Results in Nonlinear Analysis 8 (2025) No. 1, 163–171
https://doi.org/10.31838/rna/2025.08.01.015
Available online at www.nonlinear-analysis.com

Results in Nonlinear Analysis
ISSN 2636-7556

Peer Reviewed Scientific Journal

Enhancing data security by apply a novel approach utilizing kashuri fundo transform and linear function combinations

Nada Sabeeh Mohammed[1], Salam Abdulhussein Sehen[2], Emad A. Kuffi[3]

[1]Department of Bioinformatics, University of Information Technology and Communications, Biomedical Informatics College Baghdad, Iraq; [2]Department of Medical Physics University of Al-Qadisiyah, College of Science, Diwaniya, Iraq; [3]Department of Mathematics Mustansiriyah University, College of Basic Education Baghdad, Iraq.

Abstract

In today's interconnected digital landscape, safeguarding sensitive data against cyber threats has emerged as our paramount challenge. To fortify defenses against intruders, continual enhancement of security measures is imperative, leveraging cutting-edge mathematical methodologies. This research presents a novel iterative cryptographic method based on the successive Kashuri Fundo Transform of a linear combination of functions and complemented by its inverse counterpart, specifically tailored for decryption purposes. Beginning with a comprehensive procedural framework, we substantiate our findings through empirical results. Moreover, we extend the applicability of this methodology through generalization and iterative refinement, thereby bolstering its resilience against potential breaches.

Key words and phrases: Cryptography Kashuri Fundo Transform Information Security Encryption Decryption.

Mathematics Subject Classification (2010): 44-XX Integral Transforms

1. Introduction

Information stands as a valuable asset requiring vigilant safeguarding against unauthorized exploitation. Cryptography emerges as a pivotal security technique ensuring the protection of information

Email addresses: nada.sabeeh@uoitc.edu.iq (Nada Sabeeh Mohammed); salam.sehen@qu.edu.iq (Salam Abdulhussein Sehen); emad.kuffi@uomustansiriyah.edu.iq (Emad A. Kuffi)

Received January 21, 2025; Accepted February 13, 2025; Online March 4, 2025

transmitted across diverse communication channels. It safeguards confidential data traversing platforms such as e-commerce, movable communication, secret emails, enterprise transactions, and monetary information. Through diverse mathematical methodologies, cryptography fortifies the implementation of various cryptographic mechanisms, thereby ensuring the secure exchange of information over networks. Mathematics is integral to information security, standing as a cornerstone in cryptography—a formidable tool used to safeguard sensitive data. Within cryptosystems, various mathematical techniques are employed to bolster security measures. Among these techniques lies the shift cipher, which hinges on modular arithmetic, as expounded by Kahate [1]. The Hill cipher leverages concepts from Linear Algebra, employing matrix multiplication and inversion as elucidated by Stinson [2]. In [3], Vinothkumar et al introduced novel encryption and decryption methods based on matrix theory. Raj and Sridhar [4] innovatively proposed an identity (ID)-based El-Gamal encryption/decryption method. In 2021 a novel encryption scheme was introduced based on graph theory principles [5]. In [6], presented a groundbreaking cryptosystem leveraging Laplace transforms, which Hiwarekar [7] extended to include exponential, hyperbolic sine, and cosine functions, presenting an iterative approach to cryptography. Cryptography encompasses a plethora of methods that employ various transforms, often integrating the powerful Laplace transform. Jadhav and Hiwarekar [8] devised an innovative by employing the Laplace-Elzaki transform in cryptography and decryption. Idowu et al. [9] introduced another method employing the Kamal transform for encoding and decoding data. Adeyefai et al. [10] explored encryption and decryption techniques using both the Laplace transform and its inverse. In [11] Behrouz Forouzan introduced simplify the difficult concepts of cryptography and network security In [12], this study delves into a pioneering cryptographic approach that encrypts plain text by leveraging coefficients extracted from a Taylor series of the logarithm function, each multiplied by its corresponding index. In [13], this study introduces a pioneering cryptographic and decryption technique employing iterative methods using both the Elzaki transforms and its inverse. Integral transformations have proven invaluable in tackling a multitude of challenges spanning technology, science, and engineering [14, 15]. Most notably, the groundbreaking Sadik transform has been recently utilized for encrypting and decrypting original textual data [16, 17]. In this paper, we will use the Kashuri Fundo transform in encryption, as this transformation is of great importance in solving many problems such as steady heat transfer problems, as well as solving decay problems, in addition to finding the unknown function in integral transformations and other problems [18–23].

