ISSN 0304-9892 (Print) ISSN 2455-7463 (Online)

Jñānābha ज्ञानाभ

(HALF YEARLY JOURNAL OF MATHEMATICAL SCIENCES)
[Included : UGC-CARE List]

Volume 55(I)

SPECIAL ISSUE

Proceedings: 5th International Conference and Golden Jubilee Celebrations of VPI (IC-RA-MSA-ET 2022) JNU, New Delhi, India

JULY 2025

Published by :

The Vijñāna Parishad of India
विज्ञान परिषद ऑफ इण्डिया
[Society for Applications of Mathematics]
DAYANAND VEDIC POSTGRADUATE COLLEGE
(Bundelkhand University)
ORAI-285001, U. P., INDIA
www.vijnanaparishadofindia.org/jnanabha

ISSN 0304-9892 (Print) ISSN 2455-7463 (Online)

Jñānābha

ISSN 0304-9892 (Print) ISSN 2455-7463 (Online)
www.vijnanaparishadofindia.org/jnanabha
***Jñānābha* Vol. 55 (I) Special Issue 2025, 1-15**
Proceedings: 5th International Conference and Golden Jubilee Celebrations of VPI (IC-RA-MSA-ET 2022) JNU, New Delhi, India

ADVANCED ENCRYPTION TECHNIQUE USING BISYMMETRIC RHOTRIX AND DNA CODES WITH ELLIPTIC CURVE CRYPTOGRAPHY

[1]Shalini Gupta, [2]Ruchi Narang, [3]Gajendra Pratap Singh, [4]Kritika Gupta and [5]Kamalendra Kumar

[1, 2, 4]Department of Mathematics & Statistics, Himachal Pradesh University, Shimla, India-171005
[3]School of Computational and Integrative Sciences, Jawaharlal Nehru University, New Delhi, India-110067
[5]Department of Basic Science, Shri Ram Murti Smarak, College of Engineering and Technology Bareilly, India-243202
Email: shalini.garga1970@gmail.com, ruchinarang8878@gmail.com, gajendra@gmail.jnu.ac.in, kritika993@gmail.com, kamlendra. 14kumar@gmail.com

(Received: October 09*,* 2024*; In format: December* 07*,* 2024*; Revised: May* 28*,* 2025*; Accepted: July* 13*,* 2025*)*

DOI: https://doi.org/10.58250/jnanabha_SI.2025.55101

Abstract

Within cryptography, various methods like *DES* (Data Encryption Standard), *IDEA* (International Data Encryption Algorithm), and Blowfish are employed to enhance security during encryption and decryption processes. In today's scenario, rhotrices assume a pivotal role in cryptography, utilizing mathematical algorithms for encrypting and decrypting confidential messages. This paper explores the utilization of bisymmetric rhotrix alongside elliptic curve cryptography, and uses *DNA* Codes to devise a secure and robust encryption and decryption algorithm. Here, the message is divided into blocks of 24 characters each. Using a *DNA* code sequence, we combine the string of the first message block with a 128-bit random integer and the private key coordinates to derive an elliptic curve point for encryption. Encryption transforms each message point into a pair of cipher points, authenticated with a digital signature to ensure data integrity. Decryption reverses this process and verifies the signature. This method guarantees secure message exchange, mutual authentication, and data integrity, making it suitable for various cryptographic applications. Additionally, we have implemented this scheme in Python and, through rigorous testing, measured the time required for encryption and decryption, demonstrating our cryptographic approach's efficiency and practical feasibility.

2020 Mathematical Sciences Classification: 12E20; 94A60
Keywords and Phrases: Elliptic curve cryptography, finite field, maximum distance separable rhotrix, *DNA* codes.

1 Introduction

Cryptography, a technology rooted in mathematical science, serves to conceal data through encryption, shielding it from unauthorized access. Utilizing a secret key, designated recipients can decrypt stored confidential information even across insecure channels. Tracing its origins back to 2000 BC as documented by Biggs [3], cryptography derives its name from the Greek "Kryptos," meaning hidden. The discipline is commonly categorized into two main branches: symmetric key and asymmetric key encryption. Symmetric encryption, or single-key encryption, encompasses methods like the Hill cipher algorithm, *AES* (Advanced Encryption Standard), and Blowfish. On the other hand, asymmetric key encryption includes algorithms such as the elliptic curve algorithm, *RSA*, and the Diffie-Hellman key exchange algorithm. In the sphere of Elliptic Curve Cryptography (*ECC*) based mapping and text encryptions, researchers and scientists investigate multiple strategies to improve the security, efficiency, and applicability of these cryptographic methods. A key focus is on optimizing efficiency and performance, particularly by developing *ECC* schemes that demand minimal computation and memory, which is essential for resource-limited environments such as *IoT* devices.

Elliptic curve cryptography, introduced by Miller [19], is distinguished as a robust cryptosystem, offering significantly faster performance compared to the Diffie-Hellman algorithm—which in fact is twenty times faster. Koblitz [13] further advanced *ECC* by introducing an algorithm over a finite field, which is renowned

for its ability to provide uniform security across varying bit sizes, thereby reducing bandwidth requirements and enhancing complexity [14]. *ECC* is a leading algorithm known for being very efficient and offering strong security. To thwart attackers and enhance the security of the data, novel methods are emerging from diverse areas of mathematics, including rhotrix analysis and finite fields [18, 31, 32, 33, 34, 35, 36, 37, 38]. Kumari, *et al.* [16] attempted to provide a secure communication architecture to achieve confidentiality and data integrity more strongly. The proposed system implements a secure system using Elliptic curve cryptography for cryptographic algorithms and integrates the checksum estimation method. For validation and authentication, the cryptographic technique is used.

A key of this research is security analysis, which involves rigidly evaluating the resistance of *ECC*-based schemes to various attacks, including the growing threat of quantum attacks. Privacy and confidentiality are important factors, leading to research into *ECC* protocols that enable anonymous communication and safeguard user privacy using methods like homomorphic encryption. Effective key management strategies are essential, addressing challenges related to key generation, distribution, and revocation to maintain secure *ECC* system. The benefits of *ECC*-based text encryption and mapping schemes are substantial. *ECC* provides robust security based on the elliptic curve discrete logarithm problem, and its efficiency allows for faster computations and reduced resource requirements. This efficiency enhances secure communication protocols, enabling quicker and more secure data exchanges. Proper implementation of *ECC* requires a deep understanding of its mathematical foundations, as errors can lead to vulnerabilities.

Key management is another critical aspect of *ECC*-based schemes. Secure key storage and exchange protocols are essential for maintaining security. Traditional *ECC*-based text encryption schemes often rely on secure channels or protocols to share the code table during initialization. However, these methods can be vulnerable to interception or man-in-the-middle attacks, especially when a secure channel is not available. Adversaries may exploit weaknesses in transmission or compromise the code table, leading to decryption errors or unauthorized access to sensitive information.

Parida, *et al.* [23] proposed a robust elliptic curve based image encryption and authentication model for both grayscale and color images, where the model used the secure Elliptic Curve Diffie-Hellman (*ECDH*) key exchange to compute a shared session key along with the improved *ElGamal* encoding scheme. 3D and 4D Arnold Cat maps are used to effectively scramble and transform the values of plain image pixels. Genç *et al.* [5] proposed a new message encryption algorithm using an elliptic curve over finite fields. This new method converts each character of the message to its hexadecimal unicode value and then separates the value divided into blocks that contain one character.

On the basis of key size, Khan *et al.* [17] focused on, studied, and compared the efficiency in terms of security among the well-known public key cryptography algorithms, namely *ECC* (Elliptic Curve Cryptography) and *RSA* (Rivets Shamir Adelman). Bao [2] analyzed the security of elliptic curves from the performance comparison of *ECC* and *RSA*. Moreover, this paper implemented *RSA* and *ECC* using random private keys, and the sample data input is 64-bit, 8-bit, and 256-bit. Kumar *et al.* [15] proposed a novel approach to enhance image encryption by combining the power of a chaotic map, elliptic curve cryptography, and genetic algorithm. Sharma *et al.* [40, 41] proposed a new text encryption scheme (*TEXCEL*), and image encryption scheme using mapping of the characters to a point on an elliptic curve. Gupta *et al.* [10, 11] used elliptic curve cryptography for implementation and verification of double fold encryption scheme and explained a comprehensive encryption and authentication framework tailored for both grayscale and color images. Furthermore, they presented an asymmetric variant of the Affine-Hill cipher, designed specifically for block-based image encryption to ensure superior cipher image quality

Similar to matrices, rhotrix—a coupled matrix structure—was introduced by Ajibade [1] in 2003. Sani [24] subsequently presented a generalized row-column multiplication method for $n-$dimensional rhotrices. These developments contribute to fortifying cryptographic protocols and bolstering data security in an increasingly interconnected digital landscape. Since its inception, rhotrix literature has developed, attracting numerous researchers to explore its applications in cryptography [6, 7, 8, 9, 25, 27, 28, 29, 30, 39]. Yakubu *et al.* [42, 43] introduced several innovative methods for storing and transmitting data using rhotrices. They use rhotrices for encrypting a secret message in a polygraphic cipher system and inverse of rhotrices for decrypting the message.

A novel cryptosystem is proposed by Namasudra [21] using *DNA* cryptography and *DNA* steganography for the cloud-based *IoT* infrastructure. Here, the confidential data is encrypted by using a long secret key. Then, it is hidden in an image. Thus, the proposed cryptosystem not only hides the data, but also encrypts

the confidential data prior to storing it on the cloud server, and it resists many security attacks in the cloud-based *IoT* infrastructure. Singh *et al.* [26] have discussed many approaches based on *DNA* cryptography with applications and limitations. Zhang *et al.* [44] presented a new image encryption scheme based on *DNA* sequence addition operation and chaos is presented, where, a *DNA* sequence matrix is obtained by encoding the original image and divide the *DNA* sequence matrix into some equal blocks and use the *DNA* sequence addition operation to add these blocks. Then, the *DNA* sequence complement operation was performed to the result of the added matrix by using two Logistic maps.

In the face of technological progress, safeguarding data from attackers remains a paramount challenge. In our current study, we introduce a novel extended version of the *Elgamal* and *ECC* cryptosystems along with encoding and decoding using *DNA*. This enhanced approach employs invertible rhotrices containing elements derived from irreducible polynomials over finite fields. By leveraging this technique, decryption complexity is heightened, and bandwidth usage is minimized. Our proposed cryptosystem guarantees robust security and data authenticity, all while utilizing relatively smaller key sizes compared to alternative systems. Importantly, access and decryption of the data are restricted solely to the intended recipient, ensuring privacy and confidentiality.

1.1 Objectives of the Present Work

Objectives of the present work are:

1. To conduct a thorough background study and improve the literature review on secure and efficient authenticated text encryption and mapping schemes using *ECC*.
2. To use *DNA* coding for the construction of mapping points, which enhances the security of the algorithm.
3. To propose a methodology that maps the characters of a message to points on an elliptic curve and then to the rhotrix. This approach enhances cryptographic security by mapping the characters of the message to points on the elliptic curve. By using elliptic curve coordinates as keys, it ensures robustness. Additionally, it eliminates the traditional need for sharing a code table between sender and receiver, thereby reducing communication overhead.
4. Furthermore, the proposed methodology will be evaluated and validated based on various performance metrics, including encryption time, decryption time, cipher data size, and resistance to different types of attacks.

1.2 Organisation of the Present Work

The rest of the work is organized as follows: Section 2 illustrates the preliminaries necessary for understanding the paper. Section 3 highlights the proposed methodology. Section 4 provides the mathematical workings and proof of the proposed encryption scheme. Section 5 presents experimentation, results, and performance analysis of the proposed scheme. Finally, Section 6 concludes the paper with future scope.Top of Form

2 Preliminaries

2.1 Rhotrix ([1]).

Ajibade defined a 3–dimensional rhotrix, which is in some way between 2×2 and 3×3 matrices as follows:

$$R = \left\langle \begin{array}{ccc} & a & \\ b & h(R) & d \\ & e & \end{array} \right\rangle.$$

Here, $h(R)$ denotes the heart of the rhotrix and $a, b, d, e \in \mathbb{R}$, are elements of an odd dimensional rhotrix. This concept was expanded by Mohammed [20] to generalize a rhotrix of order n as:

$$R_n = \left\langle \begin{array}{ccccccc} \cdots & \cdots & \cdots & a_1 & \cdots & \cdots & \cdots \\ \cdots & \cdots & a_2 & a_3 & a_4 & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{\frac{t-n+2}{2}} & \cdots & \cdots & a_{\frac{t+1}{2}} & \cdots & \cdots & a_{\frac{t+n}{2}} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & a_{t-3} & a_{t-2} & a_{t-1} & \cdots & \cdots \\ \cdots & \cdots & \cdots & a_t & \cdots & \cdots & \cdots \end{array} \right\rangle,$$

where $t = \frac{n^2+1}{2}$, $a_i \in \mathbb{R}$. Here $h(R) = \frac{a_{t+1}}{2}$, is the heart of R_n.

In general notation, we denote a rhotrix as $R = \langle h(R), a_i \rangle$, $1 \leq i \leq t$, $i \neq \frac{t+1}{2}$. Heart oriented rhotrices are well-known in rhotrix literature. The algebra and analysis of rhotrices were defined by Ajibade.

The addition and heart-based multiplication of rhotrices is defined as: If $P = \langle h(P),\ a_i\rangle$ and $Q = \langle h(Q), b_i\rangle$ be two rhotrices, then

$$P + Q = \langle h(P) + h(Q),\quad a_i + b_i\rangle,$$

$$PQ\ = \langle \mathrm{h(P)\ h(Q)}\ ,\ \ a_i\ \mathrm{h(Q)} + b_i\ \mathrm{h(P)}\ \rangle,\ 1 \le i \le t,\ \ i \neq \frac{t+1}{2}.$$

After that, generalization of this heart-based multiplication is given by Mohammed [20]. Sani [25] proposed the alternative multiplication of rhotrices, row column multiplication which is similar to the multiplication of two matrices.

$$PQ = \left\langle \begin{array}{ccc} & af + dg & \\ bf + eg & h(P)\,h(Q) & aj + dk \\ & bj + ek & \end{array} \right\rangle.$$

Then generalization of this row–column multiplication was also later given by Sani [24] as:

$$P_n \circ Q_n = \langle a_{i_1 j_1}, c_{l_1 k_1}\rangle \circ \langle b_{i_2 j_2}, d_{l_2 k_2}\rangle$$
$$= \left\langle \sum_{i_2 j_1 = 1}^{t} (a_{i_1 j_1} b_{i_2 j_2}),\ \sum_{l_2 k_1 = 1}^{t} (c_{l_1 k_1} d_{l_2 k_2}) \right\rangle,\ \ t = \frac{n+1}{2},$$

where P_n and Q_n are $n-$dimensional rhotrices.

2.2 Finite Field ([18]).

A non-empty finite set $\mathbb{F}$ is termed a finite field if it is an abelian group under both addition and multiplication. In computer science, positive integers are typically stored as $n-$bit words, where n can be 8, 16, 32, 64, and so on. Consequently, the maximum range of integers that can be represented is $2^n - 1$.

A Galois field is a finite field containing finite elements. Additionally, $GF(p)$ encompasses the set $\mathbb{Z}_p$, where p denotes the largest prime number less than 2^n. The elements within this field are $n-$bit words, as described in the works of Chen [4] and Hell *et al.* [12].

2.3 Bisymmetric Matrix ([22]).

A bisymmetric matrix is a square matrix which is symmetric about both of its main diagonals. More precisely, an $n \times n$ matrix B is bisymmetric if it satisfies both $B = B^T$ and $BE = EB$ where E is the $n \times n$ exchange matrix. For example

$$B = \begin{bmatrix} a & b & c & d \\ b & f & g & c \\ c & g & f & b \\ d & c & b & a \end{bmatrix},$$

where $a,\ b,\ c,\ d\ f, g$ are real numbers.

2.4 Elliptic Curve Cryptography ([13]).

ECC, introduced in 1986 by Victor Miller and Neil Koblitz, emerged as a viable alternative to traditional public key cryptosystems like *RSA* and *ElGamal*. Mathematically, *ECC* offers robust security and superior performance compared to its counterparts.

The general form of an elliptic curve E is expressed as:

$$y \equiv\ x^3\ +\ ax\ +\ b\ (\mathrm{mod}\ p).$$

In elliptic curves over prime fields $GF(p)$ with $p\ >\ 3$, the parameters a and b must satisfy the condition $4a^3 + 27b^2\ \not\equiv\ 0\ (\mathrm{mod}\ p)$. Points on an elliptic curve are typically represented using affine coordinates. Here, the key operations for working with points on an elliptic curve are:

1. Addition of two points: Given two points $P_1(x_1\ , y_1)$ and $P_2(x_2, y_2)$ on an elliptic curve, the sum of two points $P_3(x_3, y_3) = P_1(x_1, y_1) + P_2(x_2, y_2)$ is calculated, where
$$x_3\ =\ \lambda^2\ -\ x_1 -\ x_2,\ \ y_3 =\ \lambda(x_1 - x_3) - y_1,$$
and
$$\lambda =\ \frac{y_2 - y_1}{x_2 - x_1}.$$
2. Doubling a point $P(x_1, y_1)$, is given by:
$$x_2\ =\ \lambda^2\ - 2x_1,$$
$$y_2 = \lambda(x_1 - x_2) - y_1,$$
where
$$\lambda\ =\ \frac{3{x_1}^2 +\ a}{2y_1}.$$

2.5 DNA Encoding and Decoding ([44]).

A *DNA* sequence contains four nucleic acid bases A (adenine), C (cytosine), G (guanine), and T (thymine), where A and T are complementary, and G and C are complementary. In the binary, 0 and 1 are complementary, so 00 and 11 are complementary, and 01 and 10 are also complementary.

2.5.1 Addition and Subtraction Algebraic Operation for DNA Sequences

With the rapid developments in *DNA* computing, some biology operations and algebraic operations based on the *DNA* sequence have been presented by researchers [20, 25], such as the addition operation. The addition and subtraction operations for *DNA* sequences are performed according to traditional addition and subtraction in the $\mathbb{Z}_2$. For example, $11 + 10 = 01$, $01 - 11 = 10$. The details of the addition and subtraction rules are shown in Tables 2.1 and 2.2. From Table 2.1, we can see that any two rows are complementary, and Table 2.2 is the same. In other words, the addition algebraic operation table is a double helix structure which satisfies the Watson–Crick complement regulation. Subtraction is the inverse operation of addition, but whose structure is not a double helix structure. However, we also can find the complement of every base in the Table 2.2. In this paper, we will use addition rules given in Table 2.1 to obtain mapping point.

Table* 2.1: Addition operation for DNA sequence:*

+	T	A	C	G
T	C	G	T	A
A	G	C	A	T
C	T	A	C	G
C	A	T	G	C

Table* 2.2: Subtraction operation for DNA sequence:*

-	T	A	C	G
T	C	G	T	A
A	A	C	G	T
C	T	A	C	G
C	G	T	A	C

2.6 ECC Encryption Scheme ([13]).

Suppose Alice and Bob are two parties who want to communicate a message securely. They agree on using a specific elliptic curve and a generator point G.

1. Alice chooses her private key n_A.
2. Bob chooses his private key n_B.
3. Alice's public key is generated as $P_A = n_A\ G$.
4. Bob's public key is generated as $P_B = n_B\ G$.

When Alice wants to send a message M to Bob, she uses Bob's public key and a random integer t for encryption. Alice creates the ciphertext $T = \{tG,\ M + t\ P_B\}$. Different values of the random integer t will generate different ciphertexts for the same message, making decryption without the private key difficult. Bob can decrypt the message using his private key. He subtracts $n_B(tG)$ from $M + t\ P_B$ to retrieve the original message M.

2.7 Elliptic curve Diffie-Hellman key exchange ([13]).

Let m and n be the private keys of Alice and Bob, respectively. Alice's public key is $m\ G$ and Bob's public key is $n\ G$. These public keys are exchanged over an open channel. Alice then multiplies her private key with Bob's public key, and Bob multiplies his private key with Alice's public key. Both Alice and Bob will obtain the same result. This method of key exchange between users is known as the Elliptic Curve Diffie-Hellman ($ECDH$) key exchange.

