ISSN 2278-3091
Volume 10, No.4, July - August 2021
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse011042021.pdf
https://doi.org/10.30534/ijatcse/2021/011042021

A New Cryptography Scheme Based on Laplace Transform and a Substitution-Permutation Network

Abdoualwase M. Al-Azzani[1], Moammar. A. M. Rageh[2], Ghaleb H.Al-Gaphari[3]
[1,2,3]Faculty of Computer & Information Technology (FCIT),
Sana'a University, Sana'a, Yemen
[2]moammer07171@gmail.com
[1]amalezzani71@gmail.com
[3]drghalebh@gmail.com

ABSTRACT

The aim of cryptography is to convert plaintext into ciphertext which can be transmitted via insecure communication channels, so that, it impossible this ciphertext cannot be used for plaintext reproduction without knowing the corresponding key. Certain current Laplace transformation-based encryption methods have been proven to exhibit various security defects, such as the size of the secret key used for decryption usually greater than the size of the Plaintext, because that the secret key represents the quotient of Laplace transform values on 26, and these values larger than plaintext values. Therefore ,the encryption process is not important, as well as the possibility of obtaining the plaintext without knowing the secret key. To solve this problem, this paper proposes a new scheme cryptosystem based on Laplace Transform with using substitution boxes. The message is encrypted in many cycles, the secret key is added in each cycle and resultants values from the Laplace transform are substituting with the corresponding values from the substitution box that would be determined based on quotient and remainder values of Laplace transform values on block length. The security analysis and statistical results demonstrate that the proposed scheme provides a higher security level against different cryptographic attacks.

Keywords: S-Box, Laplace Transform, Cryptography, Remainder(R), Quotient(Q).

1. INTRODUCTION

Information security is a collection of procedures aimed at preventing unauthorized access or alterations to data. If the hacker somehow manages to break through the security firewall, passwords, and other measures taken to keep them out, cryptography becomes the only safeguard keeping them from reading protected data. So, cryptography helps individuals and organizations to protect their data. Two popular types of cryptography are: symmetric key and asymmetrickey. A symmetric or private key method is more efficient at translating large amounts of data and requires less computing power than an asymmetric key technique[18].A block cipher is one of the most critical components of symmetric cryptography. There is a type of popular block cipher is termed the substitution- permutation network (SPN)([11], [17]). These ciphers convert plaintext blocks using different numbers of rounds into respective ciphertext blocks. In each round, substitutions and permutations are performed on the input bits. A substitution operation uses a substitution box to replace one block of bits with another block of bits. The locations of the bits or bytes in the input block are modified by a permutation process. Block ciphers that use substitution and permutation operations include AES, SHARK, SQUARE, DES, and others. S-box and permutation are important components of a secure block cipher identified by Claude Shannon. The basic purpose of an S-box is the confusion that refers to making the relationship between the ciphertext and the secret key as complex and involved as possible, and the purpose of permutation is the diffusion that refers to dissipating the statistical structure of plaintext over blocks of ciphertext. S-box is an important nonlinear component used in block ciphers which significantly affects their security[17]. Substitution permutation network added property of confusion. So, finding the ciphertext key is difficult because any change in the key it will affect in the ciphertext[1].

A.P.Hiwarekar[9] presented a new scheme for block cipher purpose. The encryption process is based on series expansion of f(rt), multiplying said series with t^k, multiplying the numerical codes of the letters of a plaintext message with the coefficients of the first terms of the series. so that, alphabets decoded as set of 1,2,3,…,26. Then, determining the Laplace transform of the subsequent finite series, with a view of utilizing the resulting coefficients of the last series as the basis of the cyphertext. The ciphertext represents the resultants values modulo 26, the quotients obtained in the modular arithmetic represent the security key. In every encryption process, the sender must send the secret key to compute coefficients of the series. Decryption is done by inverse Laplace transform. Gupta and Mishra[8], Gençoğlu[6] showed that this scheme is a "weak" scheme because the encryption method is independent of the Laplace transform and ciphertext can be decrypted by elementary modular arithmetical arguments. Roberto.P, Briones[3]replaced the formulation of the encryption process by using the coefficients of n randomly selected terms from the infinite series for the plaintext of length n. In the literature, there are several articles on Laplace transform-based cryptography schemes ([5], [2], [12], [10], [13]).