2. Foundations and Advanced Applications: Definitions and Standard Results in Cryptography

In this section, we will present some definitions and results.

2.1 Definitions

Definition 1: *Plain text In cryptography, plain text refers to the original message or data that is intelligible and readable to anyone.*

Definition 2: *Cipher text: In cryptography, cipher text refers to the transformed message or data resulting from applying encryption techniques to plaintext. This transformed form is designed to be unintelligible to unauthorized individuals, ensuring secure transmission and storage of sensitive information.*

Definition 3: *Encryption: Encryption is the process of converting a plain text message into cipher text using specific encoding techniques. This procedure ensures that the original message becomes unintelligible to unauthorized parties, thereby enhancing the security and confidentiality of transmitted or stored information.*

Definition 4: *Decryption: refers to the process of transforming encoded messages back into plaintext, effectively revealing their original content.*

2.2. Unveiling Standard Results

Definition 5: [21] *Let us explore the functions belonging to the defined set G.*

$$G=\{g(t):\exists Y,g_1,g_2>0,|\,g(t)\,|<Ye^{\frac{|t|}{g_j^2}}\ \text{ if }\ t\in(-1)^j X[0,\infty)\}$$

For any function in the set G, the constant Y must be a finite number. The parameters g_1 and g_2 may be finite or infinite.

Definition 6: [21] *The Kashuri Fundo transform (KFT), represented in the group G and indicated by $K(.)$, is described as follows:*

$$\mathfrak{K}\{g(t)\}(w)=B(w)=\frac{1}{w}\int_0^\infty e^{\frac{-t}{w^2}}g(t)dt\ \ t\ge 0,-g_1<w<g_2 \tag{1}$$

or

$$\mathfrak{K}\{g(t)\}(w)=B(w)=\frac{1}{w}\int_0^\infty e^{-t}g(w^2t)dt$$

The (KFT) inverse represented by $\mathfrak{K}^{(-1)}$, is formulated as:

$$\mathfrak{K}^{(-1)}\{B(w)=g(t),t\ge 0\} \tag{2}$$

In this part, we will give the inverse Kashuri Fundo transform for some fundamental functions [21], as shown in Table 1:

We are examining the conventional expansion.

$$e^{ut}=\frac{(ut)^0}{0!}+\frac{(ut)^1}{1!}+\frac{(ut)^2}{2!}+?\frac{(ut)^3}{3!}+\cdots+(\frac{(ut)^n}{n!}=\sum_0^\infty\frac{(ut)^n}{n!} \tag{3}$$

$$\cosh(ut)=\frac{(ut)^0}{0!}+\frac{(ut)^2}{2!}+\frac{(ut)^4}{4!}+?\frac{(ut)^6}{6!}+\cdots+(\frac{(ut)^{2n}}{(2n)!}=\sum_0^\infty\frac{(ut)^{2n}}{(2n)!} \tag{4}$$

Here, we consider N as the group of natural numerals.

Table 1: Represents the Kashuri Fundo transform for some fundamental functions and its inverse.

No	Function	(KFT)	Inverse (KFT)
1	t	$\mathfrak{K}\{t^m\}=w^3$	t
2	$t^m, m\in Z$	$\mathfrak{K}\{t^m\}=m!w^{2n+1}$	t^m
3	e^{it}, i constant	$\mathfrak{K}\{e^{it}\}=\frac{w}{1-iw^2}$	e^{it}
4	$sin(it)$	$\mathfrak{K}\{sin(it)\}=\frac{iw^3}{1+i^2v^4}$	$sin(it)$
5	$cos(it)$	$\mathfrak{K}\{cos(it)\}=\frac{w}{1+i^2v^4}$	$cos(it)$
6	$sinh(it)$	$\mathfrak{K}\{sinh(it)\}=\frac{iw^3}{1-i^2v^4}$	$sinh(it)$
7	$cosh(it)$	$\mathfrak{K}\{cosh(it)\}=\frac{w}{1+i^2v^4}$	$cosh(it)$

3. Principal outcome

The following algorithm outlines the proposed methodology:

3.1 Encryption Process

The encryption method involves the following steps:

Firstly, we consider:

$$g(t) = xA[e^{ut} + \cosh(ut)],\ x,u \leq 1000 \tag{5}$$

Step 1: Select plain text T and encryption each letter as a numerical value, where $A = 0,\cdots$, and $Z = 25$.

