Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 04, April-2021

An Improved S-Box Generation Method using Metaheuristic Optimization Technique

Shubhankar Vashishta
Computer Science and Engineering
SRM Institute of Science and Technology Chennai, India

Lakshay Srivastava
Computer Science and Engineering
SRM Institute of Science and Technology Chennai, India

Dr. C. Jothi Kumar
Computer Science and Engineering
SRM Institute of Science and Technology Chennai, India

***Abstract*— Substitution boxes (S-boxes) are a crucial nonlinear component in modern block and stream ciphers' cryptanalytic resistance. Due to their relevance, there is a wide range of S-box construction techniques. The success of AES (Advanced Encryption Standard) posed cryptographers with new challenges in creating powerful substitution-boxes using various underlying approaches. There are various parameters that play a vital role in creating a robust S-Box that is secure enough to use which includes Nonlinearity, differential uniformity, absolute indicator value of global avalanche characteristics, Bits Independence Criterion (BIC), confusion characteristics, transparency order etc. We can obtain the desired value for a parameter by using various optimization techniques like PSO, GSA etc. In the proposed scheme, metaheuristic optimization technique will be used for setting the values of the above-mentioned parameters.**

Keywords*— *S-box, Particle Swarm Optimization, Gauss Iterated Map, Cryptography

I. INTRODUCTION

The protection of private data and visual information have been a major concern for years, given the transparent and vulnerable nature of Web and networking technologies. Since many years, the cryptographers have proposed different types of information protection methods. Depending on how information is interpreted encryption techniques can be divided into stream and block ciphers [1]. A block cipher is a method of text cryptography where the encryption key and algorithm are applied to the block of data at one time, called blocks, with an invariable transformation. The block cipher use permutation and replacement layers to design efficiency that shows high uncertainty and scattering properties. For such networks, substitution boxes are crucial components intended to convey the necessary nonlinear data transformation, that in turn contributes to better uncertainty and strength to various cryptographic attacks. The substitution process utilizes block bits for input and non-linearly converts them into various block bits for output [2]. It is indeed a linear conversion of the input sequence, as opposed to shuffling, which refers to the permutation process.

The advancement and improvement of proposals dedicated to the development of substitution boxes has contributed significantly to the success of the AES block cipher as well as its substitution box [3]. They are stable, with structures that emphasize on algebraic strategies, optimization, chaos function as well as structures, and so on. A dynamic and open problem is the design of effective and variable size S-boxes. The scale of the massively bulky search space is one of the essential causes of this difficulty. As a result, a chaotic metaheuristic optimization approach is constructed to develop a competent framework of an S-box with varying size that can produce effective S-boxes.

The initial conditions and control parameters of chaotic systems are highly sensitive to these systems, which is why they are regarded as good origin of entropy. They have strong responsiveness to preliminary constraints and system specifications, as well as quick auto-correlation and arbitrary nature of produced data [2][4]. Even small adjustments in the preliminary constraints and governing conditions have a significant impact on performance, making chaos-based structures ideal for the development of robust encryption algorithms. Chaos-based mechanisms on the other hand, can never exhibit chaotic behavior to every value of the preliminary constraints and governing conditions [5]. The chaos-based behavior of the selected scheme is the first requirement inside the architecture of chaotic encryption algorithms. Therefore, when choosing initial conditions and control parameters, caution must be taken. The chaos-based structures' preliminary constraints and governing conditions are real-valued in the interval in which they are described. And it has a vacuum of infinite value. Optimization algorithms are needed to pick the optimal chaos-based framework through this unlimited search space.

II. PRELIMINARIES

A. *S-box parameters*

1) Nonlinearity

The least separation of a Boolean function *f* to the collection of each affine function is used to calculate its nonlinearity measure [6]. As a result, standing nonlinearities scores should be reflected in the S-box constituent functions. The nonlinearity NL_{fn} for each Boolean function *fn* is evaluated with Eq. (1) [13]:

$$NL_{fn} = \frac{1}{2}\left(2^n - W_{max}(fn)\right) \qquad (1)$$

where, $W_{\max}(fn)$ is known as Walsh-Hadamard transform of Boolean function *fn* [7]. If a Boolean function has weak nonlinearity, it is called fragile. The increase of nonlinearity of stable Boolean functions is regarded as among the most important steps offering control resisting linear attacks [7]. Table I lists out the nonlinearity of the some the S-boxes

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 04, April-2021

used in this paper to compare the nonlinearity of the proposed scheme.