This paper proposes a cryptographic method based on Laplace transform and substitution boxes and permutation vector. So that, first we compute the Laplace transform to series expansion after adding the plaintext values as coefficients for the series and adding the secret key for the resultant's values, then computing the remainder and quotient to produce the ciphertext. The ciphertext is a value from S-Box that corresponding to the row (it is place represents the quotient) and the column (it's place represents the remainder). Repeat all steps in each iteration with a different S-Box. Here we consider randomly bijective S-boxes generation methods and satisfying chosen selected criteria to build a substitution box. The rest of the paper organization is as follows. Section 2 presents the mathematical background. Section 3 explains the proposed method. Section 4 provides a numerical example to explain the steps of the encryption and decryption from the proposed method. Finally, Section 5, concludes the findings of this research paper.

2. BACKGROUND

2.1 The Laplace Transform

If $f(t)$ is a function defined for all positive values of t, then the Laplace transform of $f(t)$ is defined as

$$\mathfrak{L}(f(t)) = \int_0^\infty f(t)e^{-st}dt = F(s) \quad (1)$$

Where $|f(t)| < Me^{st}$ at $t \longrightarrow \infty$ and $M > 0$, Here the parameter s is a real or complex number**Error! Reference source not found.**.For example, if $f(t) = e^{3t}$ then,$\mathfrak{L}(f(t)) = \frac{1}{s-3}$, and $f(t) = t^4$ then $\mathfrak{L}(f(t)) = \frac{4!}{s^5}$.

The corresponding inverse Laplace transform is $\mathfrak{L}^{-1}(F(s)) = f(t)$ for example,

if $\mathfrak{L}^{-1}(F(s)) = \frac{1}{s-3}$ then,$f(t) = e^{3t}$.

if$\mathfrak{L}^{-1}(F(s)) = \frac{1}{s^5}$ then,$f(t) = \frac{t^4}{4!}$[7], [4].

2.2Maclaurin Series

The Maclaurin series for f about c is the power series

$$f(t) = \sum_{n=0}^{\infty} \frac{f^n(0)t^n}{n!}. \quad (2)$$

Such as, the function $f(t) = t^a sinh(t)$ has Maclaurin series as follows

$$t^a sinh(t) = t^{a+1} + \frac{t^{a+3}}{3!} + \frac{t^{a+5}}{5!} + \frac{t^{a+7}}{7!} + \ldots \quad (3)$$

So, when a=2, this function become

$$tsinh(t) = t^2 + \frac{t^4}{3!} + \frac{t^6}{5!} + \ldots \quad (4)$$

and the Laplace transformation for this function is

$$\mathfrak{L}(tsinh(t)) = \frac{2!}{s^3} + \frac{4!}{3!s^5} + \frac{6!}{5!s^7} + \ldots \quad (5).$$

2.3 Permutation Function

The permutation [14] is a rearrangement of the elements of the function f from a set D into a set C is a map with first input from D and output from C such that each element of D has a unique output. $f: D \longrightarrow C$ is one-to-one if $f(x) = f(y) \Longrightarrow x = y$. The function$f$ is onto if for each element$c \in C$, it is true that there is $d \in D$ with f(d) = c. $f: D \longrightarrow C$ called a bijection if it is both one-to-one and onto. The number of permutations on a set C of N elements given N! permutations.

3. THE PROPOSED CRYPTOGRAPHY SCHEME

The proposed cryptography scheme introduced a symmetric block cryptosystem for data encryption and decryption based on Laplace transform. This scheme differs from the previous in the following: It does not need to send the quotient with ciphertext, encryption is implemented with many iterations, the secure key is added in each iteration, and using a different S-Box in each iteration for production a new ciphertext.