Step 2: The process involves converting the plain text T into numerical values, denoted as $A_(y,z)$, where the subscript $y = 0,1,2,\cdots$ denotes the location of each letter, and subscript $z = 0,1,2,\cdots$ denotes the numeral of iterations. For instance, if the given plain text is "NADA" with $m = 4$, following Step 1, the plain text converts to $N = 13, A = 0, D = 3$, and $A = 0$. Thus, it is represented as $A_{0,0} = 13, A_{1,0}, = 0, A_{2,0} = 3, A_{3,0} = 0$, and $A_{(m,0)} = 0$ for all $m \geq 4$.

Step 3: involves expressing the numbers as coefficients of $\{e^{2t} + \cosh(2t)\}$, where u is a positive constant.

$$e^{2t} = \frac{(2t)^0}{0!} + \frac{(2t)^1}{1!} + \frac{(2t)^2}{2!} + \frac{(2t)^3}{3!} + \cdots + (\frac{(2t)^n}{n!} = \sum_0^\infty \frac{(2t)^n}{n!} \tag{6}$$

$$\cosh(2t) = \frac{(2t)^0}{0!} + \frac{(2t)^2}{2!} + \frac{(2t)^4}{4!} + \frac{(2t)^6}{6!} + \cdots + (\frac{(2t)^{2n}}{(2n)!} = \sum_0^\infty \frac{(2t)^{2n}}{(2n)!} \tag{7}$$

Utilizing equation (5), with $x = 3$ and $u = 2$, we obtain

$$g(t) = 3A[e^{2t} + \cosh(2t)] \tag{8}$$

$$g(t) = 3(\sum_0^\infty \frac{(2t)^y}{y!} A_{(y,0)} + \sum_0^\infty \frac{(2t)^{2n}}{(2n)!} A_{(y,0)}), \tag{9}$$

$$= \frac{(2t)^0}{0!} A_{(0,0)} + \frac{(2t)^1}{1!} A_{(1,0)} + \frac{(2t)^2}{2!} A_{(2,0)} + \frac{(2t)^3}{3!} A_{(3,0)} + \frac{(2t)^0}{0!} A_{(0,0)} + \frac{(2t)^2}{2!} A_{(1,0)} + \frac{(2t)^4}{4!} A_{(2,0)} + \frac{(2t)^6}{6!} A_{(3,0)} \tag{10}$$

Step 4: Using the (KFT) to the function $g(t)$ as described in equation (10), yields

$$B(w) = K\{g(t)\} = K\{3A[e^{2t} + cosh(2t)]\}, \tag{11}$$

$$= 3[13w + 0 + 6w^5 + 0 + 13w + 0 + 16w^9 + 0] \tag{12}$$

$$= 78w + 0 + 18w^5 + 48w^9 + 0 \tag{13}$$

Step 5: To enhance the security of this cryptosystem, we introduce modifications where $A_{(y,1)} = (R_{(y,1)} + T) \bmod 26$ and $H_{(y,1)} = \frac{([(R_{(y,1)} + T) - A_{(y,1)}])}{26}$, Here, T is selected as $T = 5$. As shown in Table 2.

Table 2: Represents modifications that have been applied to enhance the security of the cryptosystem.

Y	$R_{y,1}$	$R_{y,1}+T=\mathfrak{R}_{y,1}$	$\mathfrak{R}_{y,1}\bmod 26=A_{y,1}$	$H_{(y,1)}=\dfrac{([(R_{(y,1)}+T)-A_{(y,1)}])}{26}$
0	78	$78+5=83$	5	3
1	0	$0+5=5$	5	0
2	18	$18+5=23$	23	0
3	48	$48+5=53$	1	2
4	0	$0+5=5$	5	0

The encrypted message is represented by the values $A_{0,0}=5, A_{1,1}=5, A_{2,1}=23, A_{3,1}=1, A_{4,1}=5$. These correspond to the cipher text FFXBF. Alongside this, the key is derived from $H_{0,1}=3, H_{1,1}=0, H_{2,1}=0, H_{3,1}=2, H_{4,1}=0$. Thus, when transmitting the plain text to the recipient, it will include the cipher text "FFXBF" along with the key series 3,0,0,2,0.

