Punjab University Journal of Mathematics (2024), 56(11), 770-780
https://doi.org/10.52280/pujm.2024.56(11)05

New Cryptosystem Using Sumudu Transform, Combination of Three Functions with Simulation and Python Code

Raut P. P.
Department of Humanities and Applied Sciences,
Shree L. R. Tiwari College of Engineering, Mira Road, Thane [M.S.], India.
Research Center: S.P. College Pune. (Savitribai Phule Pune University)
Email: rautpriti2020@gmail.com
Hiwarekar A. P.
Department of General Science (Mathematics)
Vidya Pratishthan's Kamalnayan Bajaj, Institute of Engineering and Technology,
Baramati, Pune [M.S.], India. (Savitribai Phule Pune University)
E-mail: hiwarekaranil@gmail.com

Received: 08 July, 2024 / Accepted: 22 May, 2025 / Published online: 20 June, 2025

Abstract. In today's world, information security is the most important component of our lives. Cryptography is among the best techniques designed to safeguard data security and message transmission. This paper presents a new method using successive combinations of the Sumudu transform of three functions for encoding and the inverse Sumudu transform for decoding. Starting with standard results on Sumudu transforms, we present our encryption method and obtain it as new theorems. Further, we generalized our method for the more secure algorithm. Finally, we used Python code to implement this strategy with simulation, our conclusions are based on the statistical analysis.

AMS (MOS) Subject Classification Codes: 14G50; 94A60; 11T71; 68P25
Key Words: Cryptography, Sumudu Transform, Encryption, Decryption, Information Security

1. INTRODUCTION

Information is a resource that needs to be protected to prevent unauthorized parties from misusing it. Cryptography is one of the security techniques which is used to protect information sent over different communication channels from unauthorized entities. Its main goal is to give two groups a way to communicate via an unsecured channel so the other party cannot decipher the message. There are various mathematical techniques being used to implement the different cryptographic mechanisms to protect the information shared over the network. It is based on mathematical ideas in the form of algorithms such as encryption and dec ryption process [4]. The shift cipher is one of the techniques that is based

on Modular Arithmetic to encrypt ordinary English text by setting up a correspondence between alphabetic characters and residue mod 26 [4]. Substitution cipher and Affine cipher are based on Number theory where encryption and decryption are a permutation of alphabetic characters [4]. Hill cipher is based on Linear Algebra which makes use of matrix multiplication and inverse [4].

For information security, mathematics is the most essential component. Several methods for cryptography are presented in [7], [8], [9], [12], [14], [16], [18]. Hiwarekar A. P. [5], [6], introduced a new cryptosystem using the Laplace transform of functions $sinhat$, $coshat$, e^{at}. E. Adeyefai, L. Akinolai, O. Agbolade [1] use the combination of two linear functions and Laplace transform for encoding-decoding. Raut P. P. and Hiwarekar A. P. [11], used Elzaki transform for encoding and decoding. Bodakhe D. S. and Panchal S. K. [2], introduced the encryption-decryption method using Sumudu transform. Anthony Adam Pranajaya and Iwan Sugiarto [10], Maclaurin series and Laplace transform for encryption and decryption with simulation.

There are multiple ways in cryptography to use a combination of transforms with the Laplace Transform [17], [13]. The existing cryptographic methods can be broken by general attacks [15], Tuncay M. It is imperative to create new complex cryptosystems using advanced mathematical techniques. The focus of this work is to explore new algorithms and implement them programmatically. Therefore we introduced a new cryptosystem using a linear combination of three functions and using Sumudu transforms which will be resistant to different types of attacks.

We required the following.

2. Definitions and Notations

Here, we use the standard results, and notations from [4], [3], we also use definitions of Plain text, Cipher text, Encryption-Decryption, and Sumudu transform described in [3].
Sumudu Transform: Sumudu Transform of function $f(t)$ for all real numbers, $t \geq 0$ is defined as,

$$T(u) = \int_0^\infty \frac{1}{u} e^{\frac{-t}{u}} f(t)dt, t \geq 0, \tag{2. 1}$$

provided that the integral exists.
The corresponding Inverse Sumudu Transform is $S^{-1}T(u) = f(t)$.

$$S(t^n) = n!u^n, \qquad S^{-1}(n!u^n) = t^n. \tag{2. 2}$$

We also required the following series expansions.