3.1 Encryption Algorithm

The encryption process goes through two steps:-

1) The sender and the receiver agree on the following :-
   a) Length of block ($called \quad m$).
   b) Number of cycles($called \ N$).
   c) Secret key as a vector. $Key =< k_1, k_2, \ldots, k_m >$.
   d) Randomly selected Maclaurin expansion terms of a function $f(t)$ are as a secret vector. For instance, for the function $f(t) = tsinh(t)$ in (4), the selected terms(called Rn)$Rn =< 2, 4, 1, 5, 11, 9, 6, 8, 7, 13, 14, 10, 19, 12, 20, 21 >$, with length 128-bits (m=16), consequently, the correspondingselected function termsof Rn are

$$f(t) = \frac{t^4}{3!} + \frac{t^8}{7!} + \frac{t^2}{1!} + \frac{t^{10}}{9!} + \frac{t^{22}}{21!} + \ldots + \frac{t^{42}}{41!}. \quad (6)$$

So, we can rewrite the function f(t) as

$$f(t) = \sum_{i=1}^{m} \frac{t^{2*Rn(i)}}{(2*Rn(i)-1)!}. \quad (7)$$

   e) A vector for the permutation (called Pv) $Pv =< Pv_1, Pv_2, \ldots, Pv_m >$.
   f) Building number of S-Boxes (equal to number of cycles(n)), where elements of each S-Box are distinct and randomly selected values. As shown in(Table 1). S-boxes can be defined algebraically,where the algebraic formulation involves operations in a finite field.The substitution boxes are attached as fileswith both the sender and receiver, where S-boxescan rebuilding at any time.

2) Encryptionprocess**:**The encryption algorithm consists of many phases. In the first phase, the plaintext is divide into block (as ASCII coding) with length(m). In the second phase, computing Laplace transformfor the terms of selected Maclaurin expansion with incorporate(via a simple exclusive-or operation) ASCII values as coefficients.

$$f(t) = \sum_{i=1}^{m} \frac{(2*Rn(i))!}{(2*Rn(i)-1)!\, s^{2*Rn(i)+1}} = \sum_{i=1}^{m} \frac{P'}{s^{2*Rn(i)+1}}$$

$$where \quad P' = P \oplus \left(\frac{(2*Rn(i))!}{(2*Rn(i)-1)!} \right).$$

Then, the permutation vector permute each character(byte) in first block and adding the secret key to the resultants values by the XOR operation $P_i' = P \oplus key(i)$. In the third phase, the resultants values are adding to Laplace transform values by XOR operation$P_i'' = P_i' \oplus LT_i$. In the last phase, calculate R

and Q, where $R = mod(P_i'', m)$ and $Q = quotient(P_i'', m)$ and substitute this value with a value from the first S-Box that would be determined by the intersection of the corresponds to the row with index (Q) and the column with index (R). Repeat all phases(n cycles) with a different S-Box, as in algorithm(3). We can use same the S-box in each cycle, instead of using the K different S-boxes in ncycles.

Algorthim of Encryption-

Input: Plaintext(P), key, n, m, randomly Maclaurin terms(Rn), S-Box, the permutation vector(Pv).
Output: CipherText(C)

1) Dividethe plaintext (message/image) into blocks, each block with length(m).
2) Convert each block in Plaintext into ASCII coding.
3) For $k = 1$ to N(number of cycle)
   a) For $i = 1$ to n (number of block)
   b) Use permutation(Pv) to transposition each byte in block(i);
   c) For $j = 1$ to m (m represent block length)
      i) Compute $P'_{ij} = (P_{ij} \oplus key_j)$.
      ii) Compute Laplace transform
      $$LT_{ij} = P'_{ij} \oplus \left(\frac{(2*Rn(i))!}{(2*Rn(i)-1)!}\right).$$
      iii) Compute R and Q
      $R = LT_{ij}(mod \quad m)$.
      $Q = floor(LT_{ij}/m)$.
      iv) Generate C_{ij} from S-Boxi. where $C_{ij} = SBoxi(Q, R)$ "the element in row (Q) and column(R)".
   d) End for (j)
   e) End for (i)
   f) If K< Iteration then $P_k = C_k$ (for again encryption process)
4) End for (k)

End algorithm.