TABLE I. COMPARATIVE ANALYSIS OF NONLINEARITY OF 8 x 8 S-BOXES.

Substitution box	Nonlinearity (min)
Ref [17]	84
Ref [18]	98
Ref [19]	98
Ref [20]	100
Ref [21]	102
Ref [22]	102
Ref [23]	106

2) Differential Uniformity

The differential uniformity compares an S-Box's resistivity to differential cryptanalysis. Biham and Shamir defined the cryptanalysis attack technique, which involves creating a disparity in the I/O distribution for pupose of attacking block ciphers and S-boxes [8]. If the XOR value of every output has similar uniformity to the XOR value of every input, then the cryptanalysis can be completed [9]. When the input/output distribution of an S-box is uniform, it is said to be immune. In the XOR table, the greatest value of differential uniformity (DU) shall be kept low. DU of any Boolean function *fn(x)* can determined by [13]:

$$DU(S) = \max_{\delta a \neq 0, \delta b} (\#\{a \in A | S(a) \oplus S(a \oplus \delta a) = \delta b\}) \quad (2)$$

where set Y contains every possible input value and its components have a figure of 2^n. For an S-box, the largest value of the XOR table should be small enough to prevent cryptanalysis. Table 2 compares the differential uniformity of various chaotic substitution boxes.

TABLE II. COMPARATIVE ANALYSIS OF DIFFERENTIAL UNIFORMITY OF 8 x 8 S-BOXES.

Substitution box	Differential uniformity
Ref [17]	16
Ref [18]	12
Ref [19]	12
Ref [20]	14
Ref [21]	12
Ref [22]	10
Ref [23]	10

B. Gauss Iterated Map

Gauss Iterated map is one of the most popular 1-dimensional chaotic map. It is a simple function which displays chaotic behaviour with discrete time domain and real space domain [10]. It is dictated by the Eq. (3):

$$x_{n+1} = exp(-\alpha x_n^2) + \beta \quad (3)$$

where α and β are the control parameters which govern the bifurcation and x_n is the function variable. The Gauss Iterated map produces best results when the value of α is set between 4.5 to 8 and the value of β lies between -1 to 1 [11]. Figure 1 shows great chaotic characteristics of Gauss Iterated map for α= 6.2.

