Mathematical modeling for cryptography using Mayan technique

Nour K. Salman[1], Aldhlki,Talat Jassim[1], Emad A. Kuffi[1], Ahmad Qazza[2] and Rania Saadeh[3]

Zakaria Che Muda[4]

[1] *Department of Mathematics, College of Basic Education, Mustansiriyah University, Iraq Baghdad.*
noorkareem94@uomustansiriyah.edu.iq (N.S), dr.talatjassim.edbs@uomustansiriyah.edu.iq(A.J.),
emad.kuffi@uomustansiriyah.edu.iq (E.K)
[2] *Department of Mathematics, Faculty of Science, Zarqa University, Zarqa 13110, Jordan.*
aqazza@zu.edu.jo
[3] *Department of Applied Science, Ajloun College, Al-Balqa Applied University, Ajloun, Jordan.*
r.saadeh@bau.edu.jo
[4] *Faculty of Engineering and Quantity Surveying INTI-IU University, Nilai, Malaysia.*
zakaria.chemuda@newinti.edu.my

ABSTRACT: One of the most important challenges in today's digitally interconnected society is ensuring the secrecy of digital information. As communication networks keep growing, protecting data from unwanted access has become more and more important to both adversaries and defenders. As strong mathematical tools that support a variety of cryptography frameworks, integral transformations have gained popularity. The Mayan integral transform is used in a symmetric-key cryptosystem in this paper, and an actual encryption–decryption scenario is used to illustrate how well it works. The results illustrate the efficacy of the Mayan transform in generating safe ciphertext and accurately recovering plaintext, highlighting its potential as a valuable technique for modern data protection and broader information security applications.

Keywords: Mayan integral transform, Cryptosystem, Symmetric key system, Asymmetric key system, peacekeeping, Cybercrime, Transparent institutions.

1. Introduction

Modern communication systems have made protecting digital information from misuse, manipulation, and illegal access a top priority. Since large volumes of data are transferred over open networks, trustworthy systems that can convert readable data into a protected format are necessary to guarantee confidentiality and integrity. In order to prevent adversaries from taking advantage of sensitive material while it is being sent, cryptography transforms plaintext into ciphertext that only authorized parties may decipher [1].

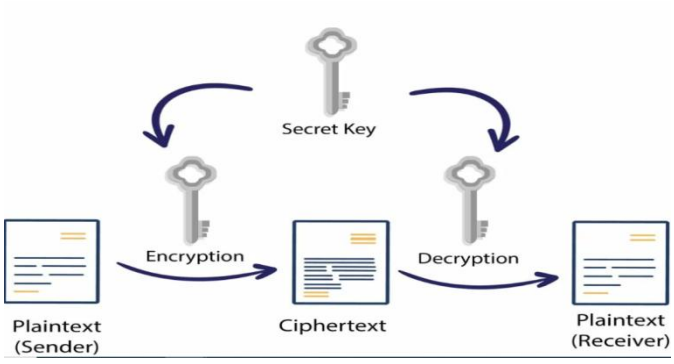

Figure 1. Main build of cryptosystems

The creation of cryptographic systems based on sophisticated mathematical transformations, like the Mayan integral technique, has become crucial to guaranteeing secure digital communication and bolstering institutional trust in light of the fast increase in cybercrime and the global movement toward transparent institutions, as highlighted by the UN Sustainable Development Goals.

The functional framework that makes encryption and decryption possible is described by a cryptosystem. Employing a key and an encryption algorithm, these systems allow the sender to produce ciphertext that may subsequently be transmitted across open channels. The recipient then utilizes a decryption technique, employing either the same key or an alternative, to get the original message [2]. Cryptographic methods may be categorized into two types based on the keying process: symmetric-key systems, in which communicating parties utilize a single secret key, and asymmetric-key systems, which employ distinct public and private keys. Contemporary applications frequently employ both methodologies to enhance efficiency and security [1].