3.2 Decryption Algorithm

Receiver receives the encrypted text publicly, the secret key, the permutation vector, and randomly selected Maclaurin expansion terms, while previously preserved substatutation Boxes . The decryption is done as to thefollowing algorithm:

Algorthim of Decryption-

Input: Ciphertext(C), key, m, randomly Maclaurin terms(Rn), S-Box, the permutation vector(Pv), cycles(K)
Output: PlainText(P)

1) Divide the ciphertext into blocks, each block with length(m).
2) Convert each block in ciphertext into ASCII code.
3) For k= N to 1 (starting from last S-Box)
g) For i= 1 to n (number of blocks)
   i) For $j = 1$ to m
      - Finding the row and the column where the element C''_{ij} in it.
      $[Q, R] = find(S - Box_k == C_{ij}'')$ the row (Q) and the column (R).
      - Compute LT values from the equation $LT_{ij} = R + Q * m$.
      - Compute $P'_{ij} = \left(LT_{ij} \oplus \left(\frac{(2*Rn(i))!}{(2*Rn(i)-1)!}\right)\right)$.
      - Compute $P_{ij} = (P'_{ij} \oplus key)$.
   ii) End for (j).
h) End for (i).
i) Use the invers of the permutation vector (Pv) to transposition each byte in block(i).
j) Convert C_k=$P_k$for again becryption.

4)End for (k).

End*a*lgorithm.

4. NUMERICAL EXAMPLE

Let us assume that it was agreed between both the sender and the receiver that the length of the block is 128 bits (m = 16) and the number of cycles is ten(n=10) and that randomly selected Maclaurin expansion terms as in(6). Therefore, the terms that are selected for finding the Laplace transform as in(8)where $Rn =< 2,4,1,5,11,9,6,8,7,13,14,10,19,12,20,21 >$, and let the key be $key =< 9,5,16,1,6,11,10,15,2,8,3,4,14,13,12,7 >$, and the permutation vector is $Pv =< 4,1,6,11,10,14,13,12,7,15,9,5,16,2,8,3 >$,of 128-bits.So, the initial values are m,n, K, Rn,Pv, and key.These initial values are considered as secret keys of the proposed encryption algorithm.

4.1 Encryption Algorithm

Lets us assume that the plaintext is P="Success#89%0A". First, the plaintext is permuted based on Pv vector as P="cSs9&%s08eAu#c" the ASCII coding is P=[99,83,115,64,57,38,94,37,115,48,56,101,65,117,35,99]. Next, we compute $P' = P \oplus key$ for each character in the block, the resultants values are P'=[106,86,99,65,63,45,84,42,113,56,59,97,79,120,47,100]. After that, adding the resultants values as coefficients for per-selected function terms by XOR operator and compute Laplace transform, the results are

$$\mathfrak{L}(f(t)) = \frac{110}{s^5} + \frac{87}{s^9} + \frac{101}{s^3} + \ldots + \frac{103}{s^{43}} \quad (8)$$

we rewrite the coefficients as a vector P"=[110,87,101,74,53,35,89,38,118,55,50,100,95,122,39,103].Finally, the ciphertext is the value from the first S-box1(see Table 1) that would be determined by the intersection of the corresponds to the row with index $\left(Q = floor\left(\frac{P''}{m}\right)\right)$ and the column with index $\left(R = P''(mod \quad m)\right)$.For instance, the ciphertext C_{11} is the value in S-Box1(see Table 1) that corresponds to the row $Q = floor(P''_{11}/8) = floor(110/16) = 6(6^{th} row)$, and the column $R = P''_{11}(mod \quad 16) = 110(mod \ 16) = 14(14^{th} column)$ that is $C_{11} = 249$ and so on. So, the first ciphertext from S-Box1 is C_1 =[249,88,165,191,41,6,142,104,34,112,20,72,19,175,147,181]. In the second cycle, the values of C1 become as plaintext, and repeat the previous steps, with S-Box2. The ciphertext that is resulting from the second cycle is

