Design of S-Box using Combination of Chaotic Functions

Tanu Wadhera[1], Gurmeet Kaur[2]
[1]*Department of Electronics and Communication Engineering, Punjabi University, Patiala, India*
[2]*Department of Electronics and Communication Engineering, Punjabi University, Patiala, India*
[1]tanu1991libra@gmail.com
[2]farishta02@yahoo.co.in

Abstract*— The cryptographic and encryption algorithms are mainly employed to ensure the security of data. The usage of chaotic functions in these algorithms can further enhance the security because of their random and unpredictable character. These algorithms make use of substitution box(S-box). In this paper a chaos-based S-box has been proposed which provides more randomness to data. The proposed S-box has been checked against attacks.

***Keywords*— Chaotic functions, Piece-wise Linear map, Advanced Encryption Scheme, Data Encryption Standard, Substitution Box, FIPS-140.**

I. INTRODUCTION

The methods for providing security must be robust, effective and cheap ensuring ease of implementation. A variety of cryptographic and encryption algorithms have been established for providing security to the data. The Advanced encryption scheme (AES) has been considered as the most protected algorithm and has replaced DES (Data Encryption Standard) [1]. The encryption algorithms have substitution box (s-box) as the primary element in them [2]. S-box is an mxn matrix, where m bit input is given to s-box and n bit output is obtained from it [2]. The security of the algorithms and networks has been ensured by the two parameters which are [2, 3]:

- Diffusion: It deals with plain-text and cipher text. The cipher text characters depend upon either some or all of the plain text characters in diffusion.
- Confusion: It deals with cipher text and the key. The small change in key would change the entire cipher text leaving the intruder in confusion of finding the cipher text.

The s-box used in these algorithms has been constructed using multiplicative inverse and an affine transformation [3]. To enhance the security of these algorithms, s-box has been implemented using chaotic functions. The chaotic function's sensitivity to initial conditions, ergodicity, mixing and unpredictable behaviour, random nature has made these functions to be the first choice for cryptographic algorithms [3, 5]. The s-box constructed using chaotic functions have been found dynamic in nature as compared to the static s-box of encryption algorithms such as AES and DES [6]. In this paper a new method of generating s-box has been proposed using three different one-dimensional chaotic maps. The generated s-box has been statistically analysed and checked against attacks. In the first section chaotic functions used for generating s-box have been discussed. In the second section the proposed method for s-box generation has been discussed. In third section s-box has been statistically analysed using FIPS 140 test and checked for avalanche effect. In the last section conclusion of the paper has been drawn.

II. SELECTED CHAOTIC FUNCTIONS

One-dimensional chaotic functions because of their simplicity have been selected for construction of s-box [4]. The three simplest functions that have been used are:

A. *Piece-wise Linear chaotic Map*

The first map that has been selected for the construction of s-box is piecewise-linear map. The map can be given as [8]:

$$X_{n+1} = \begin{cases} \frac{X_n}{p} & 0 \le X_n < p \\ \frac{X_n - p}{0.5 - p} & p \le X_n < 0.5 \\ \frac{(1 - X_n - p)}{0.5 - p} & 0.5 \le X_n < 1 - p \\ \frac{(1 - X_n)}{p} & 1 - p \le X_n \le 1 \end{cases} \quad (1)$$

Where p lies in the interval [0, 0.5] and X_0 is the initial condition such that $0 < X_0 < 1$.

B. Logistic Map

The second map that has been selected is logistic map and can be given by the equation as:

$$Y_{n+1} = A.Y_n.(1 - Y_n) \quad (2)$$

where A is the system control parameter and Y_0 is the initial condition such that $0<Y_0<1$. The parameter A can have value between 3.57 and 4 to exhibit chaotic behavior.

C. Tent Map

The third chaotic map that has been selected is Tent map and can be given by the equation as:

$$Z_{n+1} = r.(1 - |1 - 2 * Z_n|) \quad (3)$$

Where μ is the system control parameter having value in between 0 and 1, Z_0 is the initial condition with $0 < Z_0 < 1$.