3 Proposed methodology

In the proposed scheme, we begin by using *DNA* codes to map a set of twenty-four characters from the message to the elliptic curve, which introduces advanced cryptographic security. This methodology involves the multiplication of rhotrices: one containing points of the elliptic curve and a bisymmetric rhotrix, to enhance the security. Additionally, we incorporate an extra layer of security by using specific private keys and special private keys. These private keys serve a dual purpose: first, they provide the receiver with a robust means to verify that the ciphertext comes exclusively from the legitimate sender. Second, the specific private key is used in generating the mapping points, while the special private key is employed in the authentication and verification process. Importantly, we use different *DNA* sequences and random points for mapping different blocks of messages, which significantly increases the security level of our proposed methodology.

3.1 System model

Suppose Alice and Bob are two communicating parties and they want to share some message between them. Both Alice and Bob agree on a common elliptic curve with generator point G.

1. Alice chooses a random integer r in such a way that it lies between $[1,\ l\ -\ 1]$, where l is the order of generator point G. Alice keeps n_a as his private key.
2. Alice computes her public key as $P_a = n_a\ G$.
3. Bob selects a large random number n_b in such a way that it lies between $[1,\ l\ -\ 1]$. He keeps n_b as his private key.
4. The public key of Bob is $P_b = n_b\ G$. The public keys of both parties are published.
5. Alice calculates her specific private key, $A_S = n_a\ P_b\ = (a,\ b)$.
6. Bob calculates his specific private key, $B_S = n_b\ P_a = (a,\ b)$.
7. Alice calculates her special private key, $(X,\ Y) = (aG,\ bG)$, where $X = aG = (a_1,\ a_2)$.
8. Bob calculates his special private key, $(X,\ Y) = (aG,\ bG)$, where $Y = bG = (b_1,\ b_2)$.

3.2 Construction of DNA Sequence Table

In our study, we propose a method for constructing a *DNA* sequence table that will be used to encode different blocks of messages using a particular sequence. For this, we will utilize eight different sequences of *DNA* codes. By converting the binary digits of a random number r into integers and dividing that result by 8, we obtain a number between 0 and 7. We will then choose the *DNA* sequence based on the number obtained in the previous step. This approach introduces a level of cryptographic security and reproducibility to the process. We consider eight different sequences of *DNA* codes, with A and T as complements of each other, and C and G as complements of each other, as given in Table 3.1.

Table* 3.1: DNA Codes*

	0	1	2	3	4	5	6	7
00	A	A	T	T	C	C	G	G
01	C	G	C	G	A	T	A	T
10	G	C	G	C	T	A	T	A
11	T	T	A	A	G	G	C	C

1. If we obtain the number 6 by dividing the integral value of a random point by 8, we will use the sixth *DNA* sequence, assigning the value 00 to G, 01 to A, 10 to T, and 11 to C for mapping the first block of the message.
2. For the second block of the message, we will choose the next sequence (the seventh sequence), and so on. This method ensures that each block of the message is mapped using a different *DNA* sequence, thereby enhancing security. Additionally, we will convert the first block of the message into binary form, divide it into blocks of two, and then write the message using the corresponding *DNA* codes.

3.3 Algorithm for Construction of Bisymmetric Rhotrix.

Consider a five-dimensional Bisymmetric rhotrix,

$$B_3 = \left\langle \begin{array}{ccc} & a_0 & \\ a_1 & a_0 & a_1 \\ & a_0 & \end{array} \right\rangle.$$

By the definition given in 2.3, a bisymmetric rhotrix is symmetric about both of its main diagonals.

1. For the construction of the first element of bisymmetric rhotrix, we will *XOR* the first 64 binary bits of r with the last 64 binary bits of r, and the resulting element will be considered as the first element of bisymmetric rhotrix.
2. For the second element of the corresponding row and corresponding column, we will add 1 to the previous element and so on, which only Alice and Bob can determine using their private keys and public keys of each other.

This method allows us to assign all the values and construct a bisymmetric rhotrix, ensuring it remains private to Alice and Bob. For longer messages, we can use more than one bisymmetric rhotrix.

3.4 Mapping scheme

In our novel mapping scheme for character-to-point transformation on the elliptic curve, we introduce a streamlined approach that eliminates the need for a shared code table and enables the simultaneous mapping of twenty-four characters to a single elliptic curve point.

Here is the process:

1. Random point selection: Alice chooses a random integer r of 128 bits and divide it into blocks of two to make the *DNA* sequence. Subsequently, she calculates $rG = (u, v)$.
2. Alice breaks the message into blocks of twenty-four characters $m_1,\ m_2,\ m_3,\ \ldots, m_n$ each and pads last block with zero character if needed. Now, Alice converts the first block m_1 of twenty-four characters into binary digits and divides into blocks of two to make the *DNA* sequence.
3. Converts the $x-$coordinate u of rG and $y-$coordinate v of rG of specific private key into binary bits of length 128 each which are subsequently divided into blocks of two to make the *DNA* sequence.
4. Now Alice adds all *DNA* sequences of random integer r, first block of message m_1 , u and v, using *DNA* addition table. The result is denoted by x_1.
5. Substitutes this point on the elliptic curve to get $y-$coordinate. In case $y-$coordinate does not exist at point x_1. Then by adding 1 to x_1, Alice again tries to find $y-$coordinate and continues this process till Alice gets the $y-$coordinate. Denoting first mapping point as $(x_1,\ y_1)$.
6. Rhotrix mapping: For rhotrix mapping, Alice assigns row-wise entries, first mapping point as first entry of the rhotrix, and second mapping point as second entry and so on to get rhotrix R_3 (say).
7. Rhotrix multiplication: Now, Alice multiplies rhotrix R_3 with bisymmetric rhotrix B_3 to get M. Alice writes each entry of M by a sequence of points.
8. Selection of random point for different message blocks will be taken as different so as to enhance the security level and different random points $(r_1,\ r_2,\ r_3,\ \ldots\ r_n)$ for 2^{nd}, 3^{rd}, 4^{th}, . . . nth block is chosen in the following manner:

$$r_1 = r \ \oplus\ a,$$
$$r_2 = r \ \oplus\ b,$$
$$r_3 = r_1 \oplus\ r_2,$$

and so on.

3.5 Encryption

After mapping, each message point is then encrypted to a pair of cipher points T_1 and T_2.

1. Alice uses same random number r to compute T_1 as
$$T_1 = rG.$$
2. Computes cipher point T_2 as
$$T_2 = M + rP_b + Y.$$

3.6 Authentication

Adding digital signature authentication ensures the integrity and authenticity of the encryption. It guarantees that the message has not been tampered with during transmission, providing an additional layer of security. Alice performs the following steps to achieve authentication.

1. Alice calculates hash value h_S using the following algorithm
$$X = aG = (a_1,\ a_2).$$
Representing the first half of bits and last half of bits of a_1 as a_{11} and a_{12} respectively and similarly first half of bits and last half of bits of a_2 as a_{21} and a_{22} respectively.

2. Computes S as

$$S = a_{11} \oplus a_{12} \ \oplus \ a_{21} \ \oplus \ a_{22}.$$

$$h_S = SHA_{256}(S).$$

3. Computes hash value h_C of cipher text T_2 and then concatinates h_S and h_C to get H as shown below:

$$h_C = SHA_{256}(C).$$

$$H = h_S \parallel h_C.$$

4. Calculates T by performing XOR operation between b_1 and b_2 as follows:

$$T \ = \ b_1 \ \oplus \ b_2.$$

5. Calculates $r^{'}$ using the parameter r as follows:

$$r^{'} = r \ \oplus \ T.$$

6. Evaluates the digital signature $(V, \ W)$ as follows:

$$V = SHA_{256}(H),$$

$$W \ = \ (r^{'} \ - \ V \ ) \text{mod } p.$$

7. Sends the digital signature $(V, \ W)$ and ciphered text T_2 to Bob.

3.7 Verification

For verification, Bob proceeds as follows:

1. Calculates T as

$$\begin{aligned} T = \ & b_1 \ \oplus \ b_2. \\ r = & (W + V) \ \oplus \ T \\ = & (r^{'} \ - \ V + V \ ) \ \oplus \ T \\ = & \ r^{'} \ \oplus \ T \\ = & \ r. \end{aligned}$$

2. Bob calculates hash value h_S using same algorithm,

$$X = aG = (a_1, \ a_2) \, .$$

Representing the first half of bits and last half of bits of a_1 as a_{11} and a_{12} respectively and similarly the first half of bits and last half of bits of a_2 as a_{21} and a_{22} respectively.

3. Computes,

$$S = a_{11} \oplus \ a_{12} \ \oplus \ a_{21} \ \oplus \ a_{22}.$$

$$h_S = SHA_{256}(S).$$

4. Similarly, computes hash value h_C of cipher text T_2 and then concatinates h_S and h_C to get H.

$$h_C = SHA_{256}(C).$$

$$H = h_S \parallel h_C.$$

5. Calculates V from computed hash value H. If,

$$V = SHA_{256}(H),$$

So, if

$$V \ = \ V$$

then the signature is verified.

3.8 Decryption

Here, Bob computes $T_1 = rG$. When Bob gets the cipher text T_2 for each message point M, he decrypts the message using the expression:

$$\begin{aligned} T_2 - Y - n_b T_1 &= M + Y + rP_b - Y - n_b T_1 \\ &= M + rn_b G - n_b rG \\ &= M. \end{aligned}$$

To decode and retrieve the original characters of the message corresponding to the point M, Bob writes all mapping points in rhotrix form and employs the following steps:

1. Bob calculates R_3 using the following step:
$$R_3 = {B_3}^{-1} M.$$
2. From R_3, Bob gets all the mapping points. For the retrieval of the first block of the original message m_1, he subtracts random points $r,\ x_1,\ u,$ and v using the *DNA* subtraction table.
3. After receiving m_1 and by using the *ASCII* table, the original value is retrieved and the first block of the original message is decrypted.
4. Similarly, he decrypts all the blocks of the message, and hence the complete message is retrieved.

4 Mathematical Working and Proof

In this section, we detail the mathematical foundations of the encryption and decryption processes using the chosen elliptic curve. The elliptic curve used in this algorithm is defined by the equation:

$$y = x^3 + ax + b \pmod{p}.$$

Parameters of chosen elliptic curve of the form $y^2 = x^3 + ax + b \pmod{p}$ are given below:

1. $p = 115792089237316195423570985008687907853269984665640564039457584007908834671663.$
2. $a = -3.$
3. $b = 41058363725152142129326129780047268409114441015993725554835256314039467401291.$
4. $G = (0 \times 79BE667EF9DCBBAC55A06295CE870B07029BFCDB2DCE28D959F2815B16F81798,\ 0 \times 483ADA7726A3C4655DA4FBFC0E1108A8FD17B448A68554199C47D08FFB10D4B8).$

Original message

Original message to be encrypted is: **Himachal Pradesh.**

Mapping Point on Elliptic Curve

Using the proposed algorithm, the message is mapped to a point on the elliptic curve:

(106057243935852062527830419687377280111, 523414340917731399263180124611488612796013697933774554035153582611823768613 52)

Encryption Process

Alice encrypts the message, resulting in the following encrypted points:

((499409089443556344549777052136329318503937043213985145734321835721 30361621689, 101084056914798195902043242214822645509595294456635670317672712853166720897202), (521459240351806163681405602639673448608314967235801412135272677470703614892233059763263717110930621202192042684273655166253068806332402807607771050186312 6))

Decryption Process

Bob decrypts the message, recovering the original mapping point:

(106057243935852062527830419687377280111, 523414340917731399263180124611488612796013697933774554035153582611823768613 52)

The decrypted message is **Himachal Pradesh.**

Thus, we have demonstrated the detailed mathematical workings and proofs underlying the encryption and decryption processes using the chosen elliptic curve parameters.The correctness of the algorithm is verified by demonstrating that the decrypted message matches the original message. The use of elliptic curve cryptography combined with *DNA* sequencing and rhotrices ensures a robust encryption mechanism that is resistant to various cryptographic attacks.

5 Results and Analysis

5.1 Experimental Setup

The proposed Scheme was implemented using Intel Core i7 9th Generation CPU 2.00 GHz, 16 GB RAM, 1 TB SSD using Python 3 64-bit software.

5.2 Results and Analysis

In this section, we showcase the empirical results of implementing our proposed encryption scheme using Python. We assessed the performance and efficiency of the algorithm by measuring the time required for both encryption and decryption processes. These measurements offer a thorough analysis of the computational overhead associated with our cryptographic approach.

5.2.1 Encryption and Decryption Time

To assess the performance of the proposed scheme, we carried out several tests to measure the time required for both encryption and decryption. The recorded times offer insights into the computational efficiency of the algorithm under various conditions. Table 5.1 below presents the detailed results of our performance tests and results are illustrated in Figure 5.1.

***Table* 5.1:** *Encryption and decryption time of proposed scheme*

No. of characters in the message	Encryption Time (seconds)	Decryption Time (seconds)
500	0.002929	0.000007
1000	0.005326	0. 000007
2000	0.009414	0.000007
5000	0.022548	0.000009

The results indicate that the proposed scheme operates within acceptable time frames, making it suitable for practical applications. The consistently low encryption and decryption times demonstrate the efficiency of the algorithm.

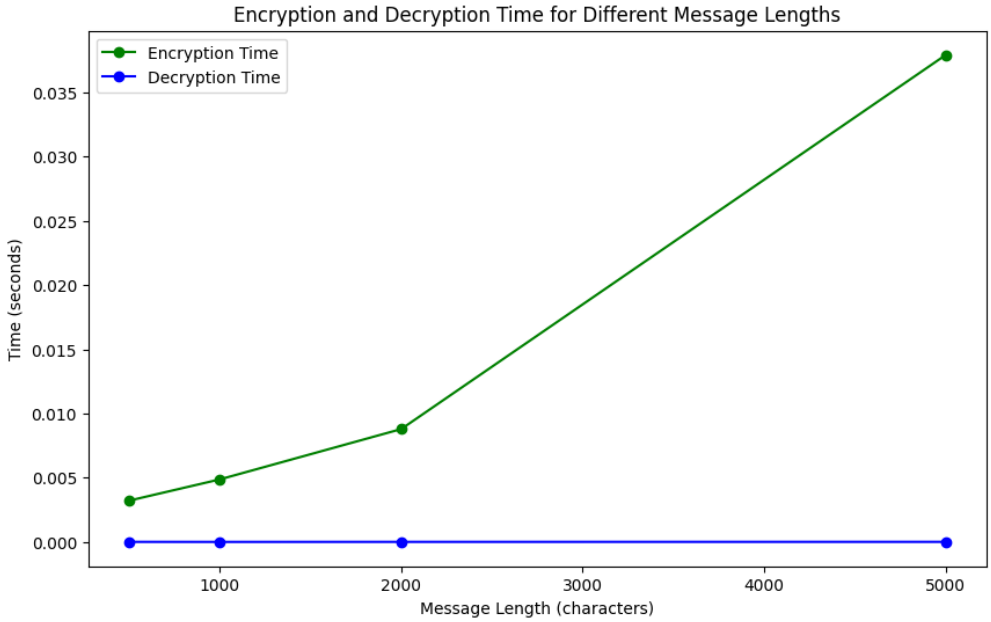

***Figure* 5.1:** *Encryption and Decryption Time for Different Message Length*

5.2.2 Timing Attack

A timing attack is a type of side-channel attack in which an adversary attempts to compromise ciphertext by analyzing the varying response times for different messages. *Figure* 5.2 illustrates the encryption time

for different data sets of the same size (100 characters) over multiple trials. Each line represents a different character set (A, B, C, and D), showing the variations in encryption time across four trials. The graph indicates that execution time varies for data sets of identical size but different content. This demonstrates the algorithm's efficiency and stability in handling data of varying content but the same size.

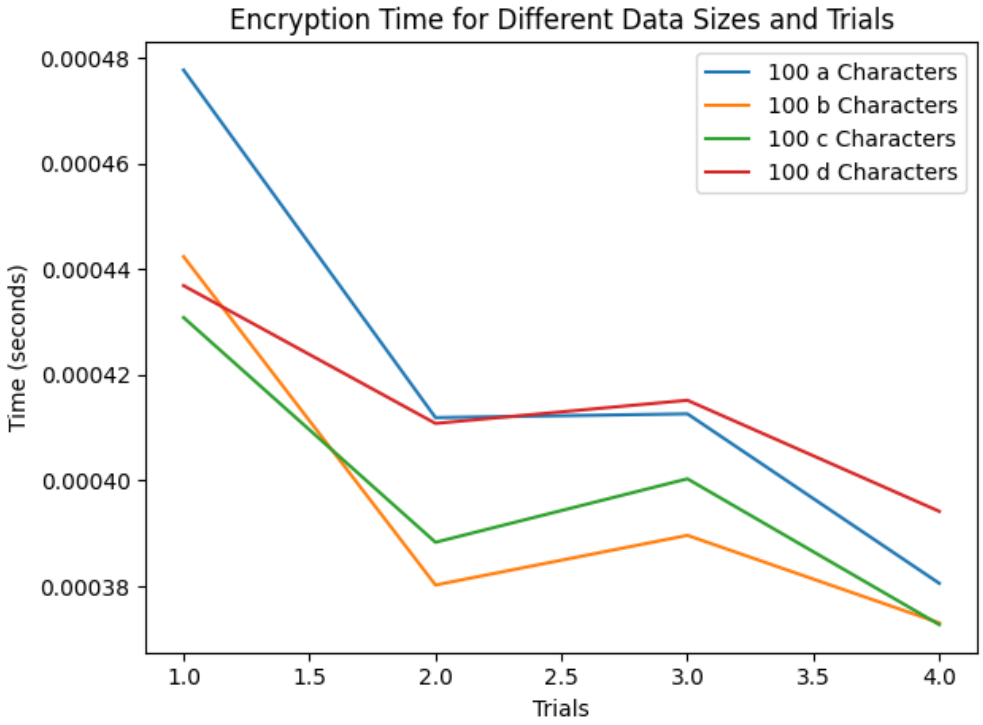

***Figure* 5.2:** *Encryption and Decryption Time for Different Message Length*

These results indicate that the proposed encryption scheme is robust and maintains efficient performance across various types of data. This makes it well-suited for practical applications where performance is a critical factor.

5.2.3 Time Complexity

The most significant operations in *ECC* are the scalar multiplications (steps 3, 4, 5, 6, 8, 18, and 22), each with a time complexity of $O(\log n)$ where n is the size of the scalar (private key or random integer). Splitting the message into blocks (step 11) has a linear time complexity $O(m)$, where m is the length of the message. Rhotrix multiplication involves elliptic curve point multiplications and additions. For $p \times p$ matrices, each matrix multiplication involves n^3 operations, and each operation is a point multiplication, this results in $O(p^3 \log n)$, where n is the scalar size used in the point multiplications. Therefore, the overall time complexity of the algorithm is dominated by the scalar multiplications and the message length, resulting in $O(m + \log n + p^3 \log n)$This efficient and practical balance between cryptographic security and performance makes the algorithm suitable for modern cryptographic applications.

5.3 Security Analysis

The security of the proposed encryption scheme is crucial for ensuring the confidentiality, integrity, and authenticity of the messages exchanged between Alice and Bob. This section offers a thorough analysis of the security features embedded in our scheme. We will evaluate the system's robustness and resilience against various potential attacks.

5.3.1 Key Space Analysis

Analyzing the key space is critical for evaluating the security of a cryptographic encryption scheme. The size of the key plays a crucial role in security, and while the algorithm used is well-known, opting for a larger key size is generally a prudent choice. However, increasing the key size also increases the computational load. The Elliptic Curve Discrete Logarithm Problem (*ECDLP*) used in Elliptic Curve Cryptography (*ECC*) is

computationally challenging, allowing users to employ smaller keys compared to traditional cryptographic methods without sacrificing security. Our implementation utilizes a 256-bit key length, which is robust enough to withstand basic attacks. For enhanced security, increasing the key length further would be advisable.