In this method, the plain text message 'NADA' transforms into “FFXBF”. This transformation exemplifies the process outlined below.

Fresh Insights in Encryption Technology:

Here, we summarize our methodology from section(3.1) as follows:

Result 1: *The plain text, consisting of n characters, is represented as* $A_{(y,0)}$, *where* $y=0,1,2,\cdots$, *under the KFT of* $A_{(y,0)}\{e^{2t}+\cosh(2t)\}$ *that is* $A_{(y,0)}$ *as a coefficient of* $\{e^{2t}+\cosh(2t)\}$ *and subsequently applying the KFT), can be transformed into cipher text* $A_{(y,1)}$.

$$A_{(y,1)})=(R_{(y,1)}+T)\bmod 26 \text{ where } T\in N, 0\le T\le 25, \text{ and } H_{(y,1)}=\frac{([(R_{(y,1)}+T)-A_{(y,1)}])}{26} \tag{14}$$

Hence:

$$R_{y,1}=\begin{cases} 2^{y}(A_{y,0}+A_{y/2,0}) & y<m \quad y:even \\ 2^{y}A_{y,0} & y<m \quad y:odd \\ 2^{(2y-m)}A_{y-[\frac{m}{2}],0} & y\ge m \quad y:even \\ 2^{(2y-m-1)}A_{y-[\frac{m+1}{2}],0} & y\ge m \quad y:odd \end{cases} \tag{15}$$

so that $A_{(y,0)}=0$,for all $y\ge m$ We now extend Result 1 to a more generalized function

A New Approach to Generalized Encryption Result

Result 2: *Converting the given n-long plain text expressed in terms of* $A_{(y,0)}$, *where* $y=0,1,2,\cdots$ *under the KFT of* $A_{(y,0)}x[e^{ut}+\cosh(ut)]$ *(i.e.,* $A_{(y,0)}$*as a coefficient of* $x[e^{ut}+\cosh(ut)]$ *and then applying the KFT), yields the corresponding cipher text* $A_{(y,1)}$.

$$A_{(y,1)}=R_{(y,1)}+T\bmod 26, \text{ where } x,u,T\in N, 0\le T\le 25, x,u\le 1000, key H_{(y,1)}=\frac{([(R_{(y,1)}+T)-A_{(y,1)}])}{26} \tag{16}$$

$$R_{y,1}=\begin{cases} xu^{y}(A_{y.0}+A_{y/2,0}) & y<m \quad y:even \\ xu^{y}A_{y,0} & y<m \quad y:odd \\ xu^{(2y-m)}A_{y-[\frac{m}{2}],0} & y\geq m \quad y:even \\ xu^{(2y-m-1)}A_{y-[\frac{m+1}{2}],0} & y\geq m \quad y:odd \end{cases} \tag{17}$$

so that $A_{(y,0)}=0$,for all $y\geq m$ Next, we iterate the previously described process using the cipher text obtained in Result 2. This iterative procedure is applied z times to the original plain text, resulting in its transformed cipher text form. The sequential application of this process is detailed in the following result.

Result 3: *Converting the provided n-length plain text, articulated as $A_{(y,0)}$, where $y=0,1,2,\cdots$ using the KFT of $A_{(y,0)}x[e^{ut}+\cosh(ut)]$ successively z times (i.e.,$A_{(y,0)}$as a coefficient of $x[e^{ut}+cosh(ut)]$ and then applying the KFT z times) results in the corresponding cipher text $A_{(y,z)}$.*

$$A_{(y,z)}=R_{(y,z)}+T \bmod 26, \text{ where } x,u,T\in N, 0\leq T\leq 25, x,u\leq 1000, keyH_{(y,z)}=\frac{([(R_{(y,z)}+T)-A_{(y,z)}])}{26} \tag{18}$$

$$R_{y,z}=\begin{cases} xu^{y}(A_{y.z-1}+A_{y/2,z-1}) & y<m \quad y:even \\ xu^{y}A_{y,z-1} & y<m \quad y:odd \\ xu^{(2y-m)}A_{y-[\frac{m}{2}],z-1} & y\geq m \quad y:even \\ xu^{(2y-m-1)}A_{y-[\frac{m+1}{2}],z-1} & y\geq m \quad y:odd \end{cases} \tag{19}$$

so that $A_{(y,z-1)}=0$,for all $y\geq m$

Remark 1: *Result 1 corresponds to a specific instance of Result 3 when $z=1, u=2,$ and $x=1$.*