III. Proposed Method For Generation Of 8x8 S-Box And Statistically Testing

S-box can be constructed using a single chaotic map [9]. The multiple chaotic functions have been combined to generate s-box which not only increases the security but also the system complexity [10]. A number of methods have been used for generating s-box and every method is different in its own style. The method proposed here is based on a transformation (T) [11]. The values of functions X, Y, Z can be obtained as [11]:

$$X = \{x(n), n = 1, 2 \ldots N \quad (4)$$

$$Y = \{y(n), n = 1, 2 \ldots N \quad (5)$$

$$Z = \{z(n), n = 1, 2 \ldots N \quad (6)$$

Where N is the number of the iterations for which the value of X, Y, Z have been calculated. The transformation T has been applied over the chaotic series generated using equations (3), (4) and (5) to convert the series in to key series and have been given as [11]:

$$T_1(X) = \text{mod}(\text{round}(L(X - \min(X)/(\max(X) - \min(X))), 256) \quad (7)$$

$$T_2(Y) = \text{mod}(\text{round}(L(Y - \min(Y)/(\max(Y) - \min(Y))), 256) \quad (8)$$

$$T_3(Z) = \text{mod}(\text{round}(L(Z - \min(Z)/(\max(Z) - \min(Z))), 256) \quad (9)$$

Where $L=10^{15}$. The key series obtained from above equations (7), (8) and (9) have been converted in to binary form using [11]:

$$T(X) = \text{dec2bin}(T_1(X)) \quad (10)$$

$$T(Y) = \text{dec2bin}(T_2(Y)) \quad (11)$$

$$T(Z) = \text{dec2bin}(T_3(Z)) \quad (12)$$

The binary sequences obtained from the equations (10), (11) and (12) have been combined to form one sequence using XOR operation [11].

$$S = T(X) \oplus T(Y) \oplus T(Z) \quad (13)$$

$\oplus$ represents the XOR operation. The efficient use of random feature of the three chaotic maps and for easier implementation XOR has been used [3]. The values obtained from equation (13) have been stored in the S-box. The values must be unique in the S-box. Any of the value repeating has been left and next unique value has been stored. The number of iterations has been increased to obtain the unique values. The s-box obtained from this method is given in Table 1. The proposed S-box has been statistically analysed using FIPS140-2 test and checked for avalanche effect.

A. FIPS 140-2 Test

The FIPS 140-2 test is statistical test suite of NIST consists of 4 tests: Monobit test, Poker test, Runs test and long runs test [12]. These tests are executed on 20, 000 bits [12]. The random sequences have to pass all the tests [12].

B. *Avalanche Test*

It is the prime feature of encryption and cryptographic algorithms to ensure the security of these algorithms [3]. An algorithm has this effect if by complementing the single input bit, on an average half of the output bits changes [3]. The formula used for finding the avalanche value is [3]:

$$av(j)=S(x)\oplus S(x_j) \tag{14}$$

Where x and x_j differs in only one bit which will be jth bit. The two input values have been selected randomly which differ by one bit. The values corresponding to the bit position difference have been arranged in pairs. For the eight bit positions the pairs have been formed and the average of bits have been calculated.

Table 1: 8x8 S-box

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

Where x and x_j differs in only one bit which will be jth bit. The two input values have been selected randomly which differ by one bit. The values corresponding to the bit position difference have been arranged in pairs. For the eight bit positions the pairs have been formed and the average of bits have been calculated.

S-box has been widely used in many algorithms for image encryption, text encryption and cryptographic networks [2, 4]. The proposed s-box has been applied to a 160x160 image to produce the encrypted image. The encrypted image has been produced using the equation given by:

$$E=S \oplus I \tag{15}$$

Where E is the encrypted image, S is the proposed s-box and I is the original 160x160 image. The original image and the encrypted image have been shown in Fig.1 (a) and 1(b).

C. Statistical Analysis of Encrypted Image

1) Histogram Analysis

The analysis of histogram of original and encrypted image has been done in order to analyze the pixels of encrypted image [4].

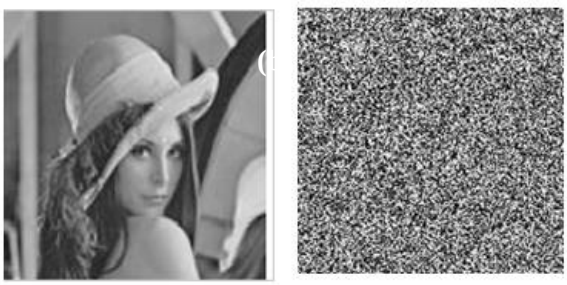


Fig. 1: (a) Original image and (b) Encrypted image.

The encrypted image must have the uniform division of pixels [4]. The parameter diffusion depends upon the uniformity of the pixels of the encrypted image [4]. The more the uniformity better will be the diffusion and hence more will be the security.