$$e^{2t} = \frac{(2t)^0}{0!} + \frac{(2t)^1}{1!} + \frac{(2t)^2}{2!} + ... + \frac{(2t)^i}{i!}. \tag{2. 3}$$

$$\cosh 2t = \frac{(2t)^0}{0!} + \frac{(2t)^2}{2!} + \frac{(2t)^4}{4!} + ... + \frac{(2t)^{2i}}{(2i)!}. \tag{2. 4}$$

$$\sinh 2t = \frac{(2t)^1}{1!} + \frac{(2t)^3}{3!} + \frac{(2t)^5}{5!} + ... + \frac{(2t)^{2i+1}}{(2i+1)!}. \tag{2. 5}$$

We also use the following Notations:

N - Set of Natural Numbers,
n - Length of Plain Text,
q - Length of Cipher Text,
P - Plain Text.

3. Encryption-Decryption Using Sumudu Transform

In this section, we present a new cryptosystem using a linear combination of three functions e^{2t}, $t^n cosh2t$ and $t^n sinh2t$ and then applying the Sumudu transform. The proposed methodologies is as follows.

Method of Encryption Here we consider

$$f(t) = aP(e^{rt} + t^n coshrt + t^n sinhrt), \quad a, n, r \in N. \tag{3. 6}$$

Step 1: Choose the plain text P, and change every alphabet into numerals so that, A = 0, B = 1, ,Z = 25.
Step 2: Chosen plain text based on Step 1, P is transformed to numerals and is represented as P_i^k, where $k = 0, 1, 2, ...$ denotes the number of iterations and $i = 0, 1, 2...$ indicates the position of letters.
Step 3: Here above P_i^0 values as the coefficient of $[e^{rt} + t^n coshrt + t^n sinhrt]$.
Step 4: Taking the Sumudu transform of the function $f(t)$ given by equation (3.6) and divide the coefficient of u^i by ${}^iP_n = \frac{i!}{(i-n)!},\ i \geq n$.
Step 5: To increase the security of this cryptosystem, we use Caesar cipher, we consider

$$P_i^1 = (B_i^1 + p)\ mod\ 26 \quad \text{and Key} \quad L_i^1 = \frac{B_i^1 + p - P_i^1}{26}. \tag{3. 7}$$

Step 6: Convert P_i^1 into letters using step 1, we get cipher text and L_i^1 is key.

We illustrate our method as follows:
Let us consider example the given plain text to be WORD. Here $n = 4$.

$$P_0^0 = 22,\ P_1^0 = 14,\ P_2^0 = 17,\ P_3^0 = 3,\ P_n^0 = 0, \forall n \geq 4. \tag{3. 8}$$

Here above P_i^0 values as the coefficient of $[e^{2t} + t^4 cosh2t + t^4 sinh2t]$, we consider here $a = 1$ and $r = 2$,

$$f(t) = P(e^{2t} + t^4 cosh2t + t^4 sinh2t). \tag{3. 9}$$

$$\text{Thus,} \quad f(t) = \sum_{i=0}^{\infty} \frac{(2t)^i}{i!} P_i^0 + \sum_{i=0}^{\infty} \frac{(2)^{2i} t^{2i+4}}{(2i)!} P_i^0 + \sum_{i=0}^{\infty} \frac{(2)^{2i+1} t^{2i+1+4}}{(2i+1)!} P_i^0. \tag{3. 10}$$

By using (2.3), (2.4) and (2.5) we have,

$$f(t) = \frac{(2t)^0}{0!}P_0^0 + \frac{(2t)^1}{1!}P_1^0 + \frac{(2t)^2}{2!}P_2^0 + \frac{(2t)^3}{3!}P_3^0 + \frac{(2)^0t^4}{0!}P_0^0 + \frac{(2)^2t^6}{2!}P_1^0 + \frac{(2)^4t^8}{4!}P_2^0 + \frac{(2)^6t^{10}}{6!}P_3^0 + \frac{(2)^1t^5}{1!}P_0^0 + \frac{(2)^3t^7}{3!}P_1^0 + \frac{(2)^5t^9}{5!}P_2^0 + \frac{(2)^7t^{11}}{7!}P_3^0. \tag{3. 11}$$