C_2 =[230,32,220,45,58,162,243,110,243,170,116,138,48,66,232,61] and so on. Into the last cycle, the values of ciphertext areC=[88,247,91,138,134,237,154,55,58,171,240,42,140,147,59,132].Figure 1: Ciphertextshows the ciphertext messages for all cycles:

C1=“ ùıkLFÔ,SSŚ5ŞO˘6Ęè”
C2=“ æ␣Ü-:cónółtŁ0Bè=”
C3=“ ă_óõã‘|!ŮÌůÂAĂËę”
C4=“ *,,ÿNlÅç<éOű(râïÍ”
C5=“ \ŔźÞ°řžôBflkñõĎ§”
C6=“ YšŮ˘Du_éJSÿ7-kÕ¸”
C7=“ u,Š3"(ë˝.eŃ,␣Íýî”
C8=“ ijbÖŐÅŒÕ_@˘ŽĄśØ+”
C9=“ À§ÖoŰÞi˘¨IŁÃ&y<Š”
C10=“ Xœ[ŁĘíŽ7:ńð*ŇŞ;Ď”

Figure 1: Ciphertext for all cycle

4.2 Decryption Algorithm

First, the ciphertext(C) is divide into blocks with length 128-bit ($m = 16$), that is C=[88,247,91,138,134,237,154,55,58,171,240,42,140,147,59,132]. Next, the plaintext is computing from the equation $P = R + Q * m$ where R represents the column and Q represents the row from the last S-Box(Table 2) that is corresponds value of ciphertext. For instance, the value $C''_{11} = 88$ is in 6^{th} row and 2^{sd} column. So, $P_{11} = 2 + 6 * 16 = 98$. the values for all character areP=[98,205,204,129,89,96,32,220,101,46,21,134,186,138,35,251]. After that, applying the inverse of Laplace transform

$$\mathfrak{L}^{-1}(F(s)) = \mathfrak{L}^{-1}\left(\sum_{i=1}^{m} \frac{P' * t^{2*Rn(i)}}{(2 * Rn(i))!}\right)$$

where $P' = P \oplus \left(\frac{(2*Rn(i))}{(2*Rn(i)-1)}\right)$.

The resultants valuesareP' =[102,197,206,139,79,114,44,204,107,52,9,146,156,146,11,209]. Then, compute $P'' = P' \oplus Key$ for each characters in the block. The resultants values are P'' = [111,192,222,138,73,121,38,195,105,60,10,150,146,159,7,214]. Finally,we apply the inverse permutation veector on P” the results are P=[192,159,214,111,150,222,105,7,10,73,138,195,38,121,60,146]. Repeat the previous steps ten cycles. Figure 2shows the ciphertext messages for all cycles

P1=“ Xœ[ŁĘíŽ7:ńð*ŇŞ;Ď”
P2=“ À§ÖoŰÞi˘¨IŁÃ&y<Š”
P3=“ ijbÖŐÅŒÕ_@˘ŽĄśØ+”
P4=“ u,Š3"(ë˝.eŃ,␣Íýî”
P5=“ YšŮ˘Du_éJSÿ7-kÕ¸”
P6=“ \ŔźÞ°řžôBflkñõĎ§”
P7=“ *,,ÿNlÅç<éOű(râïÍ”
P8=“ ă_óõã‘|!ŮÌůÂAĂËę”
P9=“ æ␣Ü-:cónółtŁ0Bè=”
P10=“ ùıkLFÔ,SSŚ5ŞO˘6Ęè”

Figure 2: Plaintext after decryption process

Finally, adding secret key to P10 and applying the vector of permutationonthe results. The plainttext are P=“Success#89%0A”.

5. SECURITY AND STATISTICAL ANALYSIS

The MATLAB 2018 programming environment used to perform images encryption and analyze the results of the computer simulations. The picture database CVG-UGR was used to select Baboon image(256x256).