2) Entropy Analysis

Entropy is the measure of uncertainty [4]. The average information is provided by entropy [13]. The high entropy value will have high unpredictability making the access to unauthorized users a more difficult one. The entropy has been calculated using [4]:

$$H(a) = -\sum_{i=1}^{2^{N-1}} pa_i \log(a_i, 2) \tag{16}$$

Where a_i represents the pixel value and pa_i is the probability of that pixel [4]. The entropy value of a random image is 8 [4]. For highly random encrypted image the value of entropy must be near about the maximum value 8 [4].

3) *Correlation Coefficient Analysis*

This is the analysis of adjacent pixels to determine the features of texture of original image and in comparison of original, of the encrypted image [4]. The value of correlation should be very low. The lower the value the better will be the encryption method [4]. The highly correlated images have correlation coefficient value equal to ±1 [10].The formula for correlation coefficient can be given as [10]:

$$C(s1, s2) = \frac{\sum_{i=1}^{N}(xi-\mu(x))(yi-\mu(y))}{\sum_{i=0}^{N}(xi-\mu(x))^2 * \sum_{i=1}^{N}((yi-\mu(y))^2} \tag{17}$$

D. Results And Discussion

The results have been provided in the tabular and graphical form to make them clearer. The FIPS test result has been given in the form of a table. The FIPS 140-2 test has been performed on 20, 000 bits of the proposed s-box. The obtained values along with the required intervals and the accepted intervals at a significant level of α=0.0001 have been given in tabular form in Table 1. Figure 2 shows the avalanche criterion value of the proposed s-box against the standard required value.

TABLE 2
Results of FIPS-140 2 test suite.

Test Names	FIPS 140-2	Standard α=0.0001	Obtained Values
	Required Interval	Accepted Interval	
Monobit	9725~10725	9725~10725	10045
Poker	2.16~46.17	2.41~44.26	8.7104
Long Run	<26	<26	0
Run	K	K	
K=1	2315~2685	2362~2638	2576
2	1114~1386	1153~1347	1228
3	527~723	556~694	626
4	240~384	264~361	328
5	103~209	122~191	163
6+	103~209	122~191	148

The value of avalanche criterion is approximately equal to 4 for all the bit positions.

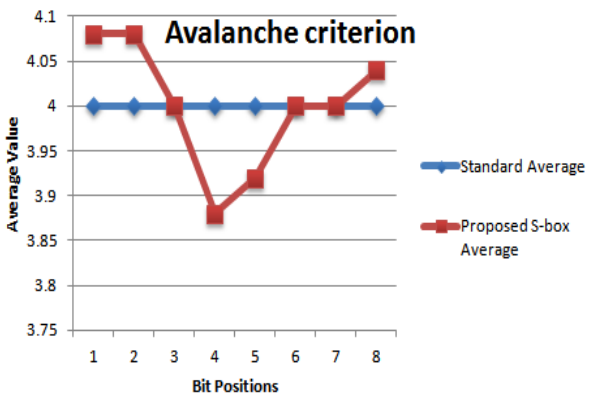
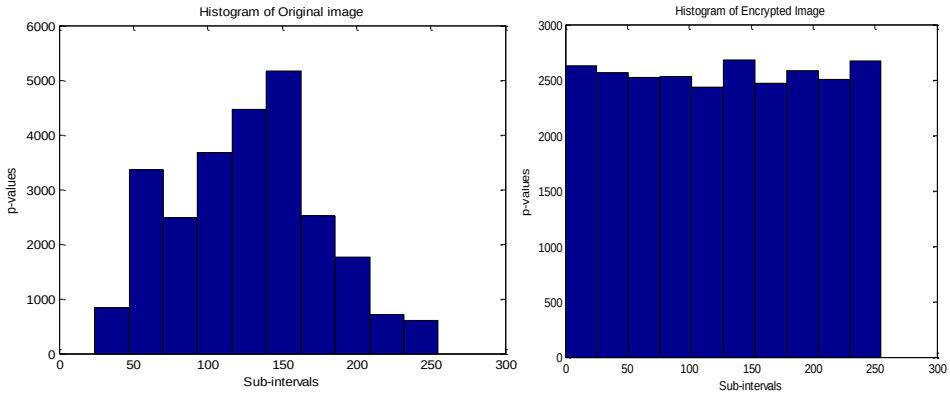


Fig.2: Avalanche effect curve against average value 4.