Using equation (3.8) and taking the Sumudu transform of the function $f(t)$ given by equation (3.10) and divide the coefficient of u^i by ${}^iP_n = \frac{i!}{(i-n)!},\ i \geq n$ we get

$$\begin{aligned} T(u) &= S[f(t)] \\ &= S[P(e^{2t} + t^4 cosh2t + t^4 sinh2t)] \\ &= 22u^0 + 28u^1 + 68u^2 + 24u^3 + 22u^4 + 44u^5 \\ &\quad + 56u^6 + 112u^7 + 272u^8 + 544u^9 + 192u^{10} + 384u^{11}. \end{aligned} \tag{3. 12}$$

The coefficient of $u^0, u^1, u^2, ...$ are denoted by B_i^1 for $i = 0, 1, 2, ...$
In this case we choose $p = 6$. where $0 \leq p \leq 25$, we have following table

i	$\mathbf{B}_i^1$	$\mathbf{B}_i^1 + \mathbf{p}$	$\mathbf{P}_i^1$	$\mathbf{L}_i^1$
0	22	28	2	1
1	28	34	8	1
2	68	74	22	2
3	24	30	4	1
4	22	28	2	1
5	44	50	24	1
6	56	62	10	2
7	112	118	14	4
8	272	278	18	10
9	544	550	4	21
10	192	198	16	7
11	384	390	0	15

Table 1: Illustration of Encryption Method

We have the values of
$P_0^1 = 2,\ P_1^1 = 8,\ P_2^1 = 22,\ P_3^1 = 4,\ P_4^1 = 2,\ P_5^1 = 24,\ P_6^1 = 10,$
$P_7^1 = 14, P_8^1 = 18,\ P_9^1 = 4,\ P_{10}^1 = 16,\ P_{11}^1 = 0,\ P_i^1 = 0,$ for $i \geq 12$
be the encoded message and key is obtained as
$L_0^1 = 1,\ L_1^1 = 1, L_2^1 = 2,\ L_3^1 = 1,\ L_4^1 = 1,\ L_5^1 = 1,\ L_6^1 = 2,\ L_7^1 = 4,$
$L_8^1 = 10,\ L_9^1 = 21,\ L_{10}^1 = 7,\ L_{11}^1 = 15.$
Therefore, the plain text **WORD** gets converted to ciphertext **CIWECYKOSEQA**. Thus, the above-described encryption technique is included in the subsequent theorem as:

Theorem 3.1. *The given n-long plain text in terms of $P_i^0, i = 0, 1, 2, ..$ can be converted to cipher text P_i^1, under Sumudu transform of $P_i^0[e^{2t} + t^n\ cosh2t + t^n\ sinh2t]$ (i.e., P_i^0 as a coefficient of $[e^{2t} + t^n\ cosh2t + t^n\ sinh2t]$ and then taking its Sumudu transform*

followed by dividing coefficient of u^i *by* ${}^iP_n = \frac{i!}{(i-n)!},\ i \geq n$*).*
Here $P_i^1 = (B_i^1 + p)\ mod\ 26, \quad p \in N, \quad 0 \leq p \leq 25$ *and* $P_i^0 = 0, \forall\ i \geq n,$
and

$$B_i^1 = \begin{cases} 2^i(P_i^0), & i < n; \\ 2^{i-n}P^0_{(i-n)/2}, & i \geq n,\ i \text{ is even, n is even;} \\ 2^{i-n}P^0_{(i-(n+1))/2}, & i \geq n,\ i \text{ is odd, n is even;} \\ 2^{i-n}P^0_{(i-n)/2}, & i \geq n,\ i \text{ is odd, n is odd;} \\ 2^{i-n}P^0_{(i-(n+1))/2}, & i \geq n,\ i \text{ is even, n is odd;} \end{cases} \tag{3. 13}$$

the key $L_i^1 = \frac{(B_i^1 + p - P_i^1)}{26}$.

Now we extend Theorem 3.1 for more generalized functions, which are included as:

Theorem 3.2. *The given n-long plain text in terms of* $P_i^0, i = 0, 1, 2, ..$ *can be converted to cipher text* P_i^1*, under Sumudu transform of* $P_i^0 a[e^{rt} + t^n\ coshrt + t^n\ sinhrt]$ *(i.e.,* P_i^0 *as a coefficient of* $a[e^{rt} + t^n\ coshrt + t^n\ sinhrt]$ *and then taking its Sumudu transform followed by dividing coefficient of* u^i *by* ${}^iP_n = \frac{i!}{(i-n)!},\ i \geq n$*).*
Here $P_i^1 = (B_i^1 + p)\ mod\ 26, \quad a,\ r,\ p \in N, \quad 0 \leq p \leq 25$ *and* $P_i^0 = 0, \forall\ i \geq n,$
and