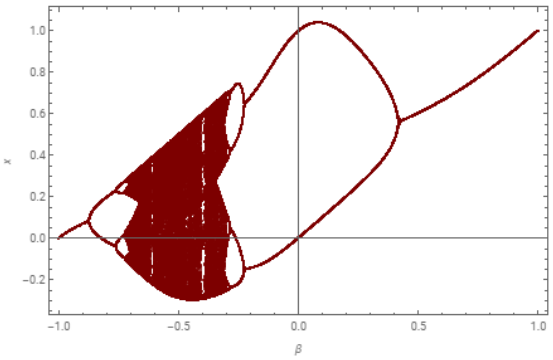


Figure 1. Bifurcation of Gaussian map at α= 6.2

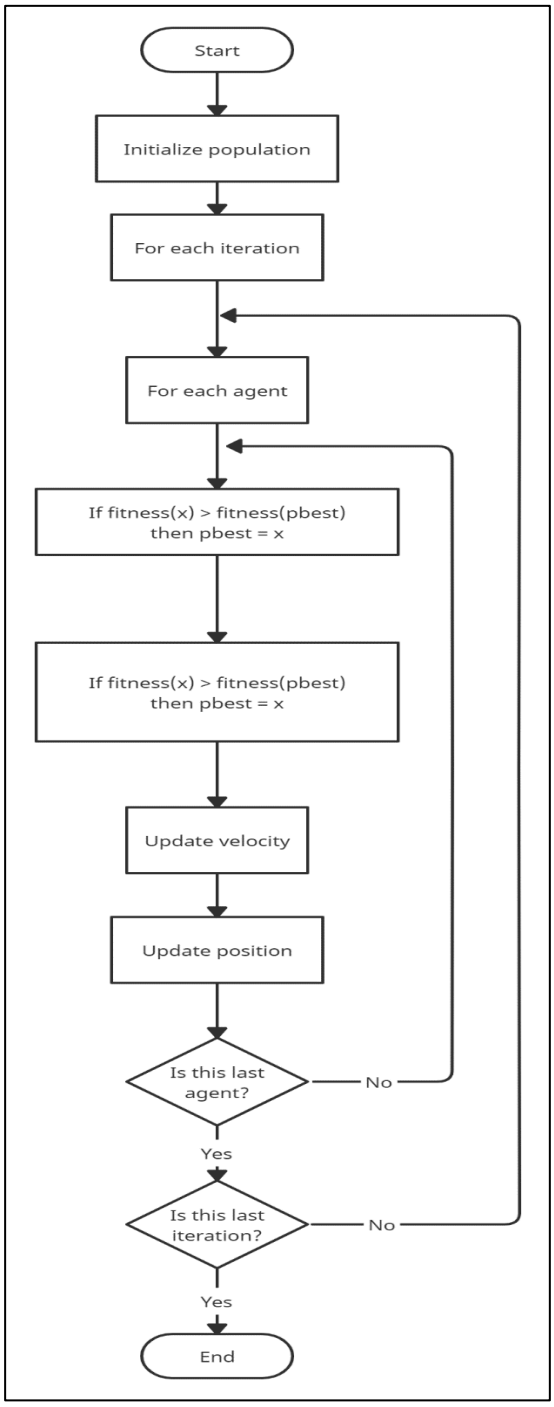


Figure 2. Flowchart of Particle Swarm Optimization.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 04, April-2021

C. Particle Swarm Optimization

Particle swarm optimization (PSO) is a metaheuristic optimization algorithm, that was proposed by Eberhart and Kennedy in the year 1995. The model was influenced by studying the behavior of fishes and birds. PSO has been used in a wide range of optimization problems, both alone and in conjunction with different algorithms [12].

Each particle obeys a specific path, being a positional vector that depends on time. Two major key pieces consist of the swarming particle's movement: a stochastic bit and a deterministic bit. By differentiating the paths of these discrete particles PSO explores the domain of an objective function. Every particle is drawn closer to the current global best position (g^*) and its personal best-known position (x_i^*) while at the same time showing a tendency to shift impulsively over time. The particle modifies the position as the best new particle present *i* when it finds a position that is better than any location previously found. At any given moment, at each iteration, there seems to be current best for every particle. The main goal is to discover the best global solution from all of the existing best solutions until they stop improving or after a certain amount of iterations.

Let the position vector and velocity be represented as x_i and v_i respectively for the i^{th} particle. The Eq. (4) defines the new velocity vector:

$$v_i^{t+1} = (w * v_i^t) + c_1 r_1 (x_i^* - x_i^t) + c_2 r_2 (g^* - x_i^t) \quad (4)$$

where x_i^t and v_i^t denotes the position and velocity of i^{th} particle at t times. r_1 and r_2 are two arbitrary vectors with values ranging from 0 to 1. The parameters c_1 and c_2 are the constants of acceleration, usually equal to, say, $c_1 \approx c_2 \approx 2$ for balanced approach in its stochastic and deterministic way. The initial positions of all the particles should be distributed sufficiently uniformly so that they can be sampled across most regions. We can then update the new location using the Eq. (5).

$$x_i^{t+1} = x_i^t + v_i^{t+1} \quad (5)$$

Here, v_i can take any value. However, it is generally bounded within a certain range [0, v_{max}].

III. PROPOSED WORK

The Gauss iterated map is used to spawn the first population of the S-boxes. The two parameters, α and β, are set to 6.2 and -0.38 respectively in Eq. (3). The reason for utilization of these particular values lies in the chaotic nature of the map. The gauss iterated map shows exemplary bifurcation for above specified values. The gauss iterated map is also used to achieve the control parameters, *k1* and *k2*, of the PSO. The research indicates that incorporating chaos through adjustment vector update contributes in a better search area exploration and use and can improve standard of the output influenced the chaos-based initialization and updating of PSO parameters [13]. Steps for the PSO technique are as follows:

A. Creating the vector of population:

Every distinct S-box is considered a single entity. Using chaotic maps, the initial population of S-boxes is created. The size of the original generated population is kept small according to the heuristics mentioned [14]. The initial population, i.e. N, is hence set to 40.

B. Setting the fitness parameter:

The fitness value for the problem is determined by a specific parameter. The nonlinearity of the S-box (particle) is observed as fitness value in the population vector in Eq. (4) and Eq. (5).