Integral transforms have been frequently used in several scientific fields and have important applications in cryptography design according to their capacity to produce complicated non-trivial mappings [3]. Different approaches utilizing both classical and contemporary integral transforms—namely Laplace, Kamal, Mahgoub, Mohand, and Aboodh—have exhibited efficacy in encryption and decryption operations [4–6]. Notwithstanding this advancement, the newly formulated Mayan integral transform remains little investigated, despite its generic framework and adaptability indicating significant promise for cryptographic applications [5].

In this article, a novel cryptographic approach for secret systems based on the Mayan integral transform is proposed and discussed through a real-world example, demonstrating the potential of using such a promising novel complex transform in the rapidly expanding field of data security. Many scholars have employed integral transformations, particularly in the last few decades, as one of the most crucial methods for text and picture encryption [15–22].

What distinguishes the Mayan transform Integration technique is its complex transform form and conditions, which is why this technique has been used in text encryption. The use of integral transformations with their inverses and series of basic functions such as polynomials, trigonometric and hyperbolic functions, or sometimes their combination, is characterized by the ease of its computational operations in encryption and decryption algorithms[15-23].

In many mathematical applications, stability analysis and better inequalities are crucial, as demonstrated by recent developments in operator theory and functional analysis. For spectrum theory and numerical analysis, the accuracy of operator estimates in Hilbert spaces is crucial, and Hazaymeh et al. [24] and Qawasmeh et al. [25] have developed stronger and more precise numerical radius inequalities to increase this precision. In support of these results, Qazza and Hatamleh [26] developed solutions for semi-linear abstract differential equations with infinite B-chains. This paper lays the theoretical groundwork for the management of complex dynamical systems with infinite dimensions. Stochastic integral equations and random systems are clarified by Qazza, Hatamleh, and Alodat's investigation of the stability of Volterra integral equation solutions with random kernels [27]. All these methods improve our understanding of operator inequalities and solution stability in many mathematical frameworks, as well as deterministic and stochastic analysis.

2. Mayan Transform Technique

A new mathematical tool that was created to expand and generalize the behavior of classical integral transforms is the Mayan integral transform. The Mayan transform can be expressed as follows [1] for a function $f(x)$ defined on the interval $[0,\infty)$:

$$MA\{f(x)\} = M(v) = \frac{1}{v^{ib}}\int_0^{\infty} e^{-v^{ia}x} f(x)dx$$

where v is a complex valued parameter satisfies $v \neq 0$.

To ensure the existence of the transform, it is assumed that $f(x)$ is a piecewise continuous on $[0,\infty)$ and satisfying $|f(x)| \leq Me^{\mu x}$, then $M(v)$ exists $\forall\ v^{ia} > \mu$.

Since,

$\|M(v)\| = \left|\frac{1}{v^{ib}}\int_0^{\infty} e^{-v^{ia}x} f(x)dx\right| \leq \frac{1}{v^{ib}}\int_0^{\infty} e^{-v^{ia}x}|f(x)|dx \leq \frac{1}{v^{ib}}\int_0^{\infty} e^{-v^{i}ax} Me^{\mu x}dx \leq \frac{M}{v^{ib}(v^{ia}-\mu)}$,
the statement is valid.

The correspondence inverse Mayan transform is given by:

$$(MA)^{-1}\{M(v)\} = f(t) = \frac{1}{2\pi i}\lim_{\tau\to 0}\int_{\delta-i\tau}^{\delta+i\tau} v^{ib}\ e^{-v^{ia}x} M(v)dv,$$

In general , $v = \delta + i\tau$ with δ and τ being real numbers.

2.1. Linearity of the Mayan method

The Mayan transform is a linear transform , the linearity of the transform can be stated as [4]:

If $MA\{Af_1(x)\} = \mathrm{M}_1(v)$ and $MA\{Bf_2(x)\} = \mathrm{M}_2(v)$,

$MA\{Af_1(x) + Bf_2(x)\} = A\ MA\{f_1(x)\} + B\ MA\{f_2(x)\} = A\ \mathrm{M}_1(v) + B\ \mathrm{M}_2(v)$.

Where A and B are constants.

2.2. Mayan transform for some basic functions

This study assumes the existence of all elementary functions (both algebraic and transcendental) and related Jafari transformations [2].