$$B_i^1 = \begin{cases} ar^i(P_i^0), & i < n; \\ ar^{i-n}P^0_{(i-n)/2}, & i \geq n,\ i \text{ is even, n is even;} \\ ar^{i-n}P^0_{(i-(n+1))/2}, & i \geq n,\ i \text{ is odd, n is even;} \\ ar^{i-n}P^0_{(i-n)/2}, & i \geq n,\ i \text{ is odd, n is odd;} \\ ar^{i-n}P^0_{(i-(n+1))/2}, & i \geq n,\ i \text{ is even, n is odd;} \end{cases} \tag{3. 14}$$

key $L_i^1 = \frac{(B_i^1 + p - P_i^1)}{26}$.

Now, for a more secure form of this algorithm, we use an iterative approach based on [6] Hiwarekar A. P. In this section, we apply Theorem 3.2 successively on each output so that cipher text in the first step becomes input (Plain text) for the next step and so on. Thus, to obtain cipher text we used this successive iteration k times on plain text. It is formalized in the following new Theorem as:

Theorem 3.3. *The given n-long plain text in terms of* $P_i^0, i = 0, 1, 2, ..$ *can be converted to cipher text* P_i^k*, under Sumudu transform of* $P_i^0 a[e^{rt} + t^n\ coshrt + t^n\ sinhrt]$ *(i.e.,* P_i^0 *as a coefficient of* $a[e^{rt} + t^n\ coshrt + t^n\ sinhrt]$ *and then taking successively* k *times its Sumudu transform followed by dividing coefficient of* u^i *by* ${}^iP_n = \frac{i!}{(i-n)!},\ i \geq n$*).*

Here $P_i^k = (B_i^k + p)\ mod\ 26, \quad a,\ r,\ p \in N, \quad 0 \leq p \leq 25$ *and* $P_i^{k-1} = 0, \forall\ i \geq n,$ *and*

$$B_i^k = \begin{cases} ar^i(P_i^{k-1}), & i < n; \\ ar^{i-n}P^{k-1}_{(i-n)/2}, & i \geq n,\ i \text{ is even, n is even;} \\ ar^{i-n}P^{k-1}_{(i-(n+1))/2}, & i \geq n,\ i \text{ is odd, n is even;} \\ ar^{i-n}P^{k-1}_{(i-n)/2}, & i \geq n,\ i \text{ is odd, n is odd;} \\ ar^{i-n}P^{k-1}_{(i-(n+1))/2}, & i \geq n,\ i \text{ is even, n is odd;} \end{cases} \tag{3. 15}$$

the key $L_i^k = \frac{(B_i^k + p - P_i^k)}{26}$.

In the next section we obtain following:

4. Programmatic Solution

For our encryption-decryption method explained in section 3, we developed new Python code that will be useful for implementation and for getting output quickly.

Programmatic Solution For Encryption-Decryption (Python Program):

Here the function is $f(t) = e^r t + t^n cohrt + t^n sinhrt$.

Enter the number of plain texts to be encrypted: 12

Enter plaintext value: SECURE

Enter values of $'r',' a',' p'$ for set 1 respectively (comma-separated values): 4, 12, 6
Enter values of $'r',' a',' p'$ for set 2 respectively (comma-separated values): 5, 12, 6
Enter values of $'r',' a',' p'$ for set 3 respectively (comma-separated values): 11, 12, 6
Enter values of $'r',' a',' p'$ for set 4 respectively (comma-separated values): 12, 12, 6
Enter values of $'r',' a',' p'$ for set 5 respectively (comma-separated values): 2, 7, 6
Enter values of $'r',' a',' p'$ for set 6 respectively (comma-separated values): 2, 12, 6
Enter values of $'r',' a',' p'$ for set 7 respectively (comma-separated values): 2, 13, 6
Enter values of $'r',' a',' p'$ for set 8 respectively (comma-separated values): 2, 14, 6
Enter values of $'r',' a',' p'$ for set 9 respectively (comma-separated values): 11, 13, 6
Enter values of $'r',' a',' p'$ for set 10 respectively (comma-separated values): 11, 13, 11
Enter values of $'r',' a',' p'$ for set 11 respectively (comma-separated values): 11, 13, 12
Enter values of $'r',' a',' p'$ for set 12 respectively (comma-separated values): 11, 13, 13