To analyze the quality of the proposed scheme, we used the majority logic criterion(MLC)[15]. To evaluate strength and robustness of the scheme in image encryption,this analytical criterion based on statistical studies such as entropy, correlation, homogeneity, contrast, and energy analysis. This analysis are used to determine the image encryption strength of an S-box.

The Baboon plaintext image is encrypted with three cycles.Figure 3shows the pictorial representation of the Baboon plain-image(1.a) and encrypted image using cycle1(1.b), cycle2(1.c), and cycle3(1.d). While theFigure 4shows the corresponding histograms of plain-image(2.a) and encrypted-image using cycle1(2.b), cycle2(2.c), and cycle3(2.d).

Table **3**. shows the MLC of the plain and encrypted Baboon images for proposed scheme and different renown schemes and their corresponding readings.

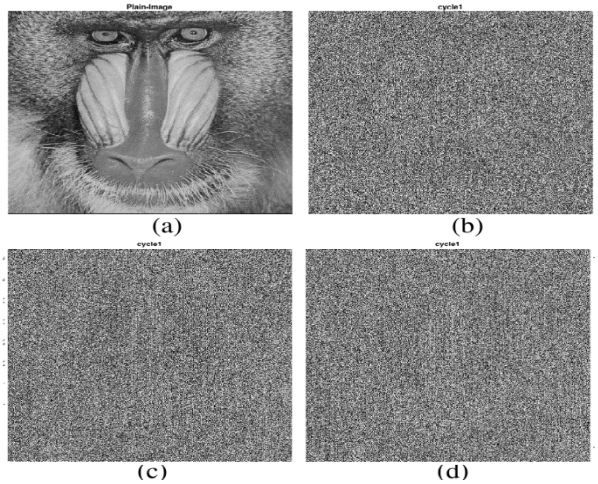

Figure 3 . (a)Baboon image, (b)Encrypted Baboon image using S-box1, (c)Encrypted Baboon image using S-box2, (d) Encrypted image using S-box3**.**

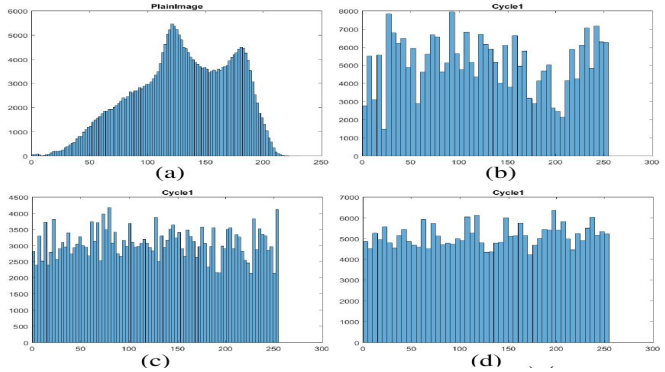

Figure 4. (a) Histogram of plain Baboon image. (b) Histogram of encrypted Baboon image using S-box1. (c)Histogram of encrypted Baboon image using S-box2. (d) Histogram of encrypted Baboon image using S-box3.

Table 1: Substitution Box 1(first S-Box)

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

Table 2: Substitution Box 10(last S-Box)

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

Table 3: Comparison of statistical analysis parameters obtained for plain and encrypted Baboon images.

Images	Entropy	correlation	Energy	Contrast	Homogeneity
PlainImage	7.358	0.830	0.089	0.617	0.787
CipherImage(cycle1)	7.4881	0.0041	0.0164	10.2438	0.3940
CipherImage(cycle2)	7.9514	0.0041	0.0156	10.2225	0.3918
CipherImage(cycle3)	7.9601	-0.0040	0.0156	10.5632	0.3879
AES	7.358	0.014	0.0160	10.50	0.400
Ref([16])	7.358	0.026	0.016	9.849	0.402

6. CONCLUSION

1. Substitution boxes added to increase the security, so thatthe breaking of the cryptosystem became difficult because the ciphertext and the plaintext having no relation directly.
2. In each cycle, after computing Laplace transform values, the quotients and remainder values are calculated, and replacing with a value from the S-Box. Therefore, the sender does not need to send quotient values with every encryption process, as in the previous cryptographic schemes based on integral transformations.