$MA\{k\} = kv^{-i(a+b)}$.

$\mathrm{MA}\{x\} = \mathrm{v}^{-\mathrm{i}(2\mathrm{a}+\mathrm{b})}$

$\mathrm{MA}\{x^2\} = 2\mathrm{v}^{-\mathrm{i}(3\mathrm{a}+\mathrm{b})}$, $\mathrm{Re(v)} > 0$

$\mathrm{MA}\{x^n\} = \mathrm{n!}\,\mathrm{v}^{-\mathrm{i}((\mathrm{n}+1)\mathrm{a}+\mathrm{b})}$, , $\mathrm{n} \in \mathbb{N}$ $\mathrm{Re(v)} > 0$.

$MA\{e^{qx}\} = \frac{1}{v^{ib}(v^{ia}-q)}$, $Re(v^{ia} - q) > 0$

$MA\ \{\sin(qx)\} = \frac{\mathrm{q}}{v^{ib}(v^{2ia}+\mathrm{q}^2)}$

$$MA\{\cos(qx)\} = \frac{v^{ia}}{v^{ib}(v^{2ia}+q^2)}$$

$$MA\{\sinh(qx)\} = \frac{\mathrm{q}}{v^{ib}(v^{2ia}-q^2)} \ , (v^{ib}(v^{2ia} - \mathrm{q}^2)\ ) > 0.$$

$$MA\{\cosh(qx)\} = \frac{v^{ia}}{v^{ib}(v^{2ia}-q^2)} , (v^{ib}(v^{2ia} - \mathrm{q}^2)\ ) > 0.$$

3. The suggested cryptography technique

The cryptographic framework proposed in this study is designed as a symmetric (secret-key) system, where both communicating parties share the same key for the encryption and decryption processes. Consequently, the security of the system relies on the confidentiality of this shared key, which must remain known exclusively to the sender and the intended receiver [6].

All characters are encoded using the expanded ASCII system, which offers 256 distinct symbols, in order to standardize the representation of textual data. This makes it easier to convert characters into the numerical values needed for the encryption process and guarantees compatibility with a variety of input formats [7].

The ciphertext is created from the encoded plaintext values during the encryption phase using the Mayan integral transform. At the receiving end, the original number sequence is recovered using the matching inverse Mayan transform and then transformed back into legible characters. A reversible yet highly structured transformation of data appropriate for safe transmission is made possible by this combination of the direct and inverse Mayan transforms, which forms the basis of the suggested cryptographic approach.

3.1. Encryption Algorithm Technique.

The sender must execute the following procedures in order to convert the readable plaintext into unintelligible ciphertext. An unprotected channel will be used to send the ciphertext that is being produced.

Step one:

Each character in the plaintext of length N is translated into its corresponding decimal value using the extended ASCII table. This ensures that the input text is represented numerically before any transformation is applied.

Step two:

The obtained ASCII values are arranged into a finite sequence referred to as the H-sequence,

$$H = \{h_0, h_1, h_2, \dots, h_{\{N-1\}}\},$$

which forms the basis for constructing the encryption polynomial.

Step three:

The polynomial created by inserting the H-sequence's components as coefficients

$$\sum_{i=0}^{N-1} h_i x^i,$$

where r is a random constant chosen beforehand and agreed upon by both sender and receiver. Thus, the polynomial takes the form

$$\sum_{i=0}^{N-1} h_i r^i x^i.$$

Step four:

Mayan transform is used to the generated polynomial function, as: $MA\{f(x)\} = MA\{H\, x \cosh(px)\}$.

Step five:

Using the formula $z_i = M_i mod 200$, where $i = 0, 1, 2, \dots, N-1$, and M_i is the coefficients of the polynomial function from step four, the decimal "ASCII code" encoding of the cipher text is evaluated.

The ciphertext's decimal "ASCII" encoding is converted back into its corresponding ASCII characters for transmission over an unprotected channel [8].

Step six:

The decryption key is generated through

$$L_i = \frac{(M_i - z_i)}{200}, \qquad i = 0,1,2, \dots, N-1,$$

and is transmitted on an encrypted connection to the receiver. In order to recreate the polynomial during the decryption phase, this key is necessary.