Sr. No.	Plain Text	r	a	p	Cipher Text
1	SECURE	4	12	6	OQAAWSOMUKOMMEUKWS
2	SECURE	5	12	6	OMICCMOUKAEWACCMKA
3	SECURE	11	12	6	OOYKUEOQQMASASWASI
4	SECURE	12	12	6	OKEACKOYCKEIMACKCK
5	SECURE	2	7	6	CKKIMSCYOWWMWMYQAU
6	SECURE	2	12	6	OYYCUIOWQAAUAUWMSE
7	SECURE	2	13	6	GGGGGGGGGGGGGGGGGG
8	SECURE	2	14	6	YOOKSEYQWMMSMSQAUI
9	SECURE	11	13	6	GGGGTGGGGGGGGTTGG
10	SECURE	11	13	11	LLLLYLLLLLLLLYYLL
11	SECURE	11	13	12	MMMMZMMMMMMMMZZMM
12	SECURE	11	13	13	NNNNANNNNNNNNAANN

Table 2 : Illustration of Python Code

5. SIMULATION

Simulation plays a crucial role in evaluating encryption algorithms. It allows us to look into the impact of changing the various components involved in the algorithm.

Change in Parameter $a,\ p,\ r$:

5.1 : The change in parameters a, p, and r, changes the output of the cipher text. As per equation (3.14), the value of r does not affect on the first letter of the cipher text. Therefore the value of the first letter of cipher text will remain the same for the given values of a and p, shown in Table 3. Here we take fixed values of $a = 12$ and $p = 6$ and only changes in value of r as shown in Table 3:

Sr. No.	Value of r	Plain Text	Cipher Text
1	4	SECURE	OQAAWSOMUKOMMEUKWS
2	5	SECURE	OMICCMOUKAEWACCMKA
3	11	SECURE	OOYKUEOQQMASASWASI
4	12	SECURE	OKEACKOYCKEIMACKCK

Table 3 : Encryption by changing value of r

5.2 : If the value of a is changed then it will generate different cipher text, shown in Table 4. Here we take fixed values of $r = 2$ and $p = 6$ and only the changes in value of a as shown in Table 4:

Sr. No.	Value of a	Plain Text	Cipher Text
1	7	SECURE	CKKIMSCYOWWMWMYQAU
2	12	SECURE	OYYCUIOWQAAUAUWMSE
3	13	SECURE	GGGGGGGGGGGGGGGGGG
4	14	SECURE	YOOKSEYQWMMSMSQAUI

Table 4 : Encryption by changing value of a

5.3 : If the value of $a = 13$ then cipher text is the repetition of only two letters and the value of those letters depends on p as shown in Table 5. Here we take fixed values of $a = 13$ and $r = 11$ and only changes in value of p shown in Table 5:

Sr. No.	Value of p	Plain Text	Cipher Text
1	6	SECURE	GGGGTGGGGGGGGTTGG
2	11	SECURE	LLLLYLLLLLLLLYYLL
3	12	SECURE	MMMMZMMMMMMMMZZMM
4	13	SECURE	NNNNANNNNNNNNAANN

Table 5 : Encryption by changing value of p

5.4 : If the value of both r and the first letter of plain text is even and $a = 13$ then the cipher text is the repetition of a single letter and the value of that letter depends on the value of p, shown in Tables 6 and 7. In particular, if we take fixed values of $a = 13$ and $r = 4$ and only changes in value of p then we have following Table 6:

Sr. No.	Value of p	Plain Text	Cipher Text
1	6	SECURE	GGGGGGGGGGGGGGGGG
2	11	SECURE	LLLLLLLLLLLLLLLLL
3	12	SECURE	MMMMMMMMMMMMMMMMM
4	13	SECURE	NNNNNNNNNNNNNNNNN

Table 6 : Encryption by taking value of $a = 13$ with same plain text

5.5 : Here we take a fixed value of $a = 13$ and the value of the first letter of plain text is even then the cipher text is the repetition of a single letter and the value of that letter depends on the value of p shown in Table 7:

Value of r	Value of p	Plain Text	Cipher Text
4	5	INTERNET	FFFFFFFFFFFFFFFFFFFFFF
6	7	MATHEMATICS	HHHHHHHHHHHHHHHHHHHHHHHHH HHHHHHHHHH
10	2	CRYPTOGRAPHY	CCCCCCCCCCCCCCCCCCCCCCC CCCCCCCCCCCC
12	8	ENCRYPTION	IIIIIIIIIIIIIIIIIIIIIIIII