The uniformity of pixels in the encrypted image has been observed by plotting histogram of the encrypted image. Fig. 3 (a) shows the histogram of original and 3 (b) of encrypted image.



(a) (b)

Fig.3: Histogram of (a) original (Plain) image and (b) encrypted image.

The histogram of encrypted image is uniform and hence more secure. Fig.4 shows the comparison of entropy of original and encrypted image pixels.

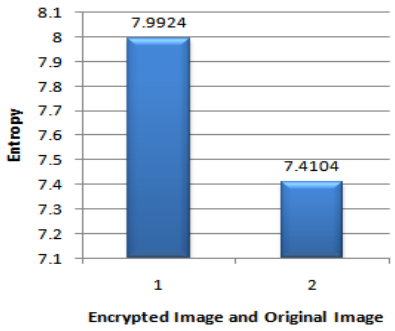


Fig.4: Comparison of encrypted and original image entropy.

The value of entropy for encrypted image is 7.9924 and for the original image is 7.4104. The values make it clear that encrypted image has much more entropy and it lies near to required vlue 8 as discussed in section 6. Table 3 shows the comparison of correlation coefficient between calculated vertically and horizontally. The horizontal and vertical value for plain image is 0.9854 and 0.9975. The horizontal and vertical coefficients for encrypted image are -0.0616 and 0.0595.

TABLE 3
Correlation coefficient :Plain Vs encrypted image.

Different Images	Vertical Correlation Coefficient	Horizontal Correlation Coefficient
Plain Image	0.9975	0.9854
Encrypted Image	0.0595	-0.0616

The values depicts that the encrypted image pixel values are less correlated as compare to the plain image. Thus, encrypted image ensures security.

IV. CONCLUSIONS

In this paper a s-box has been designed using combination of one-dimensional chaotic function. The proposed s-box has been statistically analyzed against attacks and has been applied for image encryption. The proposed s-box has passed all the tests successfully. The encrypted and original image has been compared and it can be concluded that encrypted image using proposed s-box is more secure.

REFERENCES

[1] M. Atteya, A. H. Madian, "*A Hybrid Chaos-AES Encryption Algorithm and Its Impelmention Based on FPGA"*, IEEE, pp. 217-220, 2014.
[2] J. Chandrasekaran, "*Ensemble of blowfish with chaos based S-box design for text and image Encryption*", International Journal of Network Security & its Applications (IJNSA), vol.3, no.4, pp.165-173, 2011.
[3] Rîncu and V. Iana, "S-Box Design Based on Chaotic Maps Combination" IEEE, 2014.
[4] M. Khan *et al*., "*Construction of S-box based on chaotic Boolean functions and its application in image encryption*", Neural Computing and Applications, Springer, 2015.
[5] A. Cristina et al., "*A New Pseudorandom Bit Generator Using Compounded Chaotic Tent Maps*", IEEE, 2012, 339-342.
[6] Ou, "*Design of block ciphers by simple chaotic functions*", IEEE Computational Intelligence Magazine, pp. 54-59, 2008**.**
[7] G. Zaïbi *et al*., "*On Dynamic chaotic S-Box*", IEEE, 2009.
[8] M. Asim, V. Jeoti, "*Efficient and simple method for designing chaotic s-boxes*", ETRI Journal, vol. 30, no. I, pp.170-172, 2008.
[9] M. François *et al*., "*A Fast Chaos-Based Pseudo-Random Bit Generator Using Binary 64 Floating-Point Arithmetic*", Informatic38, pp. 115-124, 2014.
[10] L. Min *et al.*, "Study on Pseudo-randomness of Some Pseudorandom Number Generators with Application", Ninth International Conference on Computational Intelligence and Security, IEEE, pp. 569-574, 2013.
[11] Security Requirements for Cryptographic Modules, Federal Information Processing Standards FIPS 140-2, March 12, 2002 [Online]. Available: http://csrc.nist.gov/publications/fips/fips1402/fips1402.pdf.
[12] K. Inayah and Rahmat Purwoko "*Insertion Attack effects on standard PRNGs ANSI X9.17 and ANSI X9.31 based on Statistical Distance Tests and Entropy Difference Tests"*, International Conference on Computer, Control, Informatics and Its Applications, IEEE, pp. 219-224, 2013.
[13] A. Vassilev and T. A. Hall, "*The Importance of Entropy to Information Security"*, IEEE Computer Society, pp. 78-81, 2014.