3.1.1. Encryption example

To explain the functioning of the proposed encryption technique, consider the following practical example.

Before commencing the encryption process, imagine that both communication parties have agreed in advance to use the random number r=2 as the common parameter for encryption and decryption. This value, coupled with the associated decryption key produced subsequently, is sent securely over a secured communication channel [9].

Step one:

Let the plaintext message to be transmitted over the unsecured channel be:

ACADEMICS

The message contains $N = 9$ characters. Converting each character into its decimal extended ASCII representation yields:

$$A = 65, \qquad C = 67, \qquad A = 65, \qquad D = 68, \qquad E = 69, \qquad M = 77, \qquad I = 73,$$

$$C = 67, \qquad S = 83.$$

Step two:

The plaintext sequence (H finite sequence) is:

$$H_0 = 65, \quad H_1 = 67, \quad H_2 = 65, \quad H_3 = 68, \quad H_4 = 69, \quad H_5 = 77, \quad H_6 = 73, \quad H_7 = 67, \quad H_8 = 83, \quad H_n = 0$$

for $n \geq 9$.

Step three:

The following polynomial function will be fitted with the finite H sequence parameters as coefficients:

$$f(x) = H_0 x + H_1 \frac{p^2 x^3}{2!} + H_2 \frac{p^4 x^5}{4!} + H_3 \frac{p^6 x^7}{6!} + H_4 \frac{p^8 x^9}{8!} + H_5 \frac{p^{10} x^{11}}{10!} + H_6 \frac{p^{12} x^{13}}{12!} + H_7 \frac{p^{14} x^{15}}{14!} + H_8 \frac{p^{16} x^{17}}{16!}.$$

Substituting $p = 2$ produces:

$$f(x) = 65x + 67\frac{2^2 x^3}{2!} + 65\frac{2^4 x^5}{4!} + 68\frac{2^6 x^7}{6!} + 69\frac{2^8 x^9}{8!} + 77\frac{2^{10} x^{11}}{10!} + 73\frac{2^{12} x^{13}}{12!} + 67\frac{2^{14} x^{15}}{14!} + 83\frac{2^{16} x^{17}}{16!}.$$

Step four:

Applying the Mayan transform to each term gives:

$$MA\{f(x)\} = MA\{65x\} + MA\{67\frac{2^2 x^3}{2!}\} + MA\{65\frac{2^4 x^5}{4!}\} + MA\{68\frac{2^6 x^7}{6!}\} + MA\{69\frac{2^8 x^9}{8!}\} + MA\{77\frac{2^{10} x^{11}}{10!}\} + MA\{73\frac{2^{12} x^{13}}{12!}\} + MA\{67\frac{2^{14} x^{15}}{14!}\} + MA\{83\frac{2^{16} x^{17}}{16!}\}.$$

This results in:

$$MA\{f(x)\} = 65v^{-i(2a+b)} + 804\, v^{-i(4a+b)} + 5200\, v^{-i(6a+b)} + 30464v^{-i(8a+b)} + 158976\, v^{-i(10a+b)} + 867328\, v^{-i(12a+b)} + 3887104\, v^{-i(14a+b)} + 16465920\, v^{-i(16a+b)} + 92471296\, v^{-i(18a+b)}.$$

Step five:

The ciphertext values are computed as:

$$z_i = M_i \, mod \, 200,$$

yielding:

$$z_0 = 65 \, mod \, 200 = 65$$

$$z_1 = 804 \, mod \, 200 = 4$$

$$z_2 = 5200 \, mod \, 200 = 0$$

$$z_3 = 30464 \, mod \, 200 = 64$$

$$z_4 = 158976 \, mod \, 200 = 176$$

$$z_5 = 867328 \, mod \, 200 = 128$$

$$z_6 = 3887104 \, mod \, 200 = 104$$

$$z_7 = 16465920 \, mod \, 200 = 120$$

$$z_8 = 92471296 \, mod \, 200 = 96$$

These values correspond to the ASCII characters:

A♦@ÇhxՀ.