C. Initializing the vectors:

The adjustment vector is defined at the start and modified after each iteration. Each place vector initializes the values of the respective S-box in the sample. As per the Eq. (4), the adjustment vector is modified. For each S-box, the best personal vectors are determined. The recently created S-box in the sample which has a higher fitness value than the preceding S-box is updated as the personal best vector (pb_i). The S-box with the highest nonlinearity in the population is used to describe the global best vector (*gb*). The AES s-box is set as global best (*gb*) in Eq. (4). The nonlinearity for AES s-box comes out to be 112. The reason for selecting AES s-box for global best position is due to the fact that it is one of the most widely used s-box having extraordinary resistance to various cryptanalytic attacks.

D. Setting parameter values:

PSO parameters like r_1 and r_2 are kept contant at 0.9 in Eq. (4). The control constants, k_1 and k_2, are randomly initialised with the chaotic value provided by the 1-dimensional gauss iterated map for the Eq. (4). The selection of control parameters is left upon the chaotic map for increased unpredictability and dynamic range of output. During the optimization process, these parameters are modified after each iteration. The PSO inertial parameter *z* is initialised to a 0.7 in Eq. (4) for the best optimization results. This parameter helps in concentration of the S-boxes in accordance to the respective nonlinearities.

E. Preprocessing and Adjustment:

The Equations (4) and (5) are used to update the adjustment vector and S-boxes for each iteration. This procedure generates certain repeating and negative values. The solution values for the S-box architecture, on the other hand, are limited to a range [0,255]. As a result, we use a preprocessing and adjustment method to eliminate the possibility of repeating and negative values. Negative values are manifested in the desired range during preprocessing using some mathematics. To preserve the bijectivity of the S-boxes, we look for repeating values during the adjustment process and replace them with missing values [15]. The nonlinearity values are updated for the newly created sample. Optimum nonlinearities are maintained and sent to the recently updated sample, which is double the size (i.e. 80) of that of the original sample, from the current sample. pb_i and gb are revamped, as previously stated. Adjustment vector is denoted by a_i^t for the i^{th} S-box and t^{th} iteration.

Initial values for $x_{n+1} = exp(-\alpha x_n^2) + \beta$:

- Gaussian map initial value, $x_n = 0.231$
- Gaussian map parameters, $\alpha = 6.2$, $\beta = -0.38$

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 04, April-2021

$$a_i^{t+1} = (za_i^t) + 0.9k_1(pb_i - p_i^t) + 0.9k_2(gb - p_i^t) \quad (6)$$

- Inertial parameter, $z = 0.7$

In order to simulate, evaluate, and optimize the output of the proposed method of generating an S-box, we use the input arguments of the method proposed. The suggested approach is evaluated by changing sample range, iterations, and inertial parameter under various scenarios and conditions. The number of iterations for optimization is set as 100.

IV. PERFORMANCE ANALYSIS

A total of 4000 S-boxes were generated and optimized by particle swarm optimization technique. The S-box in Table IV is the best outcome among the generated S-boxes. For the values of various initial parameters, the minimum value of nonlinearity of S-box comes out to be 104. The same S-box displays the differential uniformity of 8. However another optimized S-box, show in Table V, with nonlinearity 102, displayed better differential uniformity with value 6.

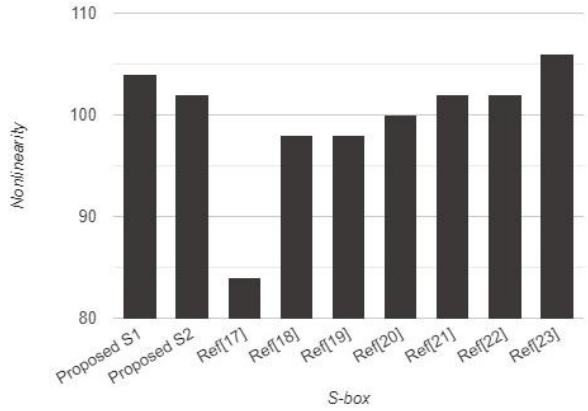
TABLE III. COMPARATIVE ANALYSIS OF PARAMETERS OF 8 x 8 S-BOXES.