5.3.2 Known Plaintext Attack

If an attacker possesses knowledge of the plaintext, the encryption method, and some plaintext-ciphertext pairs, our encryption scheme remains resilient against known plaintext attacks. This resilience is due to the use of bisymmetric rhotrix, which can only be computed by the sender and receiver using their private keys. This ensures that even when encrypting the same message multiple times, distinct ciphertexts are generated each time. As a result, known-plaintext attacks are ineffective because the bisymmetric rhotrix prevents attackers from identifying patterns or correlations between the plaintext and ciphertext, thereby thwarting attempts to decipher the message.

5.3.3 Known Ciphertext Attack

If an attacker possesses the ciphertext and knowledge of the encryption scheme but lacks the receiver's private key, decrypting the message through brute force becomes highly impractical due to the substantial key size. The sheer computational effort required makes a brute force attack infeasible, potentially taking years to complete. This renders a ciphertext-only attack practically impossible. Moreover, even if the attacker were to decrypt the message eventually, the information obtained would likely be outdated and irrelevant by the time decryption is achieved. Therefore, a ciphertext-only attack is not feasible in this algorithm.

5.3.4 Chosen Plaintext Attack

Employing an algorithm that utilizes elliptic curve coordinates and private keys to compute all entries of the bisymmetric rhotrix introduces unpredictability into the mapping process. This complexity means that even if an attacker can select plaintexts for encryption, predicting how these plaintexts will map to specific points on the curve remains challenging.

5.3.5 Chosen Ciphertext Attack

The proposed encryption scheme is resilient against Chosen Ciphertext Attacks (CCA) through multiple security measures. The use of bisymmetric rhotrices in the decryption process enhances ciphertext security, minimizing the risk of plaintext exposure even if an attack is successful. By constructing the bisymmetric rhotrices using secure key agreement protocols such as $ECDH$, each matrix entry becomes unique, increasing the difficulty for attackers to compromise other keys. This encryption method also complicates attackers' ability to infer the relationship between ciphertext and plaintext changes. Furthermore, the scheme employs secure decryption procedures capable of detecting and rejecting tampered ciphertexts, further bolstering its defence against potential CCA.

5.3.6 Collision Attack

A collision attack occurs when two distinct inputs generate the same hash value or ciphertext after being processed by a cryptographic hash function or encryption algorithm. This encryption scheme predominantly utilizes Elliptic Curve Cryptography (ECC), where collision resistance primarily concerns the cryptographic hash functions employed within ECC or related components. Our proposed scheme operates deterministically, which inherently fortifies it against collision attacks.

5.3.7 Comparative Analysis

The proposed scheme demonstrates a significant improvement in encryption and decryption times compared to existing schemes. Our experimental results show that average time required for encrypting and decrypting a message using the proposed scheme is substantially less than that of Scheme A and Scheme B as shown in Table 5.2. This improvement in efficiency makes the proposed scheme more suitable for real- time applications where speed is crucial.

Table* 5.2: Encryption and Decryption time for different schemes.*

	Proposed Scheme		Scheme A [9]		Scheme B [39]	
No. Of Characters	Ecryption Time (sec)	Decryption Time (sec)	Ecryption Time(sec)	Decryption Time (sec)	Ecryption Time (sec)	Decryption Time (sec)
1000	0.005360	0.000007	0.022000	0.001700	0.017100	0.014200
2000	0.009414	0.000007	0.050000	0.003000	0.023600	0.019400
5000	0.022548	0.000009	0.127000	0.002800	0.027200	0.023200

Furthermore, the reduced computational overhead enables the proposed scheme to be deployed on resource-constrained devices, making it a more versatile and practical solution for secure communication.

6 Conclusion

This research introduces an innovative cryptographic scheme that integrates elliptic curves, *DNA* coding, and Bisymmetric rhotrix structures to facilitate secure and authenticated communication between parties. The scheme ensures mutual authentication and robust key derivation by having a dedicated private key using the other's public key. To enhance security and randomness, the scheme employs a permuted *ASCII* table to map *ASCII* values to elliptic curve points through *DNA* coding. This approach supports the secure transformation of data using bisymmetric rhotrices constructed from specific private key coordinates. The algorithm demonstrates notable efficiency, surpassing other cryptosystems like the Diffie-Hellman algorithm, thereby reducing the time needed for message encryption and decryption. Furthermore, its security is strengthened by the use of bisymmetric rhotrix, which complicates efforts by cryptanalysts to recover the original message from the ciphertext.

References

[1] A. O. Ajibade, The concept of rhotrix in mathematical enrichment, *International Journal of Mathematical Education in Science and Technology*, **34**(2) (2003), 175-179.

[2] J. Bao, Research on the security of elliptic curve cryptography, *In 7th International Conference on Social Sciences and Economic Development,* (2022), 984-988.

[3] N. L. Biggs, Coding natural languages, *Codes: An Introduction to Information Communication and Cryptography*, (2008), 1-16.

[4] H. C. Chen and J. C. Yen, A new cryptography system and its VLSI realization, *Journal of Systems Architecture*, **49**(7-9) (2003), 355-367.

[5] Y. Genç and E. Afacan, Implementation of new message encryption using elliptic curve cryptography over finite fields, *International Congress of advanced Technology and Engineering,* (2021), 1-6.

[6] S. Gupta, R. Narang, M. Harish, and N. Dhiman, MDS block hankel-like rhotrices using conjugate elements and self-dual bases of finite fields, *Bulletin of Pure & Applied Sciences-Mathematics and Statistics*, **41**(2) (2022), 184-198.

[7] S. Gupta, R. Narang, and M. Harish, On Construction of Involutory Maximum Distance Separable Rhotrices using Self Dual Bases over Galois Field, *Ganita,* **73**(2) (2023), 123-139.

[8] S. Gupta, R. Narang, and M. Harish, Construction of MDS Rhotrices from Cauchy Rhotrices and Block Cauchy-like Rhotrices over Finite Field, *International Journal of Creative Research Thoughts (IJCRT),* **11**(2023), 345-357.

[9] S. Gupta, R. Narang, and M. Harish, On Block Toeplitz-Like MDS Rhotrices over Finite Fields, *International Ideal E-Publication,* **I** (2023), 27-34.

[10] S. Gupta, Nitish, and M. Harish, Implementation of a Secured Mapping and Authenticated Double Fold Text Encryption Scheme Using Elliptic Curve Cryptography, *Journal of Emerging Technologies and Innovative Research,* **10**(6) (2023), 780-789.

[11] S. Gupta, Nitish, and M. Harish, A hybrid authenticated image encryption scheme using elliptic curves for enhanced security, *International Journal of Information Technology,* (2024). https://doi.org/10.1007/s41870-024-01737-w

[12] M. Hell and T. Johansson, Breaking the stream ciphers F-FCSR-H and F-FCSR-16 in real time, *Journal of Cryptology*, **24** (2011), 427-445.

[13] N. Koblitz, Elliptic curve cryptosystems, *Mathematics of computation*, **177**(48) (1987), 203-209.

[14] A. Kumar, S. S. Tyagi, M. Rana, N. Aggarwal, and P. Bhadana, A comparative study of public key cryptosystem based on ECC and RSA, *International Journal on Computer Science and Engineering*, **3**(5) (2011), 1904-1909.
[15] S. Kumar and D. Sharma, A chaotic based image encryption scheme using elliptic curve cryptography and genetic algorithm, *Artificial Intelligence Review*, **57**(4) (2024), 87.
[16] A. Kumari and V. Kapoor, Competing secure text encryption in intranet using elliptic curve cryptography, *Journal of Discrete Mathematical Sciences and Cryptography*, **23**(2) (2020), 631-641.
[17] M. R. Khan, K. Upreti, M. I. Alam, H. Khan, S. T. Siddiqui, M. Haque, and J. Parashar, Analysis of elliptic curve cryptography & RSA, *Journal of ICT Standardization*, **11**(4) (2023), 355-378.
[18] R. Lidl, and H. Niederreiter, Finite fields, *Cambridge University Press*, **20** 1997.
[19] V. S. Miller, Use of elliptic curves in cryptography, *In Conference on the theory and application of cryptographic techniques*, (1985), 417-426.
[20] A. Mohammed, *Theoretical development and applications of rhotrices,* LAP LAMBERT Academic Publishing, 2011.
[21] S. Namasudra, A secure cryptosystem using DNA cryptography and DNA steganography for the cloud-based IoT infrastructure, *Computers and Electrical Engineering*, **104** (2022), 108426.
[22] M. Nouri, Bisymmetric, persymmetric matrices and its applications in eigen-decomposition of adjacency and Laplacian matrices, *International Journal of Mathematical and Computational Sciences*, **6**(7) (2012), 766-769.
[23] P. Parida, C. Pradhan, X. Z. Gao, D. S. Roy, and R. K. Barik, Image encryption and authentication with elliptic curve cryptography and multidimensional chaotic maps, *IEEE Access*, **9** (2021), 76191-76204.
[24] B. Sani, The row–column multiplication of high dimensional rhotrices, *International Journal of Mathematical Education in Science and Technology*, **38**(5) (2007), 657-662.
[25] B. Sani, An alternative method for multiplication of rhotrices, *International Journal of Mathematical Education in Science and Technology*, **35**(5) (2004), 777-781.
[26] G. Singh and R. K. Yadav, DNA based cryptography techniques with applications and limitations, *International Journal of Engineering and Advanced Technology (IJEAT)*, **8**(6) (2019), 3997-4004.
[27] P. L. Sharma and R. K. Kanwar, A note on relationship between invertible rhotrices and associated invertible matrices, *Bulletin of Pure & Applied Sciences-Mathematics and Statistics*, **30**(2) (2011), 333-339.
[28] P. L. Sharma and R. K. Kanwar, Adjoint of a rhotrix and its basic properties, *International Journal of Mathematical Sciences*, **11**(3-4) (2012), 337-343.
[29] P. L. Sharma and R. K. Kanwar, On inner product space and bilinear forms over rhotrices, *Bulletin of Pure & Applied Sciences-Mathematics and Statistics*, **31**(1) (2012), 109-118.
[30] P. L. Sharma and R. K. Kanwar, The Cayley-Hamilton theorem for rhotrices, *International Journal Mathematics and Analysis*, **4**(1) (2012), 171-178.
[31] P. L. Sharma and R. K. Kanwar, On involutory and Pascal rhotrices, *International Journal of Matematical Sciences & Engineering Applications(IJMSEA)*, **7**(4) (2013), 133-146.
[32] P. L. Sharma and R. K. Kanwar, On construction of MDS rhotrices from companion rhotrices over finite field, *International Journal of Mathematical Sciences*, **12**(3-4) (2013), 271-286.
[33] P. L. Sharma, S. Kumar, and M. Rehan, On Hadamard rhotrix over a finite field, *Bulletin of Pure & Applied Sciences-Mathematics and Statistics*, **32**(2) (2013), 181-190.
[34] P. L. Sharma, S. Kumar, and M. Rehan, On Vandermonde and MDS rhotrices over GF (2q), *International Journal of Mathematics and Analysis*, **5**(2) (2013), 143-160.
[35] P. L. Sharma and S. Sharma, Sequences of irreducible polynomials over GF (2) with three prescribed coefficients, *Recent Trends in Algebra and Mechanics*, (2014), 21-32.
[36] P. L. Sharma, S. Sharma, and N. Dhiman, Construction of infinite sequences of irreducible polynomials using Kloosterman Sum, *Bulletin of Pure & Applied Sciences-Mathematics and Statistics*, **33**(2) (2014), 161-168.
[37] P. L. Sharma, S. Sharma, and M. Rehan, On construction of irreducible polynomials over F_3, *Journal of Discrete Mathematical Sciences and Cryptography*, **18**(4) (2015), 335-347.
[38] P. L. Sharma, S. Sharma, and M. Rehan, Construction of infinite sequences of irreducible polynomials over F_2, *International Journal of Mathematical Sciences and Engneering Applications,* **9**(3) (2015), 19-35.

[39] P. L. Sharma, S. Gupta, and N. Dhiman, Construction of maximum distance separable rhotrices using Cauchy rhotrices over finite fields, *International Journal of Computer Application*, **168**(9) (2017), 8-17.
[40] P. L. Sharma, S. Gupta, H. Monga, A. Nayyar, K. Gupta, and A. K. Sharma, TEXCEL: text encryption with elliptic curve cryptography for enhanced security, *Multimedia Tools and Applications*, (2024), 1-29.
[41] P. L. Sharma, S. Gupta, A. Nayyar, M. Harish, K. Gupta, and A. K. Sharma, ECC based novel color image encryption methodology using primitive polynomial, *Multimedia Tools and Applications*, **83**(31) (2024), 1-40.
[42] D. G. Yakubu, L. B. Mathias, B. G. Lucy, and D. Lohcwat, Extension of Affine Hill cipher using rhotrices in the poly-alphabetic cipher systems, *Sci Forum Journal of Pure and Applied Science,* **45**(1) (2018), 273–284.
[43] D. G. Yakubu, L. B. Mathias, B. G. Lucy, and D. Lohcwat, A secured cryptographic technique using rhotrices in polygraphic cipher systems, *Sci Forum Journal of Pure and Applied Science,* **22**(1) (2022), 35–42.
[44] Q. Zhang, L. Guo, and X. Wei, Image encryption using DNA addition combining with chaotic maps, *Mathematical and Computer Modelling*, **52**(11-12) (2010), 2028-2035.

ISSN 0304-9892 (Print) ISSN 2455-7463 (Online)
www.vijnanaparishadofindia.org/jnanabha
***Jñānābha* Vol. 55 (I) Special Issue 2025, 16-22**
Proceedings: 5th International Conference and Golden Jubilee Celebrations of VPI (IC-RA-MSA-ET 2022) JNU, New Delhi, India

ANALYSIS OF POLLUTION CAUSING ATTRIBUTES DURING TRAFFIC ON ROADS

Shanky Garg[1] and Rashmi Bhardwaj[2]
[1]Research Scholar, USBAS, Guru Gobind Singh Indraprastha University, Dwarka, Delhi, India-110078
[2]Professor of Mathematics, University School of Basic and Applied Sciences (USBAS), Guru Gobind Singh Indraprastha University (GGSIPU), Dwarka, Delhi, India-110078
Email: shankygarg.du.or.20@gmail.com, ORCHID ID: 0000-0001-5280-7437; rashmib@ipu.ac.in; ORCHID ID: 0000-0002-0502-762X

(Received: October 09*,* 2023*, In format: October* 27*,* 2023*; Revised: March* 03*,* 2024*; Accepted March* 10*,* 2025*)*

DOI: https://doi.org/10.58250/jnanabha_SI.2025.55102

Abstract

Due to urbanization and the increase in the population, means of transportation have increased drastically because it makes traveling easy for people and also because of ease of availability. Either 2 wheeler or 3 or 4 wheeler or self-owned car or rented taxi, all are in huge demand based upon the preference of the people. But besides all these advantages, these vehicles come with a big disadvantage which will surely not only impact people's time but only have a great effect on their health and Pollution is one among them. The tremendous use of these services will definitely increase the congestion on the road, especially at the intersection points which are busy all the time and this will be dangerous as it will not only impact the pocket of the people in terms of fuel consumption but also increases the pollutions in terms of air and noise. This paper mainly deals with the critical analysis of the attributes that cause air pollution and the contribution of each type of vehicle during traffic by the number of vehicles using mutated critic and AHP method so that the traffic department can take necessary steps to reduce the traffic at these intersection points so that the consumption of fuel as well the pollutant level that increases these problems decreases.

2020 Mathematical Sciences Classification: 90B50, 90C27, 90C29.
Keywords and Phrases: Traffic, Optimization, Pollution, Air, AHP, Mutated Critic Method

1 Introduction

Continuous increase in the economy along with the enhancement in the pattern of livelihood of the people poses a threat to the environment as well as the ecology. It even creates a recession in the ecological balance. Cities are more inclined towards the development of humans and in the ecological and civilization advancement [1,13]. Over the past many years, migration of people to the cities has increased from 5% to more than 50%, and by 2050, it is expected to increase by 66% mainly in developing countries/cities. In today's era due to the increase in urbanization people need more facilities to do their daily activities and Travelling and Motorization are some of the most frequent activities that are included in their day-to-day activities [19]. Ease in the availability of transportation facilities makes it even easier for people mainly in urban areas to travel for their work/ for whatever reason they want to travel [14,15]. There is a huge linkage between these transportation facilities provided by different vehicles, overcrowded cities, and the effect on the environment as well as on the people [11]. The increase in the population somewhere gives the advantage in terms of human resources but also increases the pressure on the resources that are vulnerable to extinction like water, air, and land and somehow affects the transportation facilities too [1,12]. Due to the increase in these motorization facilities, there is a tremendous increase in the traffic on the roads which in turn increases the accidents on the roads as well as the pollution released from these vehicles also affects our health [3,7,8]. Not only air pollution but also the noise pollution caused by these vehicles mainly at the intersection points as most of the time there is a fair chance of being stuck at traffic at these points and then simultaneously increases these pollutions as well increases the mortality rate of the people at these sites [20,21]. From the recent studies, we can conclude that people living near major roadways have a high chance of being affected by the diseases caused due to this pollution [22]. Among all the pollution-causing attributes, particulate mainly PM 2.5 is the most dangerous one due to which 480000 people die in Europe. According to the

reports of the Institute for Health Effects, 95% of people all over the world breathe polluted air and die due to several diseases caused by this [5,17]. Not only air pollution but it also enhances noise pollution [4,18]. According to the report of *WHO*, Noise pollution is the second stressor after air which is caused by the traffic on roads. Besides the harmful diseases caused by air pollution, Noise pollution also affects the body in a very ways which include early death, constant stress, tension, depression, hearing problems, etc. So, there is an urgent need to overcome this issue and a need to make a balance between the environment and the ecology as both are important for survival and growth. Presently there are very few studies that consider the effect of congestion of vehicles on the environment and on the health of the people [9]. There is not a single method through which we can estimate the impact of this. It depends on the choice of the users which method they want to choose and more on the accuracy of that method. There is an urgent need to identify these factors not only theoretically but also quantitatively. There are many areas through which we can deal with this problem but in this study, we are using Multi Criteria Decision Making Techniques more specifically *AHP* (Analytical Hierarchical Process) which is basically a technique used to solve complex decision-making processes which is proposed by Satty. Here we are taking different criteria as well as the alternatives based on the objectives [17,18]. It is basically based on the subjective weights where we need a different decision maker for the data [10]. Mutated Critic Method is also a good method of *MCDM* which helps in analyzing the attributes clearly and in making the decisions. This paper mainly deals with the analysis of the attributes which cause pollution mainly air during the traffic or congestion on roads and the number or the type of vehicles which are involved in causing this. In this study, we are using both the methods which are discussed above i.e. Analytical Hierarchy Process (*AHP*) as well as the mutated critic analysis method so that the government can take immediate and proper steps based on this.

2 Methodology Used

2.1 AHP (Analytical Hierarchical Process)

Step 1. We first define the objectives hierarchy as the decision criteria. The first level consists of the objective of the overall problem then the criteria /subcriteria in the subsequent level and at the last the alternatives if we have any.

Step 2. Decision makers analyze the objectives, criteria as well and subcriteria and assign importance according to that.

Step 3. Create a pairwise matrix based on the Satty's scale rule.

Step 4. After creating a decision matrix, we calculate the local priorities with the normalized matrix and then the global weights are calculated.

Step 5. Then the consistency of the matrix is checked and result is obtained. From this we can easily rank the criteria as well as the alternatives.

2.2 Mutated CRITIC Method

Step 1. Collect the data of the given objective problem.

Step 2. Represent the data in the matrix format.

Step 3. Normalized the data using the logarithmic method as compared to the best-worst method that we used in the original critic method.

For normalization, we are using the following formulas:

$$\text{Useful Criteria } = \frac{\ln(Z_{ij})}{\ln(\prod_{i=1}^{m} Z_{ij})}. \tag{2.1}$$

where Z_{ij} represents the entry of the criteria/ subcriteria in the matrix formed.

$$\text{Lost Criteria} = (1 - \frac{\ln(Z_{ij})}{\ln\left(\prod_{i=1}^{b} Z_{ij}\right)})/(b-1). \tag{2.2}$$

where b represents the number of stations.