Step (6):

The decryption key is computed using:

$$L_i = \frac{(M_i - z_i)}{200},$$

Resulting in

$$L_0 = 0, \quad L_1 = 4, \quad L_2 = 26\,, \quad L_3 = 152\,, \quad L_4 = 794, \quad L_5 = 4336, L_6 = 19435,$$
$$L_7 = 82329\,, \quad L_8 = 462356.$$

3.2. **Decryption Algorithm Technique**.

In order to recover the original plaintext from the ciphertext received via the unprotected communication channel, the receiver must perform the decryption procedure. The process is described in the steps that follow. [10]

Step one:

The decryption key k_i and the random number r are sent via a secure channel to the recipient before decryption starts. At the same time, an unprotected channel receives the ciphertext itself. The decryption key and the ciphertext are both necessary for reassembling the original communication.

Step two:

Each character of the received ciphertext is converted into its corresponding decimal ASCII value. If the ciphertext has length N, this results in the sequence:

$$Z = \{z_0, z_1, \dots, z_{\{N-1\}}\}.$$

Step three:

The sequence of coefficients for the polynomial function that would be used in the inverse Mayan approach is generated using the decryption key that was received.

The polynomial function that would be used in the inverse Mayan approach can be generated using the following formula:

$$\left\{\frac{-\mathrm{d}}{da}\right\} \frac{v^{ia}}{v^{i\beta}(v^{2ia} - 2^2)} = \sum_{n=0}^{N-1} M_i v^{-i\left((2n+2)a+b\right)}.$$

With the coefficients M_i could be evaluated via $M_i = 200\, L_i + z_i'$

Step four:

Using the inverse Mayan transform on the polynomial function created in step three would yield the "ASCII decimal codes" of the plaintext. The following is the formula for applying the inverse Mayan approach to the specified polynomial function:

$$f(x) = MA^{-1}\{\sum_{n=0}^{N-1} M_i v^{-i((2n+2)a+b)}\}$$

Step five:

Finally, each recovered ASCII value is converted back into its character representation. This produces the original plaintext message exactly as it was before encryption.

3.2.1. Decryption example

The following example will be examined in order to illustrate the decryption algorithm approach of the proposed cryptographic mathematical form [11].

Step one:

The decryption key and the following random number were received over secure channel:

$p = 2$ and (L_i) , with i = 0, 1, 2 ...,8 is

$$0, 4, 26, 152, 794, 4336, 19435, 82329 ,462356.$$

With the following cipher text received by unsecured channel is:

A♦@▒Çhx`

Step two:

The decimal "ASCII" encoding of the received ciphertext has a finite sequence that is:

$$z_0' = 65, \quad z_1' = 67, \quad z_2' = 65, \quad z_3' = 68, \quad z_4' = 69, \quad z_5' = 77, \quad z_6' = 73,$$
$$z_7' = 67, \quad z_8' = 83$$

Step three:

Applying the given key (L_i) for i= 0,1,2,…,8 the coefficients of the infinite sequence is generated via :

$MA\left\{\frac{-\mathrm{d}}{da}\right\}\frac{v^{ia}}{v^{i\beta}(v^{2ia}-2^2)} = \sum_{n=0}^{N-1} M_i v^{-i((2n+2)a+b)}$ with $M_i = 200\, L_i + z_i'$,for i=0,1,2,… ,8.

$M_0 = 65$

$M_1 = 804$

$M_2 = 5200$

$M_3 = 30464$

$M_4 = 158976$

$M_5 = 867328$

$M_6 = 3887104$

$M_7 = 16465920$

$$M_8 = 92471296$$

So

$$MA\left\{\frac{-\mathrm{d}}{da}\right\}\frac{v^{ia}}{v^{i\beta}(v^{2ia}-2^2)} = \sum_{n=0}^{N-1} M_i v^{-i((2n+2)a+b)}\, 65v^{-i(2a+b)} + 804\, v^{-i(4a+b)} + 5200\, v^{-i(6a+b)} + 30464v^{-i(8a+b)} + 158976\, v^{-i(10a+b)} + 867328\, v^{-i(12a+b)} + 3887104\, v^{-i(14a+b)} + 16465920\, v^{-i(16a+b)} + 92471296\, v^{-i(18a+b)}$$

