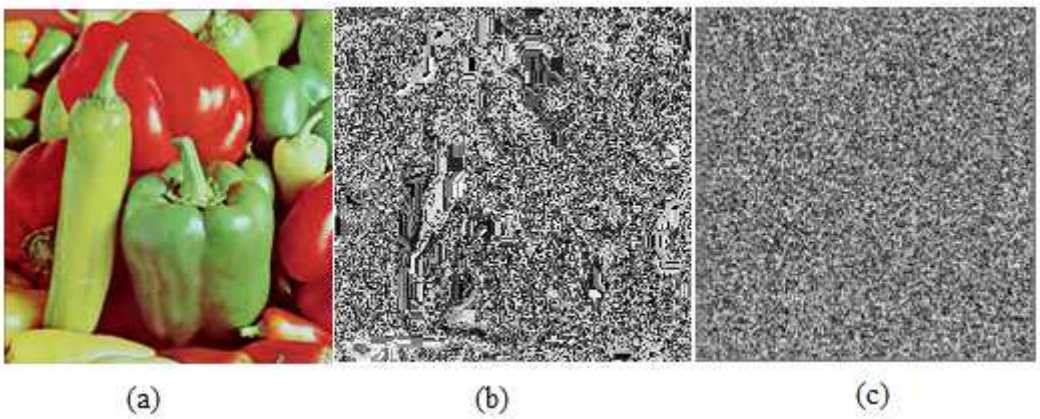


Figure 8

Capsicum Image Encryption (a) Original Image (b) First Round Encrypted Image and(c) Final Encrypted image