Step 4. Calculate the standard deviation to analyze the variability among the criteria/subcriteria.

$$\textbf{S.D.} = \sqrt{\frac{\left(Z'_{\beth j} - \overline{Z}_j\right)^2}{b-1}}. \tag{2.3}$$

where Z'_{ij} represents the normalized value of each entry in the matrix.

Z'_j bar represents the mean value of each entry in the matrix.

b represents the number of stations.

Step 5. Modified Distance correlation is used here to calculate the correlation matrix.

$$Dcor\left(_j\ ,j^{'}\right) = \frac{Dcov\left(_j\ ,j^{'}\right)}{sqrt\left(dvar(\ \ _j\ )\ dvar(j^{'})\right)}. \tag{2.4}$$

Where dj, dj$^{'}$ represents the criteria.

Step 6. Calculate the information content to analyze the information that each criterion has. It is given by: -

$$\mathrm{I.F_j} = \mathrm{S.D_j}(\sum_{j=1}^{b}(1 - Dcor(_j\ ,j^{'})). \tag{2.5}$$

Step 7. The weight of each criterion is calculated by using the information content: -

$$W_j = I.F_j / \sum_{j=1}^{m} I.F_j. \tag{2.6}$$

3 Case Study and Results

The case study area which is taken for study is Sibiu, Romania, and data is taken from the research [21]. Here in this paper, we are taking 6 pollutants emitted from the intersection of roads which are CarbonMonoxide, Hydrocarbons, NO_x, Noise, Ozone, and PM10, and 5 intersections are taken which are described in Table 3.1 below:

***Table* 3.1:** *Pollutants data*

Intersections/Pollutants	CO	HC	Nox	Noise	Ozone	PM10
Intersection 1	187	7	16	91.36	39.14	67.87
Intersection 2	170	5	23	80.56	38.22	40.33
Intersection 3	165	6	19	85.3	37.97	41.27
Intersection 4	187	10	37	78.1	40.08	43.48
Intersection 5	245	19	49	76.3	40.33	25.06
	954	**47**	**144**	**411.62**	**195.74**	**218.01**

Here Intersection i represents the Aral Miles, Semaforului Paltinului, Semaforului-U.Militara, IBIS, Turismului-Morilor resp. Here $\boldsymbol{i}$ *= 1 to 5.*

In this study, we first analyze the pollutants using the mutated critic method and then rank each intersection using the AHP method. By applying the modified critic method, we get the following results as shown in Table 3.2 below:

***Table* 3.2:** *Result Matrix with weights*

Pollutants	CO	HC	Nox	Noise	Ozone	PM10
CO	1	0.9487711	0.8009438	0.6408855	0.8481255	0.8377564
HC	0.9487711	1	0.9269491	0.7643755	0.9195976	0.8115062
Nox	0.8009438	0.9269491	1	0.9304878	0.8839028	0.8022815
Noise	0.6408855	0.7643755	0.9304878	1	0.7335265	0.8451089
Ozone	0.8481255	0.9195976	0.8839028	0.7335265	1	0.6475484
PM10	0.8377564	0.8115062	0.8022815	0.8451089	0.6475484	1
S.D.	0.0016499	0.0040613	0.0142801	0.074726	0.0454397	0.0099764
Information Content(I.F)	0.0031735	0.0066151	0.0236398	0.1558498	0.0893935	0.0205095
Weight	0.0106074	0.0221105	0.0790151	0.5209212	0.2987938	0.0685521
Weight(%)	1.0607386	2.2110542	7.901506	52.092116	29.879376	6.8552097

Here we can see the Information provided by each pollutant and the weight/ contribution of each pollution in analysing pollution.

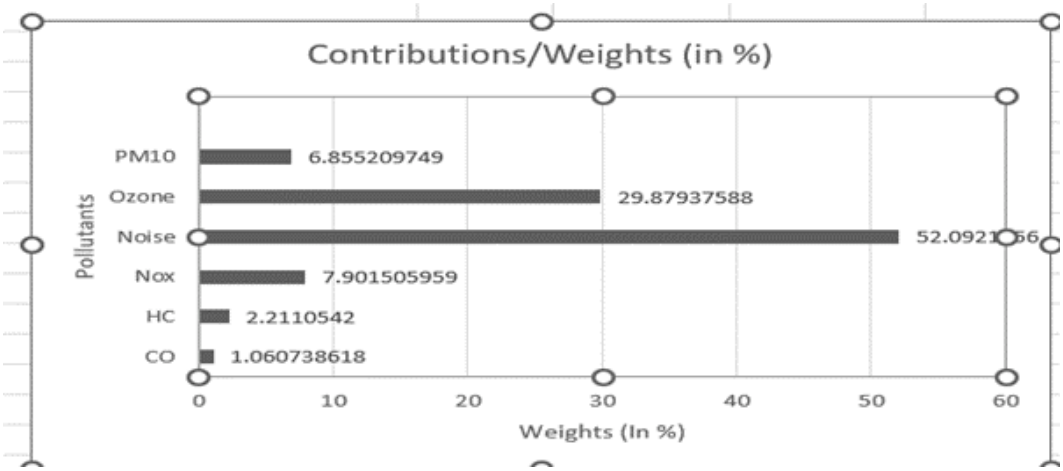

***Figure* 3.1:** *Weights of Different Criteria*

From Fig 3.1 and Fig 3.2, we can see that Noise is a major contributor in analyzing the pollution caused by traffic followed by the ozone concentration.

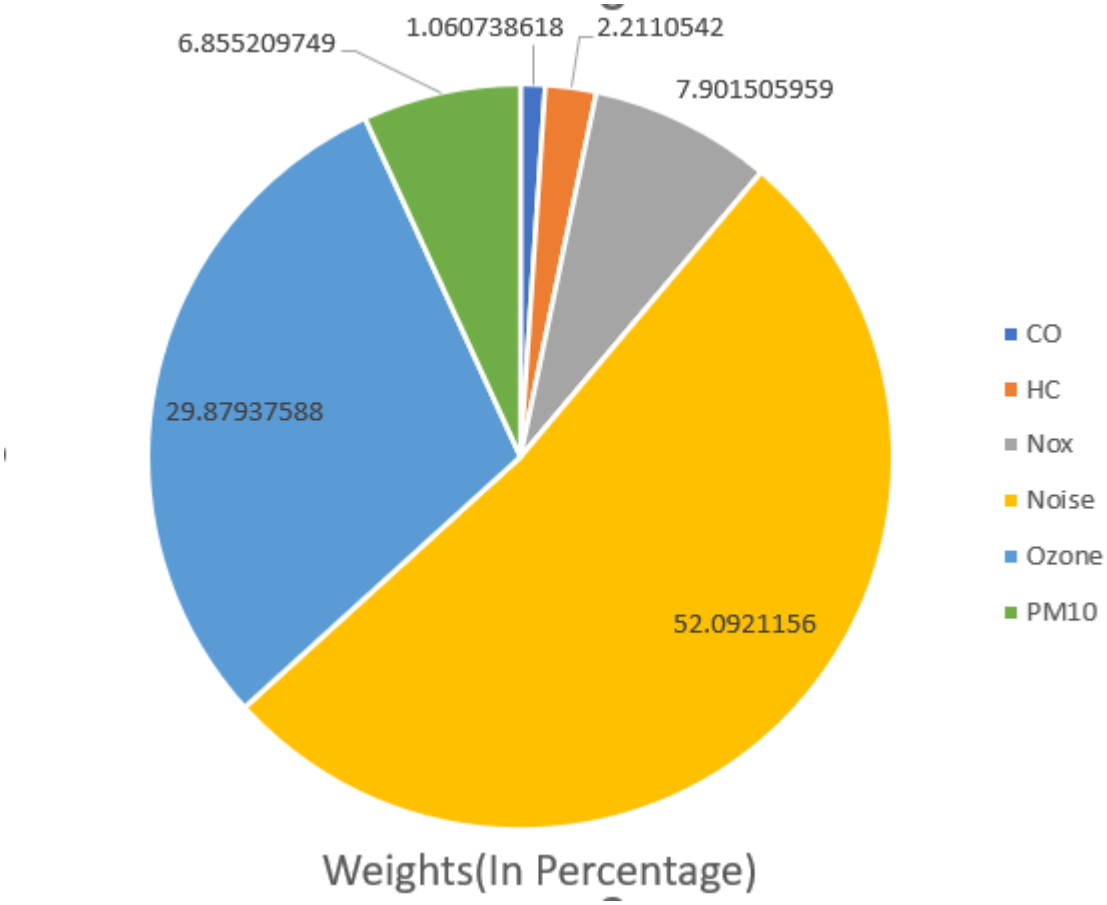

***Figure* 3.2:** *Contribution of pollutants*

After analyzing the weight of each pollutant, now we are in the position to rank the intersections roads based on the data given below:

***Table* 3.3:** *Intersection Data*

Intersection 1	Intersection 2	Intersection 3	Intersection 4	Intersection 5
1	3	2	4	5
0.333333	1	2	3	4
0.5	0.5	1	4	5
0.25	0.333333	0.25	1	2
0.2	0.25	0.2	0.5	1

After applying the AHP method, we get the following result as follows:

***Table* 3.4:** *Result Matrix (with AHP)*

	Weights
Intersection 1	41.00%
Intersection 2	24.10%
Intersection 3	21.50%
Intersection 4	8.10%
Intersection 5	5.30%
Consistency ratio	5.50%
No of comparisons	10

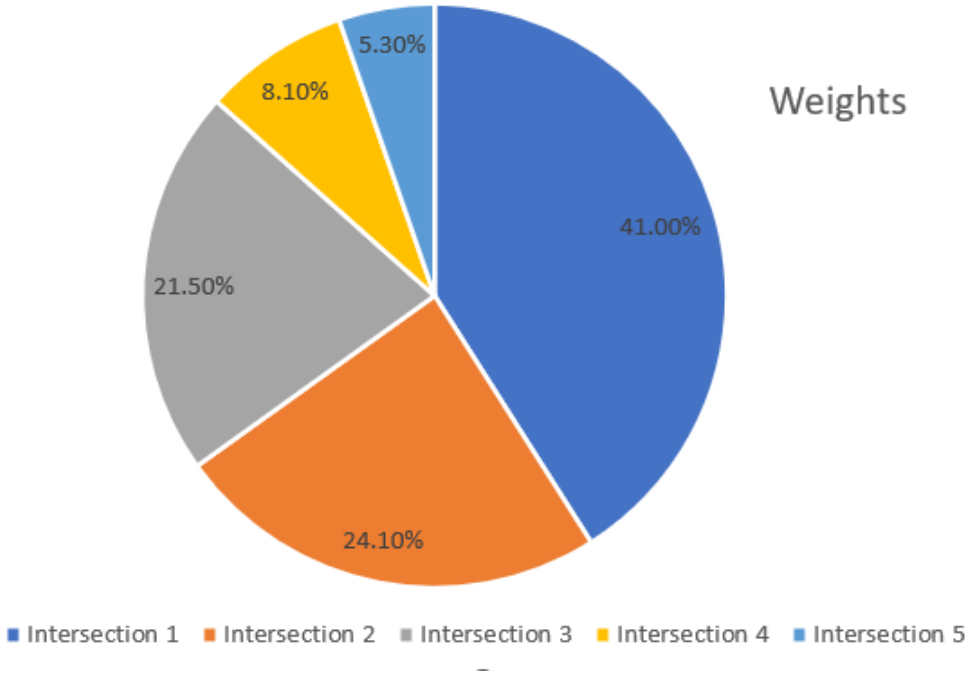

***Figure* 3.3:** *Contribution of Intersections*

4 Conclusion

As the quality of the environment continuously degrades over time due to these pollution-causing attributes/pollutants there is always a need to devise a proper methodology to reduce these pollutants. MCDM methods make a clear understanding of the results. Combining both methods, we get the overall result which can be analysed easily. From the above-calculated results, we can conclude that Intersection 1 contributes more to the pollution which means there is more congestion on these roads which does not affect the pocket of the people during the wastage of fuel, not only the time of the people because of the long waiting hours but also affect the health. Within the intersection 1 Noise attribute plays an important role in this with the maximum contribution in this. So, to reduce these negative effects we need to take steps like lowering the content of lead in fuel should be used, and Eco-friendly vehicles should be used as much as possible.

Acknowledgement. We are thankful to Guru Gobind Singh Indraprastha University for understanding this research.

References

[1] Air Quality Framework Directive 96/62/EC of the European Parliament and the Council (accessed on 9 July 2018). Available online: http://ec.europa.eu/environment/air/quality/index.htm

[2] L.R. Brown, The Economy and the Earth: The Option: Restructure or Decline. In Eco-Economy: Building an Economy for the Earth; Earth Policy Institute: Washington, DC, USA, 2001; Chapter 1.

[3] P. Beria, I. Maltese and I. Mariotti, Comparing Cost Benefit and Multi-Criteria Analysis: The Evaluation of Neighbourhoods Sustainable Mobility, Conference_Paper_files/BERIA_MALTESE_MARIOTTI.pdf (accessed on 19 August 2018). Available online: `http://ww2.unime.it/sefisast/SEFISAST/`

[4] J. Buchanan, P. Sheppard and D. Vanderpoorten, Ranking projects using the ELECTRE method. *Proceedings of the 33rd Annual Conference in Operational Research Society of New Zeeland, Auckland, New Zealand*, (August 30–September 2, 1998), 42–51.

[5] F.E. Boran, S. Gen, M. Kurt and D. Akay, A multi-criteria intuitionistic fuzzy group decision making for supplier selection with TOPSIS method. *Expert Syst. Appl.,* **36** (2009),11363–11368.

[6] S. Borza, M. Inta, R. Serbu and B. Marza, Multi-Criteria Analysis of Pollution Caused by Auto Traffic in a Geographical Area Limited to Applicability for an Eco-Economy Environment, *Sustainability,* **10** (2018),4240.

[7] N. Caterino, I. Iervolino, G. Manfredi and E. Cosenza, Applicability and effectiveness of different decision making methods for seismic upgrading building structures, *Proceedings of the XIII Convegno Nazionale L'Ingegneria Sismica, Bologna, Italy*, (June 28–July 2, 2009).

[8] Y.H. Chang and C.H. Yeh, Evaluating airline competitiveness using multiattribute decision making, *Omega*, **29** (2001), 405–415.

[9] K. Govindan and M.B. Jepsen, ELECTRE: A comprehensive literature review on methodologies and applications, *Eur. J. Oper. Res.*, **250** (2016), 1–29.

[10] C.L. Hwang and K. Yoon, *Multiple Attribute Decision Making: Methods and Applications*, Springer: New York, NY, USA, 1981.

[11] S.K. Misra and A. Ray, Comparative study on different multi-criteria decision making tools in software project selection scenario, *Int. J. Adv. Res. Comput. Sci.*, **3** (2012), 172-178.

[12] X. Ouyang and F. Guo, Intuitionistic fuzzy analytical hierarchical processes for selecting the paradigms of mangroves in municipal wastewater treatment. *Chemosphere*, **197** (2018), 634–642.

[13] Playtech. Available online: https://playtech.ro/2018/pollution-mortality-deaths-2015 (accessed on 18 June 2018).

[14] R. Ramanathan, A note on the use of the analytic hierarchy process for environmental impact assessment, *J. Environ. Manag.*, **63** (2001), 27–35.

[15] J. Ren and H. Liang, Multi-criteria group decision-making based sustainability measurement of wastewater treatment processes, *Environ. Impact Assess. Rev.*, **65** (2017), 91–99.

[16] D. Sinem, B. Ferhat and C.S. Sait, MCDM analysis of wind energy in Turkey: Decision making based on environmental impact, *Environ. Sci. Pollut. Res.*, **25** (2018), 19753–19766.

[17] T.L. Saaty, *The Analytic Network Process*, RWS Publications: Pittsburgh, PA, USA, 2001.

[18] T.L. Saaty, What is the Analytic Hierarchy Process? In Mathematical Models for Decision Support; NATO ASI Series; *Springer: Berlin/Heidelberg, Germany*, **48 (**1988), 109–121.
[19] K. Tolga and C. Kahraman, An integrated fuzzy AHP–ELECTRE methodology for environmental impact assessment, *Expert Syst. Appl.*, **38** (2011), 8553–8562.
[20] J.J. Wang, Y.-Y. Jing, C.-F. Zhang and J.-H. Zhao, Review on multi-criteria decision analysis aid in sustainable energy decision-making, *Renew. Sustain. Energy Rev.* **13** (2009), 2263–2278.
[21] M. Wang, S. Liu, S. Wang and K.K. Lai, A weighted product method for bidding strategies in multi-attribute auctions, *J. Syst. Sci. Complex.*, **23** (2010), 194–208.
[22] K. Zhang and S. Batterman, Air pollution and health risks due to vehicle traffic, *The Science of the Total Environment*, **307** (2013), 307-316.

ISSN 0304-9892 (Print) ISSN 2455-7463 (Online)
www.vijnanaparishadofindia.org/jnanabha
***Jñānābha* Vol. 55 (I) Special Issue 2025, 23-28**
Proceedings: 5th International Conference and Golden Jubilee Celebrations of VPI (IC-RA-MSA-ET 2022) JNU, New Delhi, India

ON EFFICIENT DISCRETE LOGARITHM COMPUTATION ON ELLIPTIC CURVES

[1]Shalini Gupta, [2]Kritika Gupta, [3]Gajendra Pratap Singh and [4]Kamalendra Kumar
[1, 2,]Department of Mathematics & Statistics, Himachal Pradesh University, Shimla, India-171005
[3]School of Computational and Integrative Sciences, Jawaharlal Nehru University, New Delhi, India-110067
[4]Department of Basic Science, Shri Ram Murti Smarak, College of Engineering and Technology, Bareilly, India-243202
Email: shalini.garga1970@gmail.com, kritika993@gmail.com, gajendra@gmail.jnu.ac.in, kamlendra.14kumar@gmail.com

(Received: October 10, 2023; In format: December 05, 2024; Revised: May 09, 2025; Accepted: July 14, 2025)

DOI: https://doi.org/10.58250/jnanabha_SI.2025.55103

Abstract

The proposed algorithm for computing discrete logarithms on elliptic curves involves choosing a prime with a large prime factor, an elliptic curve over the field of that prime and a random point of a certain order on the curve. The algorithm then chooses a set of primes optimized to minimize the size of a linear system and computes relations between the primes and random points on the curve using the Pollard rho algorithm. It then uses the Furer-Gathen algorithm to compute a summation polynomial for these relations and solves the linear system for the coefficients of the unknown logarithms of the prime factors of the curve's order using the conjugate gradient method and combines these logarithms to compute the discrete logarithm of any point on the curve.

2020 Mathematical Sciences Classification: 12E20, 94A60
Keywords and Phrases: Elliptic Curve; Discrete Logarithm Problem (DLP); Prime Field; Point Counting; Summation Polynoimal.

1 Introduction

Elliptic Curve Cryptography *(ECC)* is a popular public-key cryptography that offers high security and efficiency. The security of *ECC* is based on the difficulty of solving *DLP* on an elliptic curve. Given a point P on an elliptic curve and another point Q, the *DLP* involves finding an integer k such that $kP = Q$. The most common method for solving the *DLP* is the generic algorithm which has a complexity of $O(\sqrt{n})$ where n is the order of the elliptic curve. However, for certain types of elliptic curves this algorithm can be made much more efficient. One such algorithm is the Elliptic Curve Logarithm *(ECL)* algorithm proposed by Koblitz and Miller [11]. The *ECL* algorithm is a variant of the generic algorithm that uses the properties of the curve to reduce the number of points that need to be computed. The *ECL* algorithm was a major breakthrough in the field of elliptic curve cryptography and it led to the development of several other algorithms based on the same idea.

One of these algorithms is the *SEA* algorithm proposed by Schoof [15] and later improved by Elkies and Atkin. The *SEA* algorithm is a method for computing the cardinality of an elliptic curve over a prime field, which is a critical parameter in various cryptographic schemes. The complexity of *SEA* algorithm is much faster than the generic algorithm for large n. Another algorithm that builds upon the ideas of the *ECL* algorithm is the *MOV* algorithm proposed by Menezes *et al.* [13]. The *MOV* algorithm is a method for reducing the *DLP* on an elliptic curve to the *DLP* in a finite field. This allows the use of more efficient algorithms for solving the *DLP* such as the number field sieve algorithm. Semaev in 2004, invented summation polynomials and proposed to use them in construction of index calculus algorithm for elliptic curves, see [16]. He reduced the problem of point decomposition to the problem of finding solutions to summation polynomials.