Remark 2: *Result 2 corresponds to a specific instance of Result 3 when $z=1$.*

3.2 Decryption Process

To decrypt, we proceed in the reverse direction. The decryption process is outlined as follows:

Step 1: Begin with the received cipher text from the sender. If v represents the length of the cipher text and is a multiple of three, apply the function $B(w)$ as defined below, extending up to $y=\frac{2v}{3}-1$ terms. If not, expand up to $y=\frac{(2v-1)}{3}-1$ terms.

$$B(w)=\sum_{0}^{\infty}xu^{y}A_{(y,0)}w^{(2n+1)}+\sum_{0}^{\infty}xu^{2y}A_{(y,0)}w^{(4n+1))}, \tag{20}$$

$$\begin{aligned} B(w)=&xu^{0}A_{0,0}w^{1}+xu^{1}A_{1,0}w^{3}+xu^{2}A_{2,0}w^{5}+xu^{3}A_{3,0}w^{7}+xu^{0}A_{0,0}w^{1} \\ &+xu^{2}A_{1,0}w^{5}+xu^{4}A_{2,0}w^{9}+xu^{6}A_{3,0}w^{13} \end{aligned} \tag{21}$$

Step 2: Substitute the values of a and r into equation (21), where $x=3$ and $u=2$. Then, organize and rearrange equation (21) in ascending order of the power of w

$$\begin{aligned} B(w)=&xu^{0}A_{0,0}w^{1}+xu^{1}A_{1,0}w^{3}+xu^{2}A_{2,0}w^{5}+xu^{3}A_{3,0}w^{7}+xu^{0}A_{0,0}w^{1} \\ &+xu^{2}A_{1,0}w^{5}+xu^{4}A_{2,0}w^{9}+xu^{6}A_{3,0}w^{13} \end{aligned} \tag{22}$$

$$B(w)=3A_{0,0}w^{1}+6A_{1,0}w^{3}+12A_{2,0}w^{5}+24A_{3,0}w^{7}+3A_{0,0}w^{1}+12A_{1,0}w^{5}+48A_{2,0}w^{9}+192A_{3,0}w^{13} \tag{23}$$

$$B(w)=(3+3)A_{0,0}w+6A_{1,0}w^{3}+(12A_{1,0}+12A_{2,0})w^{5}+24A_{3,0}w^{7}+48A_{2,0}w^{9}+192A_{3,0}w^{13} \tag{24}$$

$$B(w)=6A_{0,0}w+6A_{1,0}w^{3}+12(A_{1,0}+A_{2,0})w^{5}+24A_{3,0}w^{7}+48A_{2,0}w^{9}+192A_{3,0}w^{13} \tag{25}$$

Step 3: Compute the inverse KFT of $\mathfrak{K}^{(-1)}[B(w)]$ as defined in equation (25).

$$\mathfrak{K}^{(-1)}[B(w)]=\frac{6A_{0,0}t^{0}}{0!}+\frac{6A_{0,0}t^{1}}{1!}+\frac{12(A_{1,0}+A_{2,0})t^{2}}{2!}+\frac{24A_{3,0}t^{3}}{3!}+\frac{48A_{2,0}t^{4}}{4!}+\frac{192A_{3,0}t^{5}}{5!} \tag{26}$$

Step 4: instructs us to translate the encrypted text into numerical values, adhering to the conversion where A equals $0, B=1, C=2$, and so forth until Z, which equals 25. Each term in this numerical sequence is represented as $A_{(y,1)}$, where y ranges from 0 onwards. For any y value that is greater than or equal to $v, A_{(y,1)}$ is defined as 0. For the cipher text FFXBF, the transformation into numerical values is as follows: $A_{1,0}=5, A_{1,1}=5, A_{2,1}=23, A_{3,1}=1, A_{4,1}=5,$. The corresponding key values are $H_{0,1}=3, H_{1,1}=0, H_{2,1}=0, H_{3,1}=2, H_{4,1}=0$.