REFERENCES

1. Ammar S Alanazi. **A dual layer secure data encryption and hiding scheme for color images using the three-dimensional chaotic map and lah transformation.** *IEEE Access*, 9:26583–26592, 2021.
2. R Bhuvaneswari and K Bhuvaneswari**. Application of yang transform in cryptography.** *International Journal of Engineering, Science and Mathematics*, 9(3):41–45, 2020.
3. Roberto Pulmano Briones. **Modification of an encryption scheme based on the laplace transform.** *International Journal of Current Research*, 10(7):71759–71763, 2018.
4. Lokenath Debnath and Dambaru Bhatta. ***Integral transforms and their applications.*** CRC press, 2014.
5. MuharremTuncayGencoglu**. Embedded image coding using laplace transform for turkish letters.** *Multimedia Tools and Applications*, 78(13):17521–17534, 2019.
6. M TuncayGençoğlu. **Cryptanalysis of a new method of cryptography using laplace transform hyperbolic functions.** *Communications in Mathematics and Applications*, 8(2):183–189, 2017.
7. BS Grewal. ***Higher engineering mathematics***, khanna pub, 2005.
8. Praneesh Gupta and Prasanna Raghaw Mishra. **Cryptanalysis of "a new method of cryptography using laplace transform".***In Proceedings of the Third International Conference on Soft Computing for Problem Solving*, pages 539–546. Springer, 2014.
9. AP Hiwarekar. **A new method of cryptography using laplace transform.** *International Journal of Mathematical Archive*, 3(3):1193–1197, 2012.
10. Binoy Joseph and Bindhu K Thomas. **A new (k, n) secret sharing symmetric-key cryptographic method using ascii conversion and laplace transforms.***Malaya Journal of Matematik (MJM)*, 8(3), pp.1203—1205, 2020
11. Dragan Lambić and MiodragŽivković**. Comparison of random s-box generation methods.***Publications de l'institutmathematique*, 93(107):109–115, 2013.
12. G Nagalakshmi, A Chandra Sekhar, and D Ravi Sankar. **Asymmetric key cryptography using laplace transform.***International Journal of Innovative Technology and Exploring Engineering*, 2020
13. G Nagalakshmi, A Chandra Sekhar, N Ravi Sankar, and K Venkateswarlu**. Enhancing the data security by using rsa algorithm with application of laplace transform cryptosystem.** *International Journal of Recent Technology and Engineering*, 8(2), 2019
14. Abdul Razaq, Hanan A Al-Olayan, Atta Ullah, Arshad Riaz, and Adil Waheed. **A novel technique for the construction of safe substitution boxes based on cyclic and symmetric groups.** *Security and Communication Networks*, 2018.
15. Tariq Shah, Iqtadar Hussain, Muhammad Asif Gondal, and Hasan Mahmood. **Statistical analysis of s-box in image encryption applications based on majority logic criterion.** *International Journal of Physical Sciences*, 6(16):4110–4127, 2011.
16. Nasir Siddiqui, Fahim Yousaf, Fiza Murtaza, Muhammad Ehatisham-ul Haq, M Usman Ashraf, Ahmed M Alghamdi, and Ahmed S Alfakeeh. **A highly nonlinear substitution-box (s-box) design using action of modular group on a projective line over a finite field.** *Plos one*, 15(11):e0241890, 2020.
17. Mohamed, Kamsiah and Ali, Fakariah Hani HjMohd and Ariffin, Suriyani. **A New Design of Permutation Function Using Spiral Fibonacci in Block Cipher,***International Journal of Advanced Trends in Computer Science and Engineering*, Vol. 9(1.3), pp. 445-450,2020.
18. M. Ghanti and S. K. Bandyopadhyay**. A proposed method for cryptography using random key and rotation of text.***International Journal of Advanced Trends in Computer Science and Engineering*, Vol. 6, pp. 18-22, March-April 2017.