In recent years, several new algorithms have been proposed for computing discrete logarithms on elliptic curves. Gaudry [6] in 2009, was the first to use Semaevs proposal to solve *ECDLP* and he created index calculus algorithm for elliptic curves defined over the field $\mathbb{F}(q^n)$ where q is a prime or prime power and $n > 1$. He proved that *ECDLP* can be solved in heuristic time $O(q^{(2-2/n)})$. But his results were not applicable to

prime field elliptic curves. Subsequently, Diem [3] in 2011 used the Semaevs approach and solved *ECDLP* in time $e^{(O(max(logq,n^2)))}$.
Further, Huang *et al.* [8], Faugere *et al.* [4], Joux and Vitse [9], Galbraith and Gebregiyorgis [5] used the concept of symmetries to get relevant results in case of index calculus algorithm for elliptic curves. To get better running time Semaev [17], Karabina [10] and Huang *et al.* [8] reduced the degree of system of polynomial equations involved in the point decomposition problem at the cost of large number of variables. Semaev [14] in his original proposal took the case of prime field elliptic curves. The difficulty in prime field case is that one cannot use the Weil descent in point decomposition problem. In 2016, Petit *et al.* [16] discussed the case of index calculus algorithm for prime field elliptic curves and suggested to use Factor base as $\{(x, y) \in E(F_p)|L(x) = 0\}$, where p is prime and L is a rational map which can be decomposed into maps of lower degree thus making the algorithm more efficient. Further, in 2018, Amadori *et al.* [1] worked over index calculus algorithm for prime field elliptic curves. Ansari ([2] propose oblique elimination as a way to solve the Elliptic Curve Discrete Logarithm Problem *(ECDLP)*.
In this paper, we propose a new algorithm for computing the discrete logarithm of a point on an elliptic curve over a prime field. Our algorithm is based on the ideas of the *ECL* algorithm and the *SEA* algorithm but it also incorporates several new optimizations to improve efficiency. In particular, our algorithm optimizes the choice of primes used in the algorithm and it uses faster algorithms for point counting, polynomial evaluation and linear system solving.

2 Preliminaries

In this section, we discuss some basic preliminaries which are necessary to understand the proposed work.

2.1 Elliptic Curves

An elliptic curve is a type of algebraic curve defined by an equation of the form $y^2 = x^3 + ax + b$, where a and b are constants in a finite field $\mathbb{F}_p$. The set of solutions (x, y) to this equation, together with a point at infinity, forms an abelian group under a geometric operation called point addition. The group has a finite order, denoted by n, which is the number of points on the curve over $\mathbb{F}_p$. The order n is always even and is related to the prime p and the coefficients a and b through the Hasse's theorem, which bounds n by $p + 1 - 2\sqrt{p}$.
Elliptic curves have several desirable properties for cryptographic applications, including efficient point multiplication, resistance to certain attacks, and the existence of efficient algorithms for computing discrete logarithms.

2.2 Discrete Logarithm Problem on Elliptic Curves

Given an elliptic curve E defined over a finite field $\mathbb{F}_p$ of order n and a point P on E, the Discrete Logarithm Problem *(DLP)* on E asks to find an integer k such that $kP = Q$, where Q is a known point on E. The security of many cryptographic protocols based on elliptic curves, such as elliptic curve cryptography *(ECC)*, relies on the intractability of the *DLP*.

2.3 Pohlig-Hellman Algorithm

The Pohlig-Hellman algorithm is a general algorithm that works for any abelian group of order n. It involves factoring the order n into its prime factors and then solving the *DLP* for each prime factor using the Chinese Remainder Theorem. The time complexity of this algorithm is $O(\sqrt{p}\log(p)\log(n))$, where p is the largest prime factor of n.

2.4 Index Calculus Algorithm

The Index Calculus algorithm is a more specialized algorithm that works for elliptic curves with a small number of prime factors in the order n. It involves computing a set of smooth points on the curve and then using them to construct a system of linear equations in the unknown discrete logarithms. The time complexity of this algorithm depends on the size of the smoothness bound and can be as low as $O(\exp(\sqrt{\log(n)\log(\log(n))}))$.

2.5 SEA Algorithm

SEA algorithm is a specialized algorithm that works for elliptic curves with a prime order. It involves computing the cardinality of the curve using the Schoof's algorithm and then using it to reduce the *DLP* on the curve to a *DLP* on a finite field. The time complexity of this algorithm is $O(\sqrt{p}\log(p)^2\log(n))$.

2.6 Furer-Gathen Algorithm

The Furer-Gathen algorithm is a fast algorithm for polynomial multiplication. The algorithm is used in the algorithm for computing the discrete logarithm of a point on an elliptic curve to compute the summation

polynomial.

2.7 Conjugate Gradient Method

The conjugate gradient method is an iterative method for solving systems of linear equations. The method is used in the proposed algorithm for computing the discrete logarithm of a point on an elliptic curve to solve the linear system of equations obtained from the summation polynomial.

3 Proposed Algorithm for Computing Discrete Logarithm

The proposed algorithm aims to efficiently compute discrete logarithms on elliptic curves defined over a prime field $\mathbb{F}_p$. In the first step, a prime p and an elliptic curve E of order n are selected with the additional requirement that $p+1$ has a large prime factor. Subsequently, a random point P on E is chosen and its order q is computed. If q is not a factor of n, a new point is chosen until a suitable one is found. The algorithm then employs the Schoof's Elliptic Curve Algorithm *(SEA)* to determine the cardinality of E. To optimize efficiency, a set of small primes $p_1, p_2, ..., p_k$ is selected and discrete logarithms of random points $Q_1, Q_2, ..., Q_k$ with respect to P are computed using the baby-step giant-step algorithm. The Pollard rho algorithm is subsequently applied to establish relations between the chosen primes and the computed discrete logarithms. The relations are combined into a summation polynomial $S(x)$ using the Furer-Gathen algorithm. The linear system $S(x) = 0$ is then solved using the conjugate gradient method yielding coefficients representing the unknown logarithms of the prime factors of n. Finally, the discrete logarithm of any point on E is computed by combining the determined logarithms of the prime factors of n. This algorithm offers a comprehensive and efficient approach for solving the discrete logarithm problem on elliptic curves combining various well-established algorithms to enhance computational performance.

Input: An elliptic curve E defined over a prime field $\mathbb{F}_p$ of order n
Output: The discrete logarithm of a point on E
Step 1 Choose a prime p such that $p + 1$ has a large prime factor, and an elliptic curve E over the field $\mathbb{F}_p$ of order n;
Step 2 Choose a random point P on E and compute its order q. If q is not a factor of n, choose another point and repeat until a point of order q is found;
Step 3 Compute the SEA of E to obtain its cardinality n;
Step 4 Choose a set of primes $p_1, p_2, ..., p_k$ such that the product of all p_i is less than $n^{1/4}$;
Step 5 Choose random points $Q_1, Q_2, ..., Q_k$ on E, and compute their discrete logarithms with respect to P using the baby-step giant-step algorithm;
for $i \leftarrow 1$ **to** k **do**
  Step 6 Compute the set of relations $a_{i,j}$ between p_i and the discrete logarithms of Q_i with respect to P using the Pollard rho algorithm;
end
Step 7 Compute the summation polynomial $S(x)$ for the set of relations $a_{i,j}$ using the Furer-Gathen algorithm;
Step 8 Use the conjugate gradient method to solve the linear system $S(x) = 0$ for the coefficients of the unknown logarithms of the prime factors of n;
Step 9 Compute the discrete logarithm of any point on E by combining the computed logarithms of the prime factors of n;

Algorithm 1: Proposed Algorithm for Computing Discrete Logarithms on Elliptic Curves

This algorithm is designed to be more efficient than previous algorithms for computing discrete logarithms on elliptic curves particularly for curves with large prime order and a relatively small number of primes in the set. It achieves this by optimizing the choice of primes in Step 4 to minimize the size of the linear system in Step 8 and using more efficient algorithms for point counting, polynomial evaluation, and linear system solving.

4 Mathematical Working and Proof

Step 1: Choose a factor base B and find a set of smooth relations R :
We choose a factor base $B = \{2, 3, 5, 7, 11\}$.
We compute some multiples of the point $P = (3, 7)$ of the elliptic curve

$$y^2 = x^3 - 23x + 47 \ mod\ 97,$$

until we find some smooth relations with respect to B.

We find the following smooth relations:

$$\begin{aligned} 2P &= (47, 95); \\ 3P &= (5, 20); \\ 5P &= (1, 32); \\ 7P &= (22, 23); \\ 11P &= (84, 12). \end{aligned}$$

We choose 4 of these relations to form a set R given by

$$R = \{2P, 3P, 5P, 7P\}$$

.

Step 2: Use polynomial evaluation techniques to find the polynomial $f(x)$ such that $f(P) = 0$.
We construct a polynomial $f(x)$ such that $f(P) = 0$ using the relations in R.
To do this, we write each relation in terms of the x - coordinate of P

$$\begin{aligned} 2P : 47 &= 3^2 - 23 + 1, 95 = 7^2 - 23.7 + 7; \\ 3P : 5 &= 3^2 - 23, 20 = 7^2 - 23.7; \\ 5P : 1 &= 3^4 - 23^3 + 23^2 - 3, 32 = 7^4 - 23^7 + 23^2.7^2 - 3.7^2; \\ 7P : 22 &= 3^3 - 23^2 + 23 - 1, 23 = 7^3 - 23^2.7 + 23^2.7 - 7. \end{aligned}$$

These equations are used to find a polynomial $f(x)$ such that $f(P) = 0$,

$$f(x) = (x - 3)^2(x - 7)(x^2 + 89x + 703).$$

Step 3: Use polynomial factorization techniques to find the factors of $f(x)$ *mod* p.
We need to factor the polynomial $f(x)$ *mod* p.
We choose $p = 101$ which is close to the square root of the largest coefficient in $f(x)$.
We compute $f(x)$ *mod* p

$f(x) = x^4 + 89x^3 + 902x^2 + 1685x + 703 \equiv x^4 - 12x^3 + 5x^2 - 16x + 96$ *mod* 101

We use a polynomial factorization algorithm to find the factors of $f(x)$ *mod* p :

$$f(x) = (x - 70)(x^3 + 48x^2 + 2x + 85) \text{ } mod \text{ } 101.$$

Step 4: We note that P has order 101, so it generates the cyclic group of points on the elliptic curve. Therefore, we can write $P = kQ$ for some integer k. Then, we have

$$f(P) = 0 = (P - 70Q)(P^3 + 48P^2Q + 2PQ^2 + 85Q^3).$$

Since $P = kQ$, we have

$$f(kQ) = 0 = (kQ - 70Q)((kQ)^3 + 48(kQ)^2Q + 2(kQ)Q^2 + 85Q^3).$$

Here, we know Q, so

$$kQ - 70Q = (84, 12) - 70(3, 7) = (-186, -478).$$

Now, we need to solve for k in the equation

$$(-186, -478)((kQ)^3 + 48(kQ)^2Q + 2(kQ)Q^2 + 85Q^3) = 0.$$

Since $(-186, -478)$ is not on the curve, we cannot use it directly to solve for k. Instead, we use the second factor

$$(kQ)^3 + 48(kQ)^2Q + 2(kQ)Q^2 + 85Q^3 \equiv 0 \text{ } (mod \text{ } 101).$$

We can compute the logarithms of Q and P with respect to the factor base B, which gives:
$\log_Q(2) = 73, \log_Q(3) = 16, \log_Q(5) = 70, \log_Q(7) = 9, \log_Q(11) = 59.$
$\log_P(2) = 1, \log_P(3) = 30, \log_P(5) = 50, \log_P(7) = 95, \log_P(11) = 64.$
We can use the Pohlig-Hellman algorithm to solve for k modulo the prime factors of the order of Q, which are 2, 5, and 101 and otain the following equations:

$$\begin{aligned} k &\equiv 33 \text{ } mod \text{ } 101, \\ k &\equiv 46 \text{ } mod \text{ } 2, \\ k &\equiv 87 \text{ } mod \text{ } 5. \end{aligned}$$

Using the Chinese Remainder Theorem, we can solve for k *mod* $101 \cdot 2 \cdot 5$,

$$k \equiv 693 \text{ } mod \text{ } 1010.$$

Finally, we can compute $\log_Q(P) = k^{-1}$ *mod* $(p - 1)$, where $p = 101$ is the order of the field. We get,

$$k^{-1} = 43 \text{ } mod \text{ } 100.$$

Therefore, the discrete logarithm of P with respect to Q is $\log_Q(P) = 43$.

5 Time Complexity

The time complexity of the new algorithm for computing discrete logarithms on elliptic curves depends on several factors, including the size of the prime p, the order q of the chosen point on the curve and the number and size of the primes in the set used in the algorithm.

Assuming that p is of size L and q is of size M, and that the number of primes in the set is k, the time complexity of the algorithm can be approximated as follows:

Point counting (SEA algorithm): $O(L^2 \log(L))$.

Baby-step giant-step algorithm: $O(\sqrt{q})$.

Pollard rho algorithm: $O(\sqrt{p_i})$.

Furer-Gathen algorithm: $O((k \log(p_i))^2 \log(k \log(p_i)))$.

Conjugate gradient method: $O((k \log(p_i))^2 \log(k \log(p_i)))$.

The dominant factor in the time complexity is the Furer-Gathen algorithm, which computes the summation polynomial, and the conjugate gradient method, which solves the linear system. These steps have a time complexity of $O((k \log(p_i))^2 \log(k \log(p_i)))$ each, where p_i is the largest prime in the set. Therefore, the total time complexity of the algorithm can be approximated as $O((k \log(p_i))^2 \log(k \log(p_i)))$.

Overall, the new algorithm is a significant advancement in the field of cryptography and elliptic curve-based cryptography in particular.

6 Conclusion

The proposed algorithm for computing discrete logarithms on elliptic curves represents a significant improvement over previous methods. By optimizing the choice of prime and point on the curve using an efficient point counting algorithm and choosing a set of primes that minimizes the size of the linear system, the proposed algorithm achieves better computational efficiency. Additionally, the use of the Furer-Gathen algorithm for polynomial evaluation and the conjugate gradient method for solving linear systems further enhances the algorithm's efficiency.

References

[1] A. Amadori, F. Pintore and M. Sala, On the discrete logarithm problem for prime-field elliptic curves, *Finite Field and Their Applications*, **51** (2018), 168-182.

[2] A. Ansari, Using oblique elimination to solve elliptic curve discrete logarithm problem, *International Journal of Engineering Technology and Management Sciences*, **6** (2022), 136-142.

[3] C. Diem, On the discrete logarithm problem in elliptic curves, *Compositio Mathematica*, **147** (2011), 75-104.

[4] J. C. Faugere, P. Gaudry, L. Hout, and G. Renault, Using symmetries in the index calculus for elliptic curves discrete logarithm problem, *Journal of Cryptology*, **27** (2014), 595-635.

[5] S. D. Galbraith and S. W. Gebregiyorgis, *Summation polynomial algorithms for elliptic curves in characteristic two*, International Conference in Cryptology in India, Springer International Publishing, (2014), 409-427.

[6] P. Gaudry, Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm, *Journal of Symbolic Computation*, **44** (2009), 1690-1702.

[7] Y. J. Huang, C. Petit, N. Shinohara, and T. Takagi, *Improvement of Faugere et al. s method to solve ECDLP*, International Workshop on Security, Springer, Berlin-Heidelberg, (2013), 115-132.

[8] Y. J. Huang, C. Petit, N. Shinohara, and T.Takagi, *On generalized first fall degree assumptions*, IACR Cryptology ePrint Archieve, (2015), **358**.

[9] A. Joux and V. Vitse, Elliptic curve discrete logarithm problem over small degree extension fields: Application to the static Diffie-Hellman Problem on, *Journal of Cryptology*, **26** (2013), 119-143.

[10] K. Karabina, *Point decomposition problem in binary elliptic curves*, International Conference on Information Security and Cryptology, Springer International Publishing, 2015.

[11] N. Koblitz and V. S. Miller, ECC (Elliptic Curve Cryptosystems), *Journal of Cryptology*, **2** (1985), 1-28.

[12] G. McGuire and D. Mueller, *A new index calculus algorithm for the Elliptic Curve Discrete Logarithm Problem and Summation Polynomial Evaluation*, IACR Cryptology ePrint Archieve, (2017).

[13] A. Menezes, P. C. Oorschot, and S. A. Vanstone, Reducing elliptic curve logarithms to logarithms in a finite field, *IEEE Transactions on Information Theory*, **39** (1993), 1639-1646.

[14] C. Petit, M. Kosters, and A. Messeng, Algebraic approaches for the elliptic curve discrete logarithm problem over prime fields, *Public-Key Cryptography*, **9615** (2016), 3-18.

[15] R. Schoof, Elliptic Curves over finite fields and the computation of square root mod p, *Mathematics of Computation*, **69** (1985), 423-450.
[16] I. Semaev, Summation polynomials and the discrete logarithm on elliptic curves, *IACR Cryptology ePrint Archieve*, (2004).
[17] I. Semaev, *New algorithm for discrete logarithm problem on elliptic curves*, 2015, arXiv: 1504.01175.
[18] Silverman, J. H., The Arithmetic of Elliptic Curves, 2nd Edition, *Graduate Texts in Mathematics*, Springer, 2009.

ISSN 0304-9892 (Print) ISSN 2455-7463 (Online)
www.vijnanaparishadofindia.org/jnanabha
***Jñānābha* Vol. 55 (I) Special Issue 2025, 29-33**
Proceedings: 5th International Conference and Golden Jubilee Celebrations of VPI (IC-RA-MSA-ET 2022) JNU, New Delhi, India

ANTI-FUZZY ALGEBRAS OVER ANTI-FUZZY FIELDS

Sanjeet Kumar[1], Manoranjan Kumar Singh[1,*] and Sudipta Gayen[2]
[1]Department of Mathematics, Magadh University, Bodh-Gaya, Bihar, India-824234
[2]Centre for Data Science, Faculty of Engineering & Technology, Siksha 'O' Anusandhan (Deemed to be University), Odisha, India-751030
Email: drsanjeetkumar1994@gmail.com, drmksingh gaya@yahoo.com, sudi23dipta@gmail.com
(Received: January 08, 2025; In format: June 09, 2025; Revised: June 30, 2025; Accepted: July 10, 2025)

DOI: https://doi.org/10.58250/jnanabha_SI.2025.55104

Abstract

This article introduces a comprehensive framework for anti-fuzzy algebra within the context of the anti-fuzzy field, broadening its fundamental concepts to cover a wider range. To facilitate this development, a collection of illustrative examples and theoretical analyses is included, providing a deeper understanding of its structural properties and possible applications.

2020 Mathematical Sciences Classification: 03E72, 08A72, 20N25.
Keywords and Phrases: Anti-fuzzy field, Fuzzy linear spaces, Anti-fuzzy algebra, Fuzzy set theory.

1 Introduction

Zadeh's [16] groundbreaking conceptualization of fuzzy sets *(FS)* transformed the field of mathematics, leading to the development of fuzzy mathematics. This innovative framework combines various ideas and methods, allowing for their use in a wide range of theoretical and practical areas. Among these, the following [1, 2, 4, 5, 6, 7, 8, 10, 11, 13] are some noteworthy contributions in pure mathematics.

The idea of fuzzy algebra (FA) over fuzzy field (FF), first introduced by Nanda [12]. However, Nanda's concepts have faced criticism. For example, Gu and Lu [9] showed that some elements of FA, as initially proposed, were illogical and needed significant changes. Nevertheless, the foundational concepts of FF and FA continue to inspire further exploration and critical analysis by other researchers. Biswas [3] and subsequently Singh [14] revisited Nanda's ideas, pinpointing limitations and suggesting necessary adjustments to strengthen these concepts. This critical discussion prompted further research into anti-fuzzy structures by several other researchers, who played a role in developing alternative ideas in this field.