Step 5: we calculate $R_{(y,0)}$ for $y=0,1,2,3,\cdots$ using the formula $R_{(y,1)}=26*H_{(y,1)}+A_{(y,1)}-T$. The initial values provided are $R_{0,0}=78, R_{1,0}=0, R_{2,0}=48, R_{4,0}=0$.

Step 6: involves multiplying each coefficient of the function $g(t)=\mathfrak{K}^{(-1)}[B(w)]$ from equation (26) by the factorial of the power of t. Subsequently, we equate the resulting $R_{(y,0)}$ value to solve for the $A_{(y,0)}$ *s*. This process yields the values: $A_{0,0}=13A_{0,1}=0, A_{2,1}=3, A_{4,1}=0$.

Step 7: we organize the $A_{(y,0)}$ values sequentially and apply the transformation outlined in Step 4. This results in $13=N, 0=A, 3=D$, and $0=A$. Therefore, the cipher text "FFXBF" translates to the word "NADA".

The encrypted message "FFXBF", upon applying the inverse KFT, decrypts to the word NADA. This decryption process is elucidated through the following explanation.

Decryption Outcome

Result 4: *The encrypted input cipher text represented as* $A_{(y,1)}$ *for* $y=0,1,2,\cdots$ *with a specified value of* T *and key* $H_{(y,1)}$, *can be converted into plain text* $A_{(y,0)}$ *through the inverse Elzaki Transform of* $A_{(y,0)}[e^{2t}+\cosh(2t)]$, *where*

$$A_{y,z}=\begin{cases}\dfrac{\{26H_{y,1}+A_{y,1}-T\}-\{2^{y}A_{y/2,0}\}}{2^{y}} & y<m \quad y: even\\[2ex] \dfrac{\{26H_{y,1}+A_{y,1}-T\}}{2^{y}} & y<m \quad y: odd\\[2ex] \dfrac{\{26H_{y,1}+A_{y,1}-T\}-\{2^{2y-m}A_{y-[\frac{m}{2}],0}\}}{2^{y}} & y\geq m \quad y: even\\[2ex] \dfrac{\{26H_{y,1}+A_{y,1}-T\}-\{2^{2y-m-1}A_{y-[\frac{m+1}{2}],0}\}}{2^{y}} & y\geq m \quad y: odd\end{cases} \tag{27}$$

So that $m = \begin{cases} \dfrac{2v}{3} & \textit{for all } \ v \in 3Z \\ \dfrac{2v+1}{2^y} & \textit{for all } v \notin 3Z \end{cases}$

where v represents the length of the ciphertext

4. Conclusion

This research introduces a novel cryptographic method employing the Kashuri Fundo transform of linear combinations of functions. A key advantage of this algorithm lies in its capability to produce diverse output alphabets from identical input alphabets, achieved by adjusting parameters such as $'x','u','z','T'$, or all values simultaneously (as shown in Result 3). The utilization of linear combinations of functions enhances the cipher text length, thereby bolstering

4.1 This cryptosystem transforms plaintexts of even length a into ciphertexts of length 3a/2, and plaintexts of odd length b into ciphertexts of length $\frac{(3b+1)}{2}$.

4.2 Similar methodologies can be developed using the KFT of appropriate functions. Additionally, analogous outcomes can be achieved through combinations of various transforms. Therefore, there is potential for extending this research further.

4.3 The process presented in this research is valuable in cryptosystems employing dynamical keys, effectively mitigating the risk of cryptanalysis attacks.

4.4 There is potential to demonstrate that our algorithm can defend against various attacks. For instance, a Brute-Force attack relies on numerous trial-and-error attempts to receive the useable key, leveraging the foe's lack of algorithmic knowledge. By employing different values of $'x','u','T'$, *or combinations thereof, we add an additional layer of protection. Suppose we use z iterations, each with distinct values of* $'x','u',\text{and}'T'$. *In such a scenario, it becomes challenging for an attacker to discern* $3 * z$ *unique random numerals. In selected plain text and selected cipher text where the foe, where the attacker has knowledge of certain* $A_{(y,z)}$ *and* $A_{(y,z-1)}$ *values, it remains difficult for them to deduce the random numbers* $'x','u','T'$, *and the key*H *with just this information. Therefore, there are numerous avenues for further extending this work.*

REFERENCES

[1] Subhranil Som, Joytsna Kumar Mandal, and Soumya Basu. A genetic functions based cryptosystem (gfc). *IJCSNS*, 9(9):310, 2009.