Step four:

Applying the inverse Mayan transform to $f(x)$ produces:

$$MA^{-1}\{f(x)\} = MA^{-1}\{65v^{-i(2a+b)} + 804\, v^{-i(4a+b)} + 5200\, v^{-i(6a+b)} + 30464v^{-i(8a+b)} + 158976\, v^{-i(10a+b)} + 867328\, v^{-i(12a+b)} + 3887104\, v^{-i(14a+b)} + 16465920\, v^{-i(16a+b)} + 92471296\, v^{-i(18a+b)}\}$$

$$f(x) = 65x + 67\frac{2^2x^3}{2!} + 65\frac{2^4x^5}{4!} + 68\frac{2^6x^7}{6!} + 69\frac{2^8x^9}{8!} + 77\frac{2^{10}x^{11}}{10!} + 73\frac{2^{12}x^{13}}{12!} + 67\frac{2^{14}x^{15}}{14!} + 83\frac{2^{16}x^{17}}{16!}$$

Step five:

Finally, converting these ASCII values back into characters yields:

ACADEMICS.

Thus, the decryption process successfully reconstructs the original message without any loss or alteration.

4. Discussion of Results and Conclusions

The Mayan integral transform may yield an array of fundamental functions, such as trigonometric, hyperbolic, and exponential forms, by employing the complex parameters $v^{-i\alpha}$ and $v^{-i\beta}$. This adaptability offers considerable flexibility for applications necessitating varied functional structures, making the transform an essential tool for computational analysis and mathematical modeling [12].

This kind of functional richness is very beneficial to the field of cryptography. By making cryptanalysis more difficult for would-be attackers, transform-based encryption's intrinsic complexity and nonlinearity give it a tactical edge and improve data security [13].

In this paper, a new symmetric-key cryptography architecture based on the Mayan integral transform is presented and investigated. Because it does not rely on pre-existing functional templates for encryption or decryption, the proposed methodology is intrinsically universal. To verify its feasibility, a comprehensive demonstration was carried out that included both the encryption of plaintext and the subsequent decoding of the initial message. The results show that the Mayan transform can produce secure ciphertext and reliably recover plaintext, indicating its potential as a useful tool for data-security applications [14].

Moreover, the intricate parameters of the transform simplify and improve the efficiency of the underlying computing procedures. These parameters streamline the series expansions and inverse operations utilized during the encryption and decryption stages, increasing the method's overall utility.

According to all of the findings, the Mayan integral transform could serve as the mathematical foundation for developing modern encryption systems.

References

[1] E. A. Mansour, E. A. Kuffi "The Mayan Transform: A Novel Integral Transform of Complex Power Parameters"

[2] E. A. Mansour, S. Mehdi, and E. A. Kuffi, "The new integral transform and its applications," Int. J. Nonlinear Anal. Appl., vol. 12, no. 2, pp. 849–856, 2021.

[3] M. T. Gençoğlu, "Use of integral transform in cryptology," Sci. Eng. J Fırat Univ, vol. 28, no. 2, pp. 217–220, 2016.

[4] M. T. Gençoğlu, "Cryptanalysis of a new method of cryptography using laplace transform hyperbolic functions," Commun. Math. Appl., vol. 8, no. 2, pp. 183–189, 2017.

[5] G. N. Lakshmi, B. R. Kumar, and A. C. Sekhar, "A cryptographic scheme of Laplace transforms," Int. J. Math. Arch., vol. 2, no. 12, pp. 2515–2519, 2011.

[6] M. Mohand and A. Mahgoub, "The new integral transform 'Mohand Transform,'" Adv. Theor. Appl. Math., vol. 12, no. 2, pp. 113–120, 2017.

[7] C. Jayanthi and V. Srinivas, "Mathematical modeling for cryptography," Int. J. Math. Trends Technol., vol. 65, no. 2, pp. 10–15, 2019.