Substitution box	Nonlinearity (min)	Differential Uniformity
Proposed S1	104	8
Proposed S2	102	6
Ref [17]	84	16
Ref [18]	98	12
Ref [19]	98	12
Ref [20]	100	14
Ref [21]	102	12
Ref [22]	102	10
Ref [23]	106	10

Various S-boxes from the literature are compared on the basis of nonlineaity and differential uniformity shown in the Table III**.** Figure 3 shows the competence of the S-box security scheme proposed in this paper. The fact that an S-box is bijective means that it is a one-to-one mapping. That is to say, all feasible resultant vectors shall emerge only once. Since each 256 possible resultant value is unique and show up one time, both S-boxes in Table IV and V preserve bijectivity. For S-boxes that are used in block ciphers.

One of the key problems in the world of cryptography over the last two decades has been the construction of extremely nonlinear S-boxes. By using the suggested PSO dependent approach, we can chieve S-boxes that are very similar to the 8x8 S-box with nonlinearity as high as 112 [16].

Differential cryptanalysis can be restricted for an S-box demostrating minimal DU [8]. Our S-boxes are measured with differential uniformities of 8 and 6 for S1 and S2, respectively. Table III. shows that the proposed S-boxes have greater capacity than other S-boxes to reduce differential cryptanalysis. The proposed S-boxes therefore have DU efficiency and demonstrate considerable resistance to differential cryptanalysis.



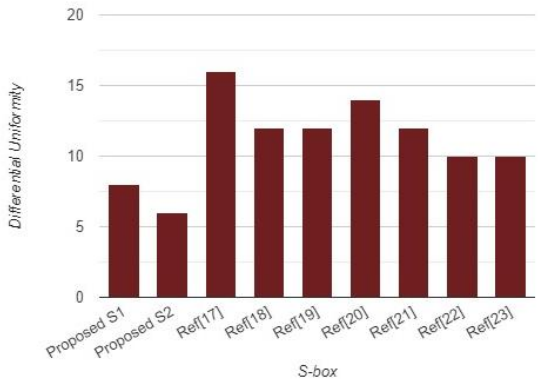


Figure 3. Comparison of nonlinearity

Figure 4. Comparison of differential uniformity

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 04, April-2021

TABLE IV. PROPOSED S-BOX S1

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

TABLE V. PROPOSED S-BOX S2

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

V. CONCLUSION

This paper implies that an effective optimisation-based S-box approach is an alternative to spontaneous and algebraic approaches. The S-boxes for high non-linearity as fitness value are developed with Particle swarm optimization. This approach uses the chaotic Gauss iterated map for original sample generation and other necessary arbitrary values. The procedure was investigated by changing the parameters of the PSO for various scenarios. The proposed method was shown to be capable of producing solid, well-encrypted S-boxes. Compared with many recent S-Boxes, the proposed S-Boxes have been found to be upstanding enough than many of their contemporaries. Thus it is possible to create strong non-linear S-boxes using the proposed technique.

VI. REFERENCES

[1] [1] Ya-Ping Zhang, Jizhou Sun and Xu Zhang, "A stream cipher algorithm based on conventional encryption techniques," Canadian Conference on Electrical and Computer Engineering 2004 (IEEE Cat. No.04CH37513), Niagara Falls, ON, Canada, 2004, pp. 649-652 Vol.2, doi: 10.1109/CCECE.2004.1345196.

[2] [2] M. Ahmad, E. Al-Solami, A. M. Alghamdi and M. A. Yousaf, "Bijective S-Boxes Method Using Improved Chaotic Map-Based Heuristic Search and Algebraic Group Structures," in IEEE Access, vol. 8, pp. 110397-110411, 2020, doi: 10.1109/ACCESS.2020.3001868.

[3] [3] Mohamed, Kamsiah & Pauzi, M N M Pauzi & Ali, Fakariah & Ariffin, Suriyani. (2014), "Study of S-box Properties in Block Cipher," I4CT 2014 - 1st International Conference on Computer, Communications, and Control Technology, Proceedings. 10.1109/I4CT.2014.6914206.

[4] [4] Z. Hua, B. Zhou and Y. Zhou, "Sine Chaotification Model for Enhancing Chaos and Its Hardware Implementation," in IEEE Transactions on Industrial Electronics, vol. 66, no. 2, pp. 1273-1284, Feb. 2019, doi: 10.1109/TIE.2018.2833049.

[5] [5] J. Sprott, Elegant Chaos Algebraically Simple Chaotic Flows. Singapore: World Scientific, 2010.