[2] Douglas R Stinson. Cryptography: theory and practice. Chapman and Hall/CRC, 2005.

[3] L Vinothkumar and V Balaji. Encryption and decryption technique using matrix theory. *Journal of computational Mathematica*, 3(2):1–7, 2019.

[4] BS Sahana Raj and Venugopalachar Sridhar. Identity based cryptography using matrices. *Wireless Personal Communications*, 120(2):1637–1657, 2021.

[5] Baizhu Ni, Rabiha Qazi, Shafiq Ur Rehman, and Ghulam Farid. Some graph-based encryption schemes. *Journal of Mathematics*, 2021(1):6614172, 2021.

[6] G Naga Lakshmi, B Ravi Kumar, and A Chandra Sekhar. A cryptographic scheme of laplace transforms. *International Journal of Mathematical Archive*, 2(12):2515–2519, 2011.

[7] AP Hiwarekar. Encryption-decryption using laplace transforms. Asian Journal of Mathematics and Computer Research, *International Knowledge Press*, 12(3):201–209, 2016.

[8] Jadhav Shaila Shivaji and AP Hiwarekar. New method for cryptography using laplace-elzaki transform. *Psychology and Education Journal*, 58(5), 2021.

[9] Akinola Emmanuel Idowu, Alao Saheed, Oderinu Rasaq Adekola, and Folorunso Esther Omofa. An application of integral transform based method in cryptograph. *Asian Journal of Pure and Applied Mathematics*, pages 13–18, 2021.

[10] Emmanuel Oluseye Adeyefa, Lukman Shina Akinola, and Oluwaferanmi David Agbolade. Application of laplace transform to cryptography using linear combination of functions. *TWMS Journal of Applied and Engineering Mathematics*, 2021.

[11] Marcelo Sampaio de Alencar. Cryptography and Network Security. River Publishers, 2022.

[12] Bashar Ahmed Sharba, Roaa Razaq Al-Khalidy, and Raghad I Hussein. A new approach of cryptography using taylor series of logarithm function.

[13] PP Raut and AP Hiwarekar. New method of cryptography with python code using elzaki transform and linear combination of function. *Communications in Mathematics and Applications*, 14(3):1245, 2023.

[14] Nada Sabeeh Mohammed and Emad A Kuffi. The complex integral transform complex sadik transform of error function. *Journal of Interdisciplinary Mathematics*, 26(6):1145–1157, 2023.

[15] Nada Sabeeh Mohammed and Emad A Kuffi. Implementation of the cst complex sadik transform to treat population expansion and decay problems. *Journal of Interdisciplinary Mathematics*, 26(6):1261–1271, 2023.

[16] Nada Sabeeh Mohammed and Emad A Kuffi. Perform the csi complex sadik integral transform in cryptography. *Journal of Interdisciplinary Mathematics*, 26(6):1303–1309, 2023.

[17] Emad A. Kuffi and Nada Sabeeh Mohammed. A modern technique of encryption using the integral sadik transform with the taylor series. In *BIO Web of Conferences*, volume 97, page 00166. EDP Sciences, 2024.

[18] Haldun Alpaslan Peker and Fatma Aybike Cuha. Application of kashuri fundo transform to decay problem. *Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, 26(3):546–551, 2022.

[19] Haldun Alpaslan Pekera, Fatma Aybike Cuha, and Bilge Peker. Solving steady heat transfer problems via kashuri fundo transform. *Thermal Science*, 26(4 Part A):3011–3017, 2022.

[20] Fatma Aybike Cuha and Haldun Alpaslan Peker. Solution of abels integral equation by kashuri fundo transform. *Thermal Science*, 26(4 Part A):3003–3010, 2022.

[21] Haldun Alpaslan Peker, Fatma Aybike Cuha, and Bilge Peker. Kashuri fundo transform for solving chemical reaction models. In *Proceedings of International E-Conference on Mathematical and Statistical Sciences: A Selcuk Meeting*, Konya, pages 145–150, 2022.

[22] HA Peker and FA Cuha. Solving one-dimensional bratus problem via kashuri fundo decomposition method. *Romanian Journal of Physics*, 68(5–6), 2023.