Table 7 : Encryption by taking value of $a = 13$ with different plain text

6. Correlation Coefficient Analysis

The relationship between the plain text and cipher text is calculated using statistical analysis using correlation coefficient. The correlation coefficient, denoted by r, can be computed using the following formula.

$$r = \sum_{i=0}^{n} (x_i - \overline{x})(y_i - \overline{y})/\sigma_x\sigma_y, \tag{6. 16}$$

where $\overline{x}$ and $\overline{y}$ are $mean$ of x and y respectively.

$$\overline{x} = \frac{1}{n}\sum_{i=0}^{n}(x_i) \text{ and } \overline{y} = \frac{1}{n}\sum_{i=0}^{n}(y_i), \tag{6. 17}$$

x_i be the coefficient of plain text and $x_i = 0,\ \forall i \geq$ length of plain text.
y_i be the coefficient of cipher text and $y_i = 0,\ \forall i \geq$ length of cipher text.
Standard deviation of x and y denoted by σ_x and σ_y respectively.

$$\sigma_x = \sqrt{\sum_{i=0}^{n}(x_i - \overline{x})^n},\ \sigma_y = \sqrt{\sum_{i=0}^{n}(y_i - \overline{y})^n}. \tag{6. 18}$$

Using standard results,

(1) If $r = 1$, indicate that the plain text and its cipher text are identical (i.e. bad encryption).
(2) If $r = 0$, that implies the cipher text is completely different from the plain text (i.e. good encryption).
(3) If $r = -1$ that gives the cipher text is the negative of the plain text.

So, the success of the encryption process depends on smaller values of r. The correlation value of our encryption method is shown in Table 8:

Sr.No.	a	r	p	**Plain Text**	**Cipher Text**	**Value of** r
1	13	2	6	HAT	TGGTGGGGG	0.094918504
2	14	2	6	WORD	CIWECYKOSEQA	0.063001145
3	13	11	6	MATHS	GGTTGGGGGTTTTGG	0.091031693
4	12	2	6	SECURE	OYYCUIOWQAAUAUWMSE	0.093034183

Table 8 : Coefficient of Correlation Value

FIGURE 1. Graph of Coefficient of Correlation

The correlation coefficients for the plain text HAT, WORD, MATHS, and SECURE are respectively $r = 0.09,\ r = 0.06,\ r = 0.09,\ r = 0.09$ (shown in Table 8 and Fig. 1). It shows that cipher text are completely different from plain text. This shows that the suggested encryption algorithm resists statistical attacks.

7. CRYPTANALYSIS

Our method is useful in resisting the different types of attacks which are listed below.

7.1. **Ciphertext Only Attack.** In this attack, the attacker has access to only a specific set of cipher texts. Suppose the attacker knows the cipher text **CIWECYKOSEQA** [Section 3 equation (3.12)]. The length of cipher text is 12 but the length of plain text WORD is 4. In this work, we used a linear combination of three functions that increases the length of cipher text. Therefore, this algorithm may prevent Cipher text Only Attacks.

7.2. **Known-Plaintext Attack.** In this attack, the attacker has access to the matching cipher text as well as the plain text. Suppose the attacker knows plain text MATHS and the corresponding cipher text [Section 3 equation (3.15) with unknown values $a = 7$, $r = 2$, $p = 6$ and $k = 3$] is **MSMCICOGSOMEMIOCUIEMQYWEIUYOQIEEK-MACASQCUAYIAMSECECAUMSIKYQGGKOUIOWSEMSKOMSAUWMSEIK UISESEKOSEIKIKAUSEKOSEIKKOQAKOYQECAUECUIAUWMWMOWCYEC**. The length of plain text is 5 and the length of cipher text is 135 letters. The length of cipher text is 27 times the length of plain text. Therefore, this algorithm may prevent a Known-Plain text Attack.

7.3. **Frequency Attack.** Frequency analysis is one of the known cipher text attacks in which the decipher the cipher text by analyzing the frequency distribution of letters. Frequency analysis can be used to break algorithm when the length of plain text and cipher text is the same. But the new cryptosystem explained in Section 3 in which the length of plain text and cipher text are different (Table 3, 4). Also, cipher text is the repetition of one or two letters (Table 5, 6, 7). Therefore, this algorithm may prevent Frequency Attack.