The primary objective of this paper is to propose a more generalized and robust framework for anti-fuzzy algebra (AFA) over the anti-fuzzy field (AFF). We present a detailed formulation of this new framework, demonstrating its comprehensiveness and conceptual appeal. Additionally, we derive several novel results that emerge naturally from this generalization. To support the validity and utility of our proposed framework, illustrative examples are provided, offering concrete insights into it.

2 Preliminaries

Definition 2.1 ([16]). *. Let G be any nonempty set. A mapping of the form $P : G \to [0, 1]$ is designated a FS of G.*

Definition 2.2 ([3]). *Let S be a field and F be a FS on S. Then F be referred to as a FF of S if the following propositions are true:*
(i) $F(w_1 + w_2) \geq \min\{F(w_1), F(w_2)\} \forall w_1, w_2 \in S$,
(ii) $F(-w_1) \geq F(w_1) \forall w_1 \in S$,
(iii) $F(w_1 w_2) \geq \min\{F(w_1), F(w_2)\} \forall w_1, w_2 \in S$,
(iv) $F\left(w_1^{-1}\right) \geq F(w_1) \forall w_1 (\neq 0) \in S$.

Definition 2.3 ([15]). *Let S be a field and F be a FS on S. Then F is referred to as a AFF of S, if the subsequent axioms are satisfied:*
(i) $F(w_1 + w_2) \leq \max\{F(w_1), F(w_2)\} \forall w_1, w_2 \in S$,
(ii) $F(-w_1) \leq F(w_1) \forall w_1 \in S$,
(iii) $F(w_1 w_2) \leq \max\{F(w_1), F(w_2)\} \forall w_1, w_2 \in S$,
(iv) $F\left(w_1^{-1}\right) \leq F(w_1) \forall w_1 (\neq 0) \in S$.

Definition 2.4 ([9]). *Let A be an algebra over field S and Ω ba a FS on A. Then Ω be designated as a FA of A over FF F of S if $\forall w_1, w_2 \in A$ and $k \in S$*
(i) $\Omega(w_1 + w_2) \geq \min\{\Omega(w_1), \Omega(w_2)\}$,
(ii) $\Omega(kw_1) \geq \min\{F(k), \Omega(w_1)\}$,
(iii) $\Omega(w_1 w_2) \geq \min\{\Omega(w_1), \Omega(w_2)\}$,
(iv) $F(1) \geq \Omega(w_1)$.

Theorem 2.1 ([16]). *Suppose F is an AFF of the field S, then*
(i) $F(0) \leq F(w_1) \forall w_1 \in S$,
(ii) $F(1) \leq F(w_1) \forall w_1 (\neq 0) \in S$,
(iii) $F(0) \leq F(1)$.

3 Anti-fuzzy Algebra

Definition 3.1 ([9]). *Let A be an algebra over the field S with Ω as a FS on A. Then Ω is said to be an AFA of A over an $AFFF$ of S if $\forall w_1, w_2 \in A$ and $k \in S$*
(i) $\Omega(\mathrm{w}_1 + \mathrm{w}_2) \leq \max\{\Omega(\mathrm{w}_1), \Omega(\mathrm{w}_2)\}$,
(ii) $\Omega(\mathrm{kw}_1) \leq \max\{\mathrm{F(k)}, \Omega(\mathrm{w}_1)\}$,
(iii) $\Omega(\mathrm{w}_1 \mathrm{w}_2) \leq \max\{\Omega(\mathrm{w}_1), \Omega(\mathrm{w}_2)\}$,
(iv) $\mathrm{F}(1) \leq \Omega(\mathrm{w}_1)$.

Example 3.1. Consider the field $S = \{Z_3, \bigoplus_3, \otimes_3\}$ and F be a FS of S characterized by

$$F(x) = \begin{cases} 0.2, & x = 0 \\ 0.3, & \text{otherwise.} \end{cases}$$

Here, we notice that F is AFF of S.
Let $A = \{0, u, v, w\}$ be a set having two binary operations "+" and "." in such a way that:

$+$	0	u	v	w
0	0	u	v	w
u	u	0	w	v
v	v	w	0	u
w	w	v	u	0

$\cdot$	0	u	v	w
0	0	0	0	0
u	0	v	0	v
v	0	0	0	0
w	0	v	0	v

Also, if a scalar multiplication over A is described as

$$\lambda x = \begin{cases} 0, & \lambda = 0 \\ x, & \text{otherwise.} \end{cases}$$

Clearly, A is an algebra over S. Assume that Ω be a FS of A described as

$$\Omega(x) = \begin{cases} 0.4, & x = 0 \\ 0.6, & \text{otherwise.} \end{cases}$$

In fact, for all $w_1, w_2 \in A$ and $k \in S$ the following can be obtained
(i) $\Omega(w_1 + w_2) \leq \max\{\Omega(w_1), \Omega(w_2)\}$,
(ii) $\Omega(kw_1) \leq \max\{F(k), \Omega(w_1)\}$,
(iii) $\Omega(w_1 w_2) \leq \max\{\Omega(w_1), \Omega(w_2)\}$,
(iv) $F(1) \leq \Omega(w_1)$.
So, Ω is an AFA of A over $AFFF$ of S.

Theorem 3.1. *If Ω be an AFA in A over an $AFFF$ in a field S, then $F(0) \leq \Omega(w_1), \forall w_1 \in A$.*
Proof: By the definition of AFF and an $AFA, F(0) \leq F(1)$ and $F(1) \leq \Omega(w_1)$. This implies that $F(0) \leq \Omega(w_1) \forall w_1 \in A$.

Theorem 3.2. *If Ω be an AFA in A over an $AFFF$ in a field S iff the following three conditions hold:*
(i) $\Omega(k_1 w_1 + k_2 w_2) \leq \max[\max\{F(k_1), \Omega(w_1)\}, \max\{F(k_2), \Omega(w_2)\}]$,
(ii) $\Omega(w_1 w_2) \leq \max\{\Omega(w_1), \Omega(w_2)\}$,
(iii) $F(1) \leq \Omega(w_1) \forall w_1, w_2 \in A$ *and* $k_1, k_2 \in S$.

Proof. Suppose Ω be an AFA in A over an AFF F in a field S. Then $\forall w_1, w_2 \in A$ and $k_1, k_2 \in S$, we have
$\Omega(k_1w_1 + k_2w_2) \leq \max\{\Omega(k_1w_1), \Omega(k_2w_2)\} \leq \max[\max\{F(k_1), \Omega(w_1)\}, \max\{F(k_2), \Omega(w_2)\}]$.

Since Ω is an anti-fuzzy algebra, the remaining two conditions hold directly. On the contrary, we assume that all three requirements of the postulation are true. Then

$$\begin{aligned}
\Omega(w_1 + w_2) &= \Omega(1w_1 + 1w_2) \\
&\leq \max[\max\{F(1), \Omega(w_1)\}, \max\{F(1), \Omega(w_2)\}], \\
&\leq \max[\max, \{\Omega(w_1), \Omega(w_1)\}, \max\{\Omega(w_2), \Omega(w_2)\}], \\
&\leq \max\{\Omega(w_1), \Omega(w_2)\}. \\
\Omega(kw_1) &\leq \Omega(kw_1 + 0w_1) \\
&\leq \max[\max\{F(k), \Omega(w_1)\}, \max\{F(0), \Omega(w_1)\}], \\
&\leq \max[\max\{F(k), \Omega(w_1)\}, \max\{\Omega(w_1), \Omega(w_1)\}], \\
&= \max[\max\{F(k), \Omega(w_1)\}, \Omega(w_1)], \\
&= \max\{F(k), \Omega(w_1)\}.
\end{aligned}$$

i.e., $\Omega(kw_1) \leq \max\{F(k), \Omega(w_1)\}$.

Clearly, we have
$\Omega(w_1w_2) \leq \max\{\Omega(w_1), \Omega(w_2)\}$ and $F(1) \leq \Omega(w_1)$.

Hence, Ω is an AFA in A over an $AFFF$ in a field S. □

Theorem 3.3. *If Ω be an AFA in A over an AFF F in a field S, then $\Omega(0) \leq \Omega(w_1), \forall w_1 \in A$.*

Proof. Suppose Ω be an AFA in A over an $AFFF$ in a field S. Then

$$\begin{aligned}
\Omega(0) &= \Omega(w_1 - w_1) \\
&= \Omega(1w_1 + (-1w_1)) \\
&\leq \max[\max\{F(1), \Omega(w_1)\}, \max\{F(-1), \Omega(w_1)\}], \\
&\leq \max[\max\{\Omega(w_1), \Omega(w_1)\}, \max\{F(1), \Omega(w_1)\}], \\
&\leq \max[\max\{\Omega(w_1), \Omega(w_1)\}, \max\{\Omega(w_1), \Omega(w_1)\}], \\
&= \max\{\Omega(w_1), \Omega(w_1)\}, \\
&= \Omega(w_1).
\end{aligned}$$

i.e., $\Omega(0) \leq \Omega(w_1), \forall w_1 \in A$. □

Theorem 3.4. *The FS Ω is an AFA in A over an $AFFF$ in a field S iff Ω^c is a FA in A over an FF F^c in a field S.*

Proof. Let Ω be an AFA in A. Then $\forall w_1, w_2 \in A$ and $k \in S$, we have

$$\begin{aligned}
\Omega^c(w_1 + w_2) &= 1 - \Omega(w_1 + w_2) \\
&\geq 1 - \max\{\Omega(w_1), \Omega(w_2)\}, \\
&= \min\{1 - \Omega(w_1), 1 - \Omega(w_2)\}, \\
&= \min\{\Omega^c(w_1), \Omega^c(w_2)\}. \\
\Omega^c(w_1w_2) &= 1 - \Omega(w_1w_2) \\
&\geq 1 - \max\{\Omega(w_1), \Omega(w_2)\}, \\
&= \min\{1 - \Omega(w_1), 1 - \Omega(w_2)\}, \\
&= \min\{\Omega^c(w_1), \Omega^c(w_2)\}. \\
\Omega^c(kw_1) &= 1 - \Omega(kw_1) \\
&\geq 1 - \max\{F(k), \Omega(w_1)\}, \\
&= \min\{1 - F(k), 1 - \Omega(w_1)\}, \\
&= \min\{F^c(k), \Omega^c(w_1)\}. \\
F^c(1) &= 1 - F(1) \\
&\geq 1 - \Omega(w_1), \\
&= \Omega^c(w_1).
\end{aligned}$$

Thus, Ω^c is a FA in A. Similarly, we can establish the converse of the above result. □

Theorem 3.5. *Let A_1 and A_2 be two algebras over a field S. Let $\rho : A_1 \to A_2$ be an onto homomorphism. If Ω_1 is an AFA in A_2 over an AFF F in S, then $\rho^{-1}(\Omega_1)$ in A_1 is an AFA over F.*

Proof. Since For all $w_1, w_2 \in A_1$ and $k_1, k_2 \in S$

$$\begin{aligned}
\rho^{-1}(\Omega_1)(k_1w_1 + k_2w_2) &= \Omega_1(\rho(k_1w_1 + k_2w_2)) \\
&= \Omega_1(k_1\rho(w_1) + k_2\rho(w_2)) \\
&\leq \max\{\Omega_1(k_1\rho(w_1)) + \Omega_1(k_2\rho(w_2))\}, \\
&\leq \max\{\max(F(k_1), \Omega_1(\rho(w_1))), \max(F(k_2), \Omega_1(\rho(w_2)))\}, \\
&= \max\left\{\max\left(F(k_1), \rho^{-1}(\Omega_1)(w_1)\right), \max\left(F(k_2), \rho^{-1}(\Omega_1)(w_2)\right)\right\}. \\
\rho^{-1}(\Omega_1)(w_1w_2) &= \Omega_1(\rho(w_1w_2)) \\
&= \Omega_1(\rho(w_1)\rho(w_2)), \\
&\leq \max\{\Omega_1(\rho(w_1)), \Omega_1(\rho(w_2))\}, \\
&= \max\left\{\rho^{-1}(\Omega_1)(w_1), \rho^{-1}(\Omega_1)(w_2)\right\}.
\end{aligned}$$

Since Ω_1 is an AFA in A_2, then we have
$F(1) \leq \Omega_1(\rho(w_1)) = \rho^{-1}(\Omega_1)(w_1) \forall \rho(w_1) \in A_2$, where $w_1 \in A_1$. Hence $\rho^{-1}(\Omega_1)$ in A_1 is an anti-fuzzy algebra over F. □

Theorem 3.6. *The Intersection of two AFAs need not be an AFA.*
We will establish this result by displaying a suitable example.

Example 3.2. Consider the field $S = \{Z_3, \bigoplus_3, \otimes_3\}$ and F be a FS of S characterized by

$$F(x) = \begin{cases} 0.1, & x = 0 \\ 0.2, & \text{otherwise.} \end{cases}$$

Here, we notice that F is the AFF of S.
Let $A = \{0, u, v, w\}$ be a set having two binary operations "+" and "." in such a way that:

+	0	u	v	w
0	0	u	v	w
u	u	0	w	v
v	v	w	0	u
w	w	v	u	0

·	0	u	v	w
0	0	0	0	0
u	0	v	0	v
v	0	0	0	0
w	0	v	0	v

Also, if a scalar multiplication over A is described as

$$\lambda x = \begin{cases} 0, & \lambda = 0 \\ x, & \text{otherwise.} \end{cases}$$

Clearly, A is an algebra over S. Assume that Ω_1 and Ω_2 are AFAs of A over AFF F of S, described as

$$\Omega_1(x) = \begin{cases} 0.5, & x = 0 \\ 0.4, & \text{otherwise.} \end{cases}$$

$$\Omega_2(x) = \begin{cases} 0.5, & x = 0 \\ 0.3, & \text{otherwise.} \end{cases}$$

Here, if we consider $\alpha =$ w and $\beta =$ w, then we have

$$\begin{aligned}
&(\Omega_1 \cap \Omega_2)(w + w) \leq \max\{(\Omega_1 \cap \Omega_2)(w), (\Omega_1 \cap \Omega_2)(w)\} \\
&\Rightarrow (\Omega_1 \cap \Omega_2)(0) \leq \max\{0.3, 0.3\} \\
&\Rightarrow 0.5 \leq 0.3
\end{aligned}$$

But it is not possible
Hence, the intersection of two $AFAs$ need not be an AFA.

Theorem 3.7. *Union of a family of AFAs is an AFA.*

Proof. Let $\{\Omega_i\}_{i\in I}$ be a family of $AFAs$ of in A over an $AFFF$ in a field S. Let $\Omega = \underset{i\in I}{\cup}\Omega_i = \mathrm{Sup}_{i\in I}\,\Omega_i$. For all $w_1, w_2 \in A$ and $k_1, k_2 \in S$, we have

$$\begin{aligned}
\Omega(k_1w_1 + k_2w_2) &= \mathrm{Sup}_{i\in I}\,\Omega_i(k_1w_1 + k_2w_2)\\
&\leq \mathrm{Sup}_{i\in I}\left[\max\left\{\max\left(F(k_1), \Omega_i(w_1)\right), \max\left(F(k_2), \Omega_i(w_2)\right)\right\}\right],\\
&= \max\left\{\max\left(F(k_1), \mathrm{Sup}_{i\in I}\,\Omega_i(w_1)\right), \max\left(F(k_2), \mathrm{Sup}_{i\in I}\,\Omega_i(w_2)\right)\right\},\\
&= \max\left\{\max\left(F(k_1), \Omega(w_1)\right), \max\left(F(k_2), \Omega(w_2)\right)\right\}.\\
\Omega(w_1w_2) &= \mathrm{Sup}_{i\in I}\,\Omega_i(w_1w_2)\\
&\leq \mathrm{Sup}_{i\in I}\left[\max\left\{\Omega_i(w_1), \Omega_i(w_2)\right\}\right],\\
&= \max\left\{\mathrm{Sup}_{i\in I}\,\Omega_i(w_1), \mathrm{Sup}_{i\in I}\,\Omega_i(w_2)\right\},\\
&= \max\left\{\Omega(w_1), \Omega(w_2)\right\}.
\end{aligned}$$

Since, each Ω_i is an AFA and then we have

$$F(1) \leq \Omega_i(w_1) \leq \sup_{i\in I}\Omega_i(w_1) = \Omega(w_1)$$

Hence, Ω is an AFA of A over an $AFFF$ in a field S.
i.e., The union of the family of $AFAs$ is an AFA. □

4 Conclusion

In this paper, we have formulated the novel conception of AFA over AFF. Here, our approach has been conceived under a sound footing of fuzzy sets and has a very wide repercussion over the results in this area. This paper displays some unique examples along with mind-boggling results in this area.

Acknowledgement. We are very much thankful to the Editor for going through it very minutely and Reviewers for their valuable and constructive suggestions to bring the paper to the present form.

References

[1] Abdlkadir Aygnolu, Halis Aygn, Introduction to fuzzy soft groups, Computers, *Mathematics with Applications,* **58** (2009), 1279-1286.
[2] R. Biswas, Intuitionistic fuzzy subgroups, *Mathematical Forum,* **10** (1989), 39-44.
[3] R. Biswas, Fuzzy fields and fuzzy linear spaces redefined, *Fuzzy sets and systems,* **33** (1989), 257-259.
[4] C. L. Chang, Fuzzy topological spaces, *Journal of Mathematical Analysis and Applications,* **24** (1968),182-190.
[5] S. Gayen, S. Jha and M. Singh, On direct product of a fuzzy subgroup with an anti-fuzzy subgroup, *International Journal of Recent Technology and Engineering,* **8** (2019), 1105-1111.
[6] S. Gayen, S. A. Edalatpanah, S. Jha, R. Kumar and others, On the Characterization of Antineutrosophic Subgroup, *Advances in Mathematical Physics,* 2023 (2023), 1-10.
[7] S. Gayen, F. Smarandache, S. Jha, M. K. Singh, S. Broumi and R. Kumar, Introduction to plithogenic hypersoft subgroup, *Neutrosophic Sets and Systems,* **33** (2020), 208-233.
[8] S. Gayen, F. Smarandache, S. Jha, M. K. Singh, S. Broumi and R. Kumar, Soft subring theory under interval-valued neutrosophic environment, *Neutrosophic Sets and Systems,* **36** (2020), 193-219.
[9] W. Gu and T. Lu, Fuzzy algebras over fuzzy fields redefined, *Fuzzy sets and systems,* **53** (1993), 105-107.
[10] W. J. Liu, Fuzzy invariant subgroups and fuzzy ideals, *Fuzzy Sets and Systems,* **8** (1982), 133-139.
[11] S. Nanda, Fuzzy fields and fuzzy linear spaces, *Fuzzy sets and systems,* **19** (1986), 89-94.
[12] S. Nanda, Fuzzy algebras over fuzzy fields, *Fuzzy sets and systems,* **37** (1990), 99-103.
[13] A. Rosenfeld, Fuzzy groups, *Journal of mathematical analysis and applications,* **35** (1971), 512-517.
[14] M. Singh, Theory of Fuzzy Structures and Applications, *Lambert Academic Publishing,* (2010).
[15] T. Srinivas, P. N. Swamy and T. Nagaiah, Anti fuzzy near-algebras over anti fuzzy fields, *Annals of Fuzzy Mathematics and Informatics*, **4** (2012), 243-252.
[16] L. A. Zadeh, *Information and control, Fuzzy sets,* **8** (1965), 338-353.