[6] [6] M. Ahmad, N. Mittal, P. Garg, and M. Maftab Khan, "Efficient cryptographic substitution box design using travelling salesman problem and chaos," Perspect. Sci., vol. 8, pp. 465–468, Sep. 2016.

[7] [7] W. Cusick and P. Stanica, Cryptographic Boolean Functions and Applications. Amsterdam, The Netherlands: Elsevier, 2009.

[8] [8] E. Biham and A. Shamir, "Differential cryptanalysis of Des. Like cryptosystems," J. Cryptol., vol. 4, no. 1, pp. 3–72, Jan. 1991.

[9] [9] M. Ahmad, C. Volos, M. Doja, and M. Beg, "A new hyperchaotic system-based design for efficient bijective substitution-boxes," Entropy, vol. 20, no. 7, p. 525, Jul. 2018.

[10] [10] K.Sakthidasan Sankaran, G.Ammu and V.Nagarajan, "Non Local Image Restoration Using Iterative Method", IEEE International Conference on Communication and Signal Processing-(ICCSP14), April 2014, pp. 1740 - 1744.

[11] [11] A. Sahay and C. Pradhan, "Gauss iterated map based RGB image encryption approach," 2017 International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 2017, pp. 0015-0018, doi: 10.1109/ICCSP.2017.8286437.

[12] [12] Yudong Zhang, Shuihua Wang, Genlin Ji, "A Comprehensive Survey on Particle Swarm Optimization Algorithm and Its Applications", Mathematical Problems in

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 04, April-2021

Engineering, vol. 2015, Article ID 931256, 38 pages, 2015. https://doi.org/10.1155/2015/931256.

[13] [13] M. Ahmad, I. A. Khaja, A. Baz, H. Alhakami and W. Alhakami, "Particle Swarm Optimization Based Highly Nonlinear Substitution-Boxes Generation for Security Applications," in IEEE Access, vol. 8, pp. 116132-116147, 2020, doi: 10.1109/ACCESS.2020.3004449.

[14] [14] Q. Bai, ''Analysis of particle swarm optimization algorithm,'' Comput. Inf. Sci., vol. 3, no. 1, p. 180, Jan. 2010.

[15] [15] Wang, Yong & Lei, Peng & Wong, Kwok-Wo, (2015), "A Method for Constructing Bijective S-Box with High Nonlinearity Based on Chaos and Optimization", International Journal of Bifurcation and Chaos, 25, 1550127,doi: 10.1142/S0218127415501278.

[16] [16] J. Daemen and V. Rijmen, The Design of RIJNDAEL: AES-The Advanced Encryption Standard. Berlin, Germany: Springer-Verlag, 2002.

[17] [17] D. Lambić and M. Nikolić, ''Pseudo-random number generator based on discrete-space chaotic map,'' Nonlinear Dyn., vol. 90, no. 1, pp. 223–232, 2017. doi: 10.1007/s11071-017-3656-1.

[18] [18] M. Khan, T. Shah, H. Mahmood, and M. Gondal, ''An efficient method for the construction of block cipher with multi-chaotic systems,'' Nonlinear Dyn., vol. 71, no. 3, pp. 489–492, 2013.

[19] [19] G. Jakimoski and L. Kocarev, ''Chaos and cryptography: Block encryption ciphers based on chaotic maps,'' IEEE Trans. Circuits Syst. I. Fundam. Theory Appl., vol. 48, no. 2, pp. 163–169, Feb. 2011.

[20] [20] G. Chen, Y. Chen, and X. Liao, ''An extended method for obtaining S-boxes based on three-dimensional chaotic Baker maps,'' Chaos Solitons Fractals, vol. 31, no. 3, pp. 571–579, 2007.

[21] [21] I. Hussain, T. Shah, and M. Gondal, ''A novel approach for designing substitution-boxes based on nonlinear chaotic algorithm,'' Nonlinear Dyn., vol. 70, no. 3, pp. 1791–1794, 2012.

[22] [22] G. Chen, ''A novel heuristic method for obtaining S-boxes,'' Chaos, Solitons Fractals, vol. 36, no. 4, pp. 1028–1036, 2008.

[23] [23] D. Lambić, ''A novel method of S-box design based on discrete chaotic map,'' Nonlinear Dyn., vol. 87, no. 4, pp. 2407–2413, 2017.