8. Conclusion and Future Scope

In this paper, we developed a new encryption techniques using a Sumudu transform of a combination of three functions. We implemented our method using Python code. The main advantage of this algorithm is that we can get different output for same input by changing the value of a or r or k or p or all values and obtained the simulation with statistical analysis. This Cryptographic scheme converts every plain text of length x to a cipher text of length $3x$ which may protect various attacks. Extension of this work is possible by using other suitable functions and transforms.

9. Acknowledgments

Raut P. P. is thankful to the Principal Dr. Deven Shah of Shree L. R. Tiwari College of Engineering, Mira Road, Thane and S.P. College Pune (Research center of Mathematics) for their support to this work. Hiwarekar A. P. is thankful to the Principal, VPKBIET, Baramati, and to the management of Vidya Pratishthan Baramati for the entire support to this work.

10. Conflict of Intrest

The authors declare that they have no competing interests

11. Funding

No funding has been received for this study.

References

[1] E. Adeyefa, L. Akinolai, and O. Agbolade. *Application of Laplace Transform to Cryptography Using Linear Combination of Functions*. TWMS Journal of Applied and Engineering Mathematics **11** (2021): 1050 – 1060.

[2] D. S. Bodakhe and S. K. Panchal. *Application of Sumudu Transform in Cryptography*. Bulletin of Marathwada Mathematical Society **16**, No.2 (2015): 1 – 6.

[3] Lokenath Debnath and Dambaru Bhatta, *Integral Transforms and their applications*, 2nd Edition, Chapman and Hall/CRC, 2007.

[4] R. S. Douglas, *Cryptography Theory and Practice*, 3rd Edition, Chapman and Hall/CRC, 2011.

[5] A. P. Hiwarekar. *Cryptography using Laplace Transform*. International Journal of Engineering Research and Applications **5**, No.4 Part-5 (2015): 102 – 106.

[6] A. P. Hiwarekar. *Encryption-Decryption using Laplace Transforms*. Asian Journal of Mathematics and Computers **12** (2016): 201 – 209.

[7] G. Naga Lakshmi, B. Ravi Kumar, and A. Chandra Shekhar. *A cryptographic Scheme of Laplace Transforms*. International Journal of Mathematical Archieve **2** (2011): 2515 – 2519.

[8] A. M., Osama S. F. and S. E., E. M. Nigm. *Security Analysis of Reverse Encryption Algorithm for Databases*. International Journal of Computer Applications **66**, No. 4 (2013): 19 - 27.

[9] A. Musheer and Shamsher M.. *A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping*. International Journal on Computer Science and Engineering **2**, No.1 (2009): 46 – 50.

[10] A. A. Pranajaya, and Iwan Sugiarto. *Simulation and Analysis on Cryptography by Maclaurin Series and Laplace Transform*. IAENG International Journal of Applied Mathematics **52**, No.2 (2022): 1 – 9.

[11] P. P. Raut and A. P. Hiwarekar. *New Method of Cryptography with Python Code Using Elzaki Transform and Linear Combination of Function*. Communications in Mathematics and Applications **14**, No.3 (2023): 1245 – 1254.

[12] B. S. Sahana Raj and Venugopalachar Sridhar. *Identity-Based Cryptography Using Matrices*. Wireless Personal Communication Springer **120** (2021): 1637 – 1657.

[13] Mampi Saha. *Application of Laplace-Mellin Transform for Cryptography*. Rai Journal of Technology Research ad Innovation **5**, No.1 (2017): 12 – 17.

[14] J. S. Shaikh and G. A. Mundhe. *Application of Elzaki Transform in Cryptography*. IJMSET **3**, No.3 (2016): 46 – 48.

[15] M. Tuncay. *Cryptanalysis use of Sumudu Transform in Cryptography*. ITM Web conferences, CME 2017, ICAAM **13** (2017): 1 – 5.

[16] H. K. Undegaonkar and R. N. Ingle. *Role of some integral transforms in cryptography*. International Journal of Engineering and advanced technology **9**, No.3 (2020): 376 – 380.

[17] J. Vashi and M.G. Timol. *Laplace and Sumudu Transforms and Their Application*. International Journal of Innovative Science, Engineering and Technology **3**, No.8 (2016): 538 – 542.

[18] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki. *A Modified AES Based Algorithm for Image Encryption*. International Journal of Computer and Information Engineering **1**, No.3 (2007): 745 – 750.