ISSN 0304-9892 (Print) ISSN 2455-7463 (Online)
www.vijnanaparishadofindia.org/jnanabha
***Jñānābha* Vol. 55 (I) Special Issue 2025, 34-40**
Proceedings: 5th International Conference and Golden Jubilee Celebrations of VPI (IC-RA-MSA-ET 2022) JNU, New Delhi, India

BURR *X* DISTRIBUTION REPRESENT TO ACCELERATED LIFE TEST WITH SAMPLING PLAN

S.Gandhiya Vendhan and K.Chitraleka
Department of Statistics, Bharathiar University, Tamil Nadu, India-641046
Email: gandhiyavendhan@yahoo.com, chitraleka2011@gmail.com
(Received: January 08*,* 2023*; Informat: February* 24,2024*; Revised: June* 02*,* 2025*; Accepted: July* 04*,* 2025*)*

DOI: https://doi.org/10.58250/jnanabha_SI.2025.55105

Abstract

This papers study on truncated life tests takes a look at while the lifetime follows the Burr *X* distribution represented in a recognition sampling plan. Accelerated lifestyles check is at the moment the focal manner of measuring invention reliability rapidly, and the layout of efficient take a look at tactics is important to ensure that *ALTs* can determine the product dependability and sensitivity analyses are executed to evaluate the make certain an impact on which the improbability inside the assumed *AF* brings at the threats. This examines the development of the idea and approach for the improvement of the most fulfilling *ALT* for the region and scale distribution, that's the furthermost purposeful and innovative shape of designing the most fulfilling *ALT* plan. A running function value represented within the sampling plans with associated threats is mentioned in the tables and related values.
2020 Mathematical Sciences Classification: 62C05, 60Exx.
Keywords and Phrases: Sampling Plan, Accelerate Life test, Producer risk, Consumer risk, Burr *X* Distribution.

1 Introduction

In the technique of manipulating the share of defective gadgets within the production, the technique is to be minimized and its miles carried out via the technique of manipulating charts. Product management way controlling the pleasant of the product using critical examination through sampling inspection plans. Reliability or life trying out includes estimating the expected durability over the years of an object. This will be an entire machine, a product, or a man or woman thing. We might also focus on a detail of an issue, which includes material assets.

An existence test is an electrical stress test that usually employs voltage and/or temperature to accelerate the appearance of damage-out reliability failures in a tool. To ensure reliability, life tests examine sampling, which usually involves accepting and rejecting a collection of things. General standards for processing the lots based on the sampled data must be precisely planned in terms of the existing test techniques for effective and efficient implementation of lifestyle examination sampling. Because a life test sample technique always includes a time-based life test, censorship and/or acceleration are frequently employed to cut down on testing time and effort.

In this work, hybrid censored *LSPs* with a specified form parameter are evolved for the Burr *X* distribution. The existence examination is presumptively conducted at a multiplied setting for which the *AF* is assumed. The development of *LSPs* has fulfilled producer and consumer risks. The outcomes of the sources of uncertainty in the acceleration factor and form parameters that were assumed were then assessed at the specific producer and client risks, and a technique for creating *LSPs* that can account for these uncertainties were also established.

2 Burr *X* distribution

Burr presented twelve distinct types of cumulative distribution features for modelling data [4]. The Burr-*X* and Burr-*XII* distribution capabilities garnered the most interest out of the one, twelve distribution capabilities. Rodriguez interprets the Burr- *XII* distribution in a radical manner [18]; also see Wingo [22]. In this work, we take into account the two-parameter Burr type *X* distribution. Two variables The cumulative distribution of the Burr- Type *X* distribution is as follows

Cumulative Distribution Function (*CDF*)

$$F(x,\alpha,\lambda)=\left(1-e^{(\frac{x}{\lambda})^2}\right)^{\alpha} \quad x\geq 0,\ \alpha\geq 0,\ \lambda\geq 0. \tag{2.1}$$

Probability Density Function (*PDF*)

$$f(x,\alpha,\lambda)=\frac{2\alpha x}{\lambda^2}e^{(\frac{x}{\lambda})^2}(1-e^{(-\frac{x}{\lambda})^2})^{(\alpha-1)} \quad x\geq 0,\ \alpha\geq 0,\ \lambda\geq 0. \tag{2.2}$$

The survival function of Burr-Type X distribution has

$$S(x,\alpha,\lambda)=1-\left(1-e^{(-\frac{x}{\lambda})^2}\right)^{\alpha} \quad x\geq 0,\ \alpha\geq 0,\ \lambda\geq 0. \tag{2.3}$$

The hazard rate is given by

$$h(x,\alpha,\lambda)=\frac{\frac{2\alpha x}{\lambda^2}e^{-(\frac{x}{\lambda})^2}\left(1-e^{-(\frac{x}{\lambda})^2}\right)^{(\alpha-1)}}{1-\left(1-e^{-\left(\frac{x}{\lambda}\right)^2}\right)^{\alpha}};\quad x\geq 0,\ \alpha\geq 0,\ \lambda\geq 0. \tag{2.4}$$

3 Review of Burr *X* distribution

In their [7] work, Khaleel *et al.* introduced the Beta Burr type X distribution, an unique non-stop distribution that extends the Burr type X distribution and has increased, reduced, and tub forms for the risk characteristic. In this study, Ahmad *et al.* [1] developed an estimation of R where y and x are independent but no longer identically distributed Burr type X random variables. To investigate the three estimating techniques, Monto Carlo simulation is accomplished. While the information is provided in businesses, Aludatat *et al.* [2] got Bayesian and non-Bayesian estimators for the parameter of the Burr type X distribution. The generated information's utility suggests that the estimators are effective. Umar Rizam Abu Bakar and Yusuf Madaki study due to Yousof and Afify [23] expands the Kum-G family and Burr X distribution by introducing a beta Kumaraswamy Burr type X distribution with six parameters. Beta Kum-BX distribution compared to a number of its sub-styles and also distinctive in-law style. Its characteristics make it a great model for symmetric right- and left-skew data sets.

We recommend medical practitioners, docs, engineers, and statisticians undertake this appropriate Beta Kum-BX in modeling their massive group of records as it consists of 3 strong fashions assets. In their study, Khaleel and Ibrahim [7], they introduced the new extension distribution for Burr X with the Beta Burr X parameter. Beta Burr X distribution derived *CDF*, *PDF*, and chance characteristic for *BBX1*. This distribution carried out rainfall facts and used statistical criteria to illustrate the goodness-of-match of the rainfall statistics. Refacy [17] this model parameters and the acceleration element have envisioned the usage of the most probability estimation approach and sample predictions are considered for future order facts. In addition, the asymptotic confidence intervals for the model parameters are mentioned. Nesor Ahmad *et al.* [3] this article discussed the gold standard increased lifestyles test plans for Burr kind X distribution with a log-linear version underneath periodic inspection and type I censoring. *ALT* plans for minimizing as var($\hat{Y}$a) below the assumptions of Burr type X distribution, periodic inspection, and type I censoring with a log-linear version.

The findings that the biased estimates have at the insurance of the decrease-z sure, the unfairness of and the anticipated asymptotic variance were explored by Surles and Padgett [20]. The work due to Raqab and Kundu [16] is intended to help readers to remember the unique components of a parameter. The relationship between the Burr-type X distribution and other well-studied distributions, such as the gamma distribution and the Weibull distribution. Homes by Irving Burr [4] will be discussed, along with the concept of the cumulative feature and the challenges of becoming the characteristic. Examples are shown and a discussion of a new cumulative feature with good-sized practicability is possible.

A thorough mathematical analysis of the beta burr type X distribution is provided in this publication by Faton Merovci, Mundher Abdullah Khaleel, *et al.* [9]. Additionally, the Fisher records matrix is used to determine the asymptotic self-belief durations for the parameters. By adding a further form parameter, Yousof and Afify [23] presented a new Burr *X-G (BX-G)* family of distributions. Through taking integer parameter values, several distributions develop into unique cases of the suggested family. A few numerical homes belonging to the new family. Plans for reputation sampling for the Burr type X distribution by Hu and Gui [5]. Tables with the minimum sample sizes are essential to guarantee the median's existence.

Sartawi and Abu-Salih have explored several facets of the single parameter ($\lambda = 1$) Burr type X distribution. where and represent the scale and shape parameters, respectively [19]. Ahmad *et al.* [3], Jaheem [6]. Nowadays, the generalized Rayleigh (GR) distribution, as effectively observed by Surles and Padgett, can be thought of as the Burr-type X distribution along the same lines as the GE distribution [20]. For the sake of clarity, In this study, The GR distribution will be used to refer to the Burr-type X distribution. It was shown that the two-parameter GR distribution and the two-parameter gamma, Weibull, and GE distributions have a lot in common.

Stress is believed to be a temporal characteristic that increases linearly. The most probabilistic strategy, as well as the McMc approach, are used to produce traditional and Bayesian estimates for version parameters. In this study, Mustafa Korkmaz and Emrah Altun *et al.* [16] explore the distribution using a few different models to demonstrate the distribution's adaptability in representing facts with heavy tails. Utilizing data from data collecting examples, a novel version of the VaR (Value of Risk) estimation with the Burr X Pareto distribution is shown. This version offers an alternative to the generalized Pareto version for financial institutions. In their [3] study, Nesar Ahmad and Sabiha Khan *et al.* take into account planning ALT for objects whose lifetimes adhere to the Burr type X failure version.

4 Accelerated Life Test

Accelerated life testing (ALT) is a technique of taking a look at and analyzing to decide how disasters could probably occur inside the destiny. ALT is a famous technique of testing because of its ability to accelerate time. ALT is regularly used while we can't manage to pay to watch for screw-ups to occur at their ordinary charge however we want to recognize how disasters are possible to occur in the future.

Consider an electronics manufacturer who wants to understand how many screw-ups will occur in 10 years (possibly for assurance functions). If the factor being examined has a mean life of 30 years, the producer cannot fairly spend several years performing a reliability check as they are ready to release their product on the market soon. By increasing the pressure on the component, failure could be induced more rapidly. If carried out efficaciously, that is equal to speed up the passage of time. The electronics manufacturer can accumulate failure facts at a ramification of stresses, to shape the correct life-pressure version, and then enter the use pressure into the life-pressure version to decide the failure distribution that is expected to arise at the use pressure.

A selection of techniques, which serve one-of-a-kind purposes, had been termed expanded existence trying out which involves the acceleration of disasters with the single motive of the quantification of the life traits of the product underneath ordinary use conditions.

4.1 Assumptions of *LSPs*

1. At time 0, under a challenging scenario for which AF is known, n devices are randomly selected from a large pool and put to the test.
2. Failed devices are not replaced by fresh ones.
3. The lifestyle examination of the prolonged state is halted either at the censoring time A or at the c failure, whichever occurs first.
4. The lot is rejected if the cth failure occurs first. The lot is approved under all other circumstances.

4.2 Constructions, of the *LSPs*

The modern world examines sampling issues, which are best described as the following hypothesis testing issue.

$$\begin{cases} H_0 : \eta U = \eta U_0 \\ H_1 : \eta U = \eta U_1 \qquad \eta U_1 < \eta U_0. \end{cases} \tag{4.1}$$

In which ηU_0 *and* ηU_1 are pre-precise constants that can be decided upon by a small number of producers and buyers. The project time tUM in the usage situation is provided and lets in $RU\ (tUM) = (1\text{-}FU\ (tUM))$ to be the reliability at the project time. The validity of the subsequent courtship is then established.

The mutual settlement on $RU\ (tUM)$ can be expressed in phrases of ηU. n the upgraded scenario, the device lives trails a Burr X distribution with the size parameter being determined by the formula $\eta A = \eta U/AF$. and the shape parameter is constant. This is, the CDF of the lifetime at the improved specification is given through.

$$F_A(t_A) = (1 - e^{(-\frac{tA}{\eta A})^2})^\theta. \tag{4.2}$$

The expanded circumstance, hypotheses (4.1) may be re-expressed as follows,

$$\begin{cases} H_0 : \eta A = \eta A_0. \\ H_1 : \eta A = \eta A_1 \quad \eta A_1 < \eta A_0. \end{cases} \tag{4.3}$$

The pattern length (n) and rejection quantity (c) are taken into account together with the *LSP* to ensure that the requirements for the next manufacturer and customer opportunity are met.

$$L(\eta A0) = Pr\left(\frac{Acceptalot}{\eta A = \eta A0}\right) = \sum_{k=0}^{c-1} \binom{n}{k} (1-q_0)^k q_0^{n-k} = 1-\alpha, \tag{4.4}$$

$$L(\eta A1) = Pr\left(\frac{Acceptalot}{\eta A = \eta A1}\right) = \sum_{k=0}^{c-1} \binom{n}{k} (1-q_1)^k q_1^{n-k} = \beta. \tag{4.5}$$

Items lives at the accelerated condition follow a Burr X distribution with scale parameter defined but shape parameter left untouched byηA . In other words, the lifetime *CDF* undert the accelerated condition is given by

$$F_A(t_A) = (1 - e^{(-\frac{tA}{\eta A})^2})^\theta. \tag{4.6}$$

The sample size (n) and the number of rejections (c) of the *LSP* must satisfy the following producer and consumer risk standards

$$\sum_{k=0}^{c-1} \binom{n}{k} (1-q_0)^k q_0^{n-k} \geq 1-\alpha, \tag{4.7}$$

$$\sum_{k=0}^{c-1} \binom{n}{k} (1-q_1)^k q_1^{n-k} \leq \beta, \tag{4.8}$$

$$q_i = 1 - \left(1 - e^{-(\frac{\tau_A}{\eta U})^2}\right)^\theta, i = 0, 1 \tag{4.9}$$

and α and β necessarily satisfy both the producer and consumer risks.

$$q_i = 1 - \left(1 - e^{-(\frac{\tau_A * AF}{\eta U})^2}\right)^\theta, \tag{4.10}$$

since $\eta_A = \frac{\eta_U}{AF}$ For i=0,1. In eq(4.10), $(\tau * AF)$ A is the same "censoring time" as the form and q_i could be interpreted as the possibility that a unit is an correspondent "censoring time" at the usage condition under testing hypotheses. The resulting *LSPs* are displayed in Tables 4.1 and 4.2 for the following combinations of parameter values.
(α,β)= (0.05,0.05),(0.01,0.01),
q_0=0.99,0.97,0.95,0.90,0.85,0.80,0.75,0.70,0.60,0.50,
q_1=0.97,0.95,0.90,0.85,0.80,0.75,0.70,0.60,0.50,0.40.

4.3 Properties of *LSPs*

The following characteristics apply to the *LSPs* in Tables 4.1 and 4.2.

1. As q_0 rises for a given, α,β and q_1, n falls.
2. For given α,β and q_0, n decreases as q_1 increases.
3. As and/or rises for a given α,β and q_1, n decreases.
4. c acts the same way as in (4.1) through 4.7 over.

Following are some explanations for property (4.1). for a given q_1 and the current q_0 consider the sample plan (n,c) that satisfies the inequality (4.7) and (4.8). According to John *et al.* the following link exists withν_1=2c and ν_2=2(n-c+1) as its parameters, of the F distribution. The summing term in (4.7) increases, as q increases because $\frac{\nu_2(1-q)}{\nu_1 q}$ decreases as q grows. In other words, as q_0 rises, the left side of inequality (4.7) gets bigger. Assume that q_0 is raised to $q_0^{'}$ and that n' is the smallest sample size needed for the given values of q_1 and $q_0^{'}$.

Example 4.1. In positive-type digital electronics, voltage is used as a stress variable to hasten breakdowns, and inverse strength dating has been successfully applied (Nelson *et al.* [12]). Given by is the AFAF for the inverse power connection (Nelson *et al.* [12]). $AF = (VA/VU)^{\nu}AF = (V_AV_U)^{\nu}$ Where V^U isthe voltage used in the circumstance (measured in V), V^A is the extended voltage, (measured in V) and ν is the tool's feature parameter. Assume that τ_A is the censoring time under the accelerated condition is 900h, η *U0* =100,0000 η *U1*=250084, α=0.05, β=0.05, then, (15) or (16) can be used to calculate q_0 and q_1. $q_0 = 1-(1-e^{(-\frac{900*5.287}{1000000})^2})^{0.2}.$, $q_1 = 1-(1-e^{(-\frac{900*5.287}{250084})^2})^{0.2}$. Then the corresponding *LSP* is approximately determined using Table 2 with $q_0 = 95$, and q_1=90, this results in (n, c) = (234, 17). Then, using Table 4.2 and $q_0 = 95$, and q_1=90, the appropriate *LSP* is roughly computed, yielding (n,c) = (234, 17).

Example 4.2. If τ_A is 500h the time spent censoring under accelerated conditions and ηU0=100,0000 η U1=180655,α=0.01, β =0.01, respectively, then equations (4.9) or (4.10) can be used to get q_0 and q_1 Using (4.10), we obtain q_0=1-(1-e$^{(-\frac{500*18.28}{1000000})^2}$)$^{0.05}$., q_1=1-(1-e$^{(-\frac{500*18.28}{180655})^2}$)$^{0.05}$. Then, using Table 4.1 and $q_0 = 95$ and $q_1 = 90$, the appropriate LSP is roughly computed, yielding (n,c) = (299,7).

Table* 4.1: Hybrid Censored For LSPs α=0.01, β = 0.01*

q_1	q_0			α=1						
	99	95	90	85	80	75	70	60	50	40
95	7,299	(b,a)		-	-	-	-	-	-	-
90	6,200	66,850	-	-	-	-	-	-	-	-
85	6,175	48,600	68,530	-	-	-	-	-	-	-
80	5,155	45,580	59,425	38,175	-	-	-	-	-	-
75	4,100	41,555	53,375	35,165	62,245	-	-	-	-	-
70	4,90	40,535	45,300	29,134	57,228	40,115	-	-	-	-
60	3,55	26,325	35,240	28,100	44,165	30,86	40,105	-	-	-
50	3,40	24,300	29,190	28,75	29,99	30,80	35,82	35,63	-	-
40	2,25	20,225	18,100	24,60	24,75	25,60	27,60	25,45	33,51	-
30	1,8	15,100	11,50	15,30	20,55	15,30	23,43	15,24	23,33	18,23

Table* 4.2: Hybrid Censored For LSPs α=0.05, β=0.05*

q_1	q_0									
	99	95	90	85	80	75	70	60	50	40
95	10,950	-	-	-	-	-	-	-	-	-
90	8,140	17,234	-	-	-	-	-	-	-	-
85	7,140	17,215	17,16	-	-	-	-	-	-	-
80	6,96	13,210	16,11	19 90	-	-	-	-	-	-
75	6,72	7 100	15,10	17, 79	23,85,	-	-	-	-	-
70	5,55	6,80	12,80	15,70	18,65	23,70	-	-	-	-
60	4,40	5,65	10,62	15, 70	18, 65	22,67	27,70	-	-	-
50	3,20	4,49	9,55	13, 60	16, 55	20 60	26, 67	45, 93	-	-
40	2,11	3,34	6,34	11, 48	14,48	18, 52	25, 64	45,94,	55, 95	-
30	1,5	1,9	3,14	11, 47	12,40	15,43	22,55	42,87	43,73	56,86

−not applicable since $q_0 \leq q_1$
[a]Sample size (n)
[b]Rejection number (c)
[c]n > 1,000

5 Applications

Application 5.1

The data collection is made up of 63 measurements of the strengths of 1.5 cm glass fibers that were originally collected by staff members at the UK National Physical Laboratory. Sadly, the document does not provide the measurement units. The numbers are 0.55, 0.74, 0.77, 0.81, 0.84, 0.93, 1.04, 1.11, 1.13, 1.24, 1.25, 1.27, 1.28, 1.29, 1.30, 1.36, 1.39, 1.42, 1.48, 1.48, 1.49, 1.49, 1.51, 1.52, 1.53, 1.54, 1.55, 1.55, 1.58, 1.59, 1.60, 1.61, 1.61, 1.62, 1.63, 1.64, 1.66, 1.66, 1.67, Smith and Naylor have also examined these data.

Application 5.2

Microcircuit failure can happen as a result of electro migration, which is the movement of atoms within the conductors of the circuit. The information below comes from a 59 conductor accelerated life test (Nelson and Doganaksoy [13]). There are no suppressed observations, and failure times are measured in hours. 6.545 9.289 7.543 6.956 6.492 5.459 8.120 4.706 8.687 2.997 8.591 6.129 11.038 5.381 6.958 4.288 6.522 4.137 7.459 7.495 6.573 6.538 5.589 6.087 5.807 6.725 8.532 6.663 6.369 7.024 8.336 9.218 7.398 6.033 10.092 7.496 4.531 7.974 8.799 7.683 7.224 7.365 6.923 5.640 5.434 7.937 6.515 6.476 6.071 10.491 5.923 In this instance, when n=59, the mean x =6.929, and the standard deviation s=1.574843.