[8] C. Paar and J. Pelzl, Understanding cryptography: a textbook for students and practitioners. Springer Science & Business Media, 2009.

[9] A. Kahate, Cryptography and network security. Tata McGraw-Hill Education, 2013.

[10] A. Kamal and H. Sedeeg, "The New Integral Transform''Kamal Transform'','' Adv. Theor. Appl. Math., vol. 11, no. 4, pp. 451–458, 2016.

[11] A. K. H. Sedeeg, M. M. AbdelrahimMahgoub, and M. A. SaifSaeed, "An Application of the New Integral 'Aboodh Transform' in Cryptography," Pure Appl. Math. J., vol. 5, no. 5, pp. 151–154, 2016.

[12] A. Stanoyevitch, Introduction to Cryptography with mathematical foundations and computer implementations. CRC Press, 2010.

[13] P. S. Kumar and S. Vasuki, "An Application of MAHGOUB Transform in Cryptography," Adv. Theor. Appl. Math., vol. 13, no. 2, pp. 91–99, 2018.

[14] W. Zhang, Y. Zhao, and S. Fan, "Cryptosystem Identification Scheme Based on ASCII Code Statistics," Secur. Commun. Networks, vol. 2020, 2020.

[15] E. A. Kuffi, S. A. Mehdi, E. A. Mansour, "Color Image Encryption Based on New Integral Transform SEE", Conference Series, 2322 (2022) 012016.

[16] N. S. Mohammed , E. A. Kuffi, "Perform the CSI complex Sadik integral transform in cryptography", Journal of Interdisciplinary Mathematics, Vol. 26 (2023), No. 6, pp. 1303–1309.

[17] E. A. Mansour, E. A. Kuffi, S. A. Mehdi, "Applying SEE Integral Transform in Cryptography", Samarra Journal of Pure and Applied Science, 16/12/2021.

[18] E. A. Mansour, E. A. Kuffi, S. A. Mehdi, "Applying Complex SEE Transformation in Cryptography", MJPS, VOL.(8), NO.(2), 2021.

[19] E. A.Kuffi and N. S. Mohammed, "A Modern Technique of Encryption Using The Integral Sadik Transform With The Taylor Series", BIO Web of Conferences 97, 00166 (2024).

[20] E. A. Kuffi ,"Perform The Complex EFG Transform in Cryptography ",Journal of University of Anbar for Pure Science (JUAPS) , 2024,(18), (01):252– 256.

[21] J. A. Jasim , M. R. Ali , E. A. Kuffi ,"Application of a new integral "KAJ Transform" technique in cryptography", Journal of Discrete Mathematical Sciences & Cryptography.

[22] P. S. JosephNg, Z. C. EricMok, K. Y. Phan, J. Sun and Z. Wei, Mitigating Social Media Cybercrime Revolutionising with AES Encryption and Generative AI. Journal of Advanced Research in Applied Sciences and Engineering Technology, 2024, *46*(2), 124-154.
[23] A. I. El-Mesady, Y. S. Hamed, and A. M. Alsharif, "Jafari Transformation for Solving a System of Ordinary Differential Equations with Medical Application," Fractal Fract., vol. 5, no. 3, p. 130, 2021.
[24] A. Hazaymeh, A. Qazza, R. Hatamleh, M. W. Alomari, an R. Saadeh (). On further refinements of numerical radius inequalities. Axioms, 2023, 12(9), 807.
[25] A. Qazza, and R. Hatamleh. The Existence of a Solution for Semi-Linear Abstract Differential Equations With Infinite B-Chains of the Characteristic Sheaf. International Journal of Applied Mathematics, 2018, 31(5), 611–620.
[26] A.M. Qazza, R.M. Hatamleh and N.A. Alodat. About the solution stability of Volterra integral equation with random kernel. Far East Journal of Mathematical Sciences, 2016, 100(5), 671.
[27]T. Qawasmeh, A. Qazza, R. Hatamleh, R. M.W. Alomari and R. Saadeh. Further accurate numerical radius inequalities. Axioms, 2023, 12(8), 801.