Application 5.3

Online Data Entry software evaluation Table 1 displays the test data from a modest online data entry software product that has been around in Japan since 1980 (Ohba [14]). The software is a little over 40,000 LOC in size. The number of shifts dedicated to running test cases and evaluating the outcomes served as the basis for calculating the testing time. Table 5.1 displays the couples of observation time and total number of faults discovered.

***Table* 5.1**

Testing time	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
Failures	2	1	1	1	2	2	2	1	7	3	1	2	2	4	1	6	1	3	1	3	1
Cumulative failures	2	3	4	5	7	9	11	12	19	21	22	24	26	30	31	37	38	41	42	45	46

6 Conclusion

For the Burr X distribution, Accelerated life test created fully hybrid censored life test sampling problem are developed under the assumption that the AF between the extended and usage scenarios as well as the form parameter are known. Sensitivity analysis of the uncertainty in AF and m show that if AF are overestimated, the real manufacturer risk will grow, whereas the real customer risk will increase asAF are underestimated.

Among the most common lifespan distributions utilised in reliability engineering is the Burr X distribution. In order to save down on testing time and effort, advanced, hybrid censored life checking out procedures are frequently used in practise. Therefore, it is highly anticipated that reliability engineers would be able to successfully and effectively employ the findings from this effort to guarantee the dependability of their products. The shape parameter is regarded as being acknowledged in this article. Future research may be successful by extending the current examination to the scenario where the form parameter is unknown. Comparisons of the current *LSPs* with the plans subject to type-I or type-II censorship with ongoing test device monitoring is another study field for the future.

References

[1] K. E. Ahmad, M. E. Fakhry and Z. F. Jaheen, Empirical Bayes Estimation of $P(Y < X)$ and Characterization of Burr-type X Model, *Journal of Statistical Planning and Inference*, **64** (1997), 297-308.

[2] K. M. Aludaat, M. T. Alodat and T. T. Alodat, Parameter Estimation of Burr Type X Distribution for Grouped Data, *Applied Mathematical Sciences*, **9** (2) (2008), 415-423.

[3] N. Ahmad, S. Khan, and M. G. M. Khan, Planning Accelerated Life Test for Burr Type X Failure Model with Type I, Censoring, *Journal of Statistical Theory and Applications*, **12** (3) (2013), 266-287.

[4] I. W. Burr, Cumulative frequency functions, *Annals of Mathematical Statistics*, **13** (1942), 215-222.

[5] M. Hu and W. Gui, Acceptance sampling plans based on truncated life tests for Burr type X distribution, *Journal of Statistics and Management Systems*, **21**(3) (2018), 323-336.

[6] Z. F. Jaheen, Bayesian approach to prediction with outliers from the Burr Type X model, Microelectron, *Reliability*, **35** (4) (1995), 703-705.
[7] M.A. Khaleel, N.A. Ibrahim, M. Shitan and F. Merovci, Beta Burr type X with application to rainfall data, *Malaysian Journal of mathematical sciences*, **11** (2017), 73-86.
[8] A. K. Mahto, Y. M. Tripathi and Shuo-Jye Wu, Statistical inference based on progressively type-II censored data from the Burr X distribution under progressive-stress accelerated life test, *Journal of Statistical Computation and Simulation*, **91** (2) (2020), 368-382.
[9] F. Merovci, M. A. Khaleel,, N. A. Ibrahim, and M. Shitan, The beta Burr type X distribution properties with the application, *SpringerPlus*, **5** (2016), 1-18.
[10] K. C. Mustafa, E. Altun, H. M. Yousof, A. Z. Afify and Saralees Nadarajah, The Burr X Pareto Distribution: Properties, applications and VaR Estimation, *Journal of Risk and Financial Management*, **11** (1) (2017), 1-16.
[11] U. Y. Madaki, M. R. A. Bakar, L. Handique, Beta Kumaraswamy Burr Type X Distribution and Its Properties, *ASEANA Journal of Science and Education*, **2** (2) (2018), 1138.
[12] W. Nelson, and T. J. Kielpinski, Theory for Optimum Censored Accelerated Tests for Normal and Lognormal Life Distribution, *Technometrics*, **18** (1976), 105 -114.
[13] W. Nelson and N.Doganoksoy, Statistical analysis of life or strength data from specimens of various sizes using the power-(log) normal model, *InRecent Advances in Life-Testing and Reliability*, CRC Press, (1995), 377-408.
[14] M. Ohba, Software reliability analysis models, *IBM Journal of Research Development*, **28** (4)(1984), 428-443.
[15] M. Z. Raqab, Order statistics from the Burr type X model, *Computers and Mathematics with Applications*, **36** (4) (1998), 111-120.
[16] M. Z. Raqab and D. Kundu, Burr type X distribution: revisited. *Journal of Probability and Statistical Sciences*, **4** (2) (2006), 179-193.
[17] R. M. Refaey, Estimating and prediction accelerated life test using constant stress for Marshall-Olkin Extended Burr Type X Distribution Based on Type-II Censoring, *Al-Azhar Bulletin of Science*, **32** (1) (2021), 45-59.
[18] R. N. Rodriguez, A Guide to the Burr Type XII Distributions, *Biometrika*, **64** (1977) 129-134.
[19] H. A. Sartawi, and M. S.Abu-Salih, Bayes Prediction Bounds for the Burr Type X Model, *Communication in Statistics- Theory and Methods*, **20** (1991), 2307-2330.
[20] J. G. Surles and W. J. Padgett, Inference for reliability and stress-strength for a scaled Burr Type X distribution, *Lifetime Data Analysis*, **7** (2) (2001), 187-200.
[21] J. G. Surles and W. J. Padgett, Some properties of a scaled Burr type X distribution, *Journal of Statistical Planning and Inference*, **128** (1) (2005), 271-280.
[22] D. Wingo, Maximum likelihood methods for fitting the burr type XII distribution to multiply (Progressively), censored life test data, *Metrika: International Journal for Theoretical and Applied Statistics, Springer,* **40** (1) (1993), 203-210.
[23] H. M. Yousof and A. Z. Afify, The Burr X Generator of Distributions for Lifetime Data, *Journal of Statistical Theory and Applications*, **16** (3) (2017) 288-305.

ISSN 0304-9892 (Print) ISSN 2455-7463 (Online)
www.vijnanaparishadofindia.org/jnanabha
***Jñānābha* Vol. 55 (I) Special Issue 2025, 41-52**
Proceedings: 5th International Conference and Golden Jubilee Celebrations of VPI (IC-RA-MSA-ET 2022) JNU, New Delhi, India

BERNOULLI WAVELET COLLOCATION APPROACH FOR FRACTIONAL ZAKHAROV-KUZNETSOV EQUATION

S. Kumbinarasaiah[1], R. Yeshwanth[2] and S. Dhawan[3]
[1,2]Department of Mathematics, Bangalore University, Bengaluru, Karnataka, India-560056
[3]Department of Mathematics, CCS HAU Haryana, India-125004.
Email: kumbinarasaiah@bub.ernet.in, yeshwanth@bub.ernet.in, sharanjeet@hau.ac.in
(Received: October 09, 2023; In format: May 21, 2025; Revised: June 2024, 2015; Accepted: July 04, 2025)

DOI: https://doi.org/10.58250/jnanabha_SI.2025.55106

Abstract

Fractional partial differential equations (*PDEs*) of particular classes, like the nonlinear fractional Zakharov-Kuznetsov equation, are the subject of this work. We propose a novel methodology, the Bernoulli wavelet collocation method (*BWCM*). A collocation approach based on the Bernoulli wavelets is used to solve such equations. After that, we translate the mathematical model into an algebraic system of equations by utilizing the wavelet features. One can obtain an approximation answer using the Newton-Raphson method to solve these algebraic equations. Tables and graphs are used to analyze and compare the results with other methods reported in the literature. With the help of suitable parameter settings and a thorough explanation of the physical behavior of the solutions, these results are visually described. Two numerical problems are provided to demonstrate the precision of the stated approach. Many fractional *PDEs*, as is well known, lack exact solutions, and several semi-analytical approaches depend on regulating parameters to function; however, this method is parameter-free. It also takes less time to run the applications and is simple to apply. The numerical method based on wavelets that have been proposed is efficient and appealing from a computational standpoint. The suggested method's convergence analysis is presented in terms of the theorem. The numerical computations and visualizations are done in Matlab.

2020 Mathematical Sciences Classification: 65M70, 65T60
Keywords and Phrases: Partial differential equations; Collocation method; Integration; Bernoulli wavelets; Newton Raphson technique

1 Introduction

Fractional differential equations (*FDEs*) have drawn much attention from researchers in the last ten years because they can be applied to improve real-world problems in various engineering and physics domains. Countless scientific miracles in signal processing, probability, chemical physics and statistics, electrochemistry of corrosion, acoustics, and electromagnetics are accurately represented by fractional order differential equations [10]. Differential equations of integer order can be considered generalized by nonlinear *PDEs* [8]. Fractional partial differential equations (*FPDEs*) are indispensable for modeling many real-world problems in the present day. Fractional calculus can be called the calculus of this century [4] due to its wide range of applications in various fields of science and technology. Nonlinear *PDEs* are used to simulate the main problems in the physical sciences, including mathematical physics. Fractional order is crucial in studying nonlinear physical phenomena because it helps solve nonlinear evolution problems. This article presents a fractional-time numerical method for solving two-dimensional nonlinear Zakharov-Kuznetsov equations using Bernoulli wavelets. The Zakharov-Kuznetsov equation describes the isotropic evolution of a nonlinear ion-acoustic wave; many observations suggest that the wave travels discontinuously in time, and some properties hidden in a nonlinear wave must be investigated over a range of time scales. For example, the laminar theory may explain the main flow characteristic of a flow in a tube; however, a fractional model is needed to clarify the vortex close to the boundary at a shorter time scale.

In this present study, the fractional nonlinear Zakharov-Kuznetsov equation in time is studied:

$$\frac{\partial^{\alpha} u}{\partial t^{\alpha}} + a\frac{\partial u^{p}}{\partial x} + b\frac{\partial^{3} u^{q}}{\partial x^{3}} + c\frac{\partial^{3} u^{r}}{\partial x\,\partial y^{2}} = 0, \tag{1.1}$$

where α is a parameter that characterizes fractional derivatives and u is a function of y, x, and t. The behavior of ion-acoustic waves is represented by the natural numbers p, q, and r, and the real constants a, b, and c, where $0 < \alpha \leq 1$.

In the presence of a constant magnetic field, ion-acoustic waves which are composed of cold ions and hot isothermal electronsare hardly nonlinear in plasma. This kind of three-dimensional nonlinear equation was initially discovered while studying steady-state magnetized lossless plasma in order to demonstrate weakly ion-acoustic waves. The foundation for the development of this idea is a dependable and effective computing process for studying nonlinear fractional differential equations. Given that they are used in the mathematical modeling of real-world issues. However, throughout the past three decades, new approaches to the explanation of non-linear differential systems with fractional order have been discovered. Simultaneously, new computer techniques and symbolic programming have been developed. The analytical and numerical solutions of non-linear fractional differential equations are crucial. Since non-linear fractional differential equations are used to mathematically model most complex processes. In light of this, numerous approaches to solving these equations can be found in the literature, A robust computational approach for Zakharov-Kuznetsov equations via Shehu transform [30], Solution for fractional Zakharov-Kuznetsov equations by using two reliable techniques [36], Computational Technique to study Analytical Solutions to Fractional Modified Zakharov-Kuznetsov equation [1], Numerical Investigation of Fractional-Order Zakharov-Kuznetsov equation [32], Numerical Simulation of Fractional Zakharov-Kuznetsov equation using Projected Differential Transform method [19], Solitary wave solutions of Fractional Zakharov-Kuznetsov equation arising in Quantum Magneto Plasma [20], Approximate Analytical Solutions to Generalized and Modified Zakharov-Kuznetsov equations [25], New exact solutions of Zakharov-Kuznetsov equations by Sardar-subequation method [38], Analytical solution of Fractional Zakharov-Kuznetsov equations [33], Modified Homotopy methods for generalized fractional Zakharov-Kuznetsov equations [2].

In applied and computational numerical exploration, wavelet analysis is a relatively new and developing discipline. Wavelets are mathematical functions that aid in breaking up data into distinct recurrent components and encourage the examination of each element of data with a scale-appropriate purpose. When analyzing physical situations with discontinuities and strong spikes in the sign, wavelets outperform standard Fourier methods. A new mathematical technique called the wavelet transform can break down a signal into several lower-resolution levels by adjusting a single wavelet function's scaling and shifting components. An increasingly used tool in the computational and applied sciences is Bernoulli wavelets. They have been used in many contexts, including signal analysis and data compression. The following is a list of some mathematical issue categories that the wavelet approach can handle: Modeling anomalous infiltration and diffusion using variable-order nonlinear fractional differential equations [5], differential equations for neutral delays [7], Dirichlet boundary condition for fractional partial differential equations [26], fractional delay DEs [27], Nonlinear Lane-Emden Type Singular Equations [3], singular Volterra integro-DEs [34], Caputo fractional delay DEs [11], Jeffery-Hamel flow numerical solution using wavelet approach [12, 28], A unique method for fractional linked multidimensional Equation of Navier-Stokes [13], Utilizing a novel coupled wavelet approach, the nonlinear reaction-diffusion equation is addressed [9]; a successful numerical simulation employing the Laguerre wavelet approach to solve a class of Fokker-Planck equations [35], Brusselator chemical model of fractional order using the Fibonacci wavelet collocation approach [21], Studying the biological pest model in tea plants using the Haar wavelet technique [14], convection diffusion equation by legendre wavelet [6], taylor wavelet approach for the Fredholm Integro-differential equation [37], comparative study of wavelet methods for solving Bernoullis equation [31].Utilizing the Differential Transformation Method and Hermite Wavelet Method to Address Nonlinear Temperature Distribution in a Rectangular Moving Porous Fin [29], MHD boundary layer flow analysis of a viscous fluid using the Bernoulli wavelet method [15], Ultraspherical wavelets through the Benjamin Bona Mohany equation [22], Haar wavelet technique to study Chlamydia transmission [17], study of fractional Klein-Gordan equation [23], wavelet approach for fractional PDEs [39], Fibonacci wavelets approach for fractional *SEIR* & smoking model [24]. The main goal is to introduce and describe a novel numerical technique for estimating the approximate solution to impossible-to-solve nonlinear *PDEs*. The outcomes are contrasted with alternative methods found in the literature. As per the present literature review, Fractional Zakharov-Kuznetsov equations have not been solved using *BWCM*.

Section 2 provides an overview of the study's structure and describes the properties of the Bernoulli wavelet idea, which forms the basis for the rest of the research. Section 3 gives a few theorems on the

Bernoulli wavelet. Section 4 provides the Bernoulli wavelet collocation method for solving Zakharov-Kuznetsov equations. Section 5 displays numerical findings and a discussion. Section 6 concludes with a final analysis.

2 Preliminaries of Fractional derivative and Bernoulli wavelet

Definition 2.1. *The Riemann-Liouville's fractional integral operator of $f \in C_\mu$ of order $\delta \geq 0$ defined as [16]*

$$J_s^\delta f(s) = \begin{cases} f(s) & \text{if } \delta = 0 \\ \frac{1}{\Gamma(\delta)} \int_0^s (s-t)^{\delta-1} f(t) dt & \text{if } \delta \geq 0\,. \end{cases}$$

The gamma function is indicated here by the symbol Γ. Where, C_μ is continuous linear space.

Definition 2.2. *The Caputo fractional derivative of $f(t) \in C_\mu$ is defined as,*

$$\frac{\partial^\delta f(t)}{\partial t^\delta} = \frac{1}{\Gamma(m-\delta)} \int_0^t (t-s)^{m-\delta-1} f^{(m)}(s) ds$$

For $m-1 < \delta \leq m$, $t > 0$, m is any positive integer, $f(t) \in C_\mu^m$, $\mu \geq -1$, where, C_μ^m is continuous linear space containing $f^m(t)$.

Bernoulli wavelets

Bernoulli wavelets $U_{n,m}(t) = U(k, \hat{n}, m, t)$ have four parameters; $n = 1, 2, 3, \cdots, 2^{k-1}$, k is a +ve integer, m be the degree of the Bernoulli polynomials, $\hat{n} = n - 1$, and t be the normalized time. One can define Bernoulli wavelets as [3, 16, 18] on the interval $[0, 1)$.

$$U_{n,m}(t) = \begin{cases} 2^{\frac{k-1}{2}} \tilde{b}_m(2^{k-1}t - \hat{n}), & \frac{\hat{n}}{2^{k-1}} \leq t < \frac{\hat{n}+1}{2^{k-1}}, \\ 0, & \text{Otherwise}, \end{cases}$$

with

$$\tilde{b}_m(t) = \begin{cases} 1, & m = 0, \\ \frac{1}{\sqrt{\frac{(-1)^{m-1}(m!)^2}{(2m)!} a_{2m}}} b_m(t), & m > 0. \end{cases}$$

Where $n = 1, 2, \cdots, 2^{k-1}, m = 0, 1, 2, \cdots, M-1$. The coefficient $\frac{1}{\sqrt{\frac{(-1)^{m-1}(m!)^2}{(2m)!} a_{2m}}}$ is for normality, $q = \hat{n}\, 2^{-(k-1)}$ is the translation parameter, and $p = 2^{-(k-1)}$ is the dilation parameter. In this case, the well-known Bernoulli polynomials of degree m, denoted as $b_m(t)$, are well defined by; $b_m(t) = \sum_{i=0}^m \binom{m}{i} a_{m-i} t^i$, where a_i, $i = 0, 1, \cdots, m$ are Bernoulli numbers.

3 Convergence Analysis

Theorem 3.1. *Let $u(x, y, t)$ be the continuous bounded real function on $[0, 1) \times [0, 1) \times [0, 1)$. Then, Bernoulli wavelet expansion of $u(x, y, t)$ is uniformly converges to $u(x, y, t)$.*

Proof. Let $u(x, y, t)$ is continuous on $[0, 1) \times [0, 1) \times [0, 1)$ and is bounded by real number k. Assume that

$$u(x, y, t) = \sum_{i,j,k=1}^{\infty} \sum_{l,m,n=0}^{\infty} a_{ijk}^{lmn} \psi_{i,l}(x)\, \psi_{j,m}(y)\, \psi_{k,n}(t),$$

$$a_{ijk}^{lmn} = \langle u(x, y, t),\ \psi_{i,l}(x)\, \psi_{j,m}(y)\, \psi_{k,n}(t) \rangle\,,$$

where $\langle , \rangle$ represents the inner product. Hence

$$\begin{aligned} a_{ijk}^{lmn} &= \int_0^1 \int_0^1 \int_0^1 u(x, y, t) \psi_{i,l}(x)\, \psi_{j,m}(y)\, \psi_{k,n}(t) dx dy dt, \\ &= \int_0^1 \int_0^1 \psi_{i,l}(x)\, \psi_{j,m}(y) \int_l u(x, y, t) 2^{\frac{k-1}{2^2}} \bar{b_m}(2^{k-1}t - n + 1) dt dx dy, \end{aligned}$$

where $I = \left[\frac{n-1}{2^{k-1}}, \frac{n}{2^{k-1}}\right)$, put $2^{k-1}t - n + 1 = P$, then

$$a_{ijk}^{lmn} = 2^{\frac{k-1}{2}} \int_0^1 \int_0^1 \psi_{i,l}(x)\, \psi_{j,m}(y) \int_0^1 u(x, y, \frac{P-1+n}{2^{k-1}} \bar{b_m}(P)) \frac{dP}{2^{k-1}} dx dy$$

$$a_{ijk}^{lmn} = 2^{\frac{k-1}{2}} \int_0^1 \int_0^1 \Big[\int_0^1 u(x,y,\frac{P-1+n}{2^{k-1}}) \bar{b_m}(P)dP \Big] \psi_{i,l}(x)\psi_{j,m}(y)dxdy.$$

By generalized mean value theorem for integrals

$$a_{ijk}^{lmn} = 2^{\frac{k-1}{2}} \int_0^1 \int_0^1 u\Big(x,y,\frac{\xi_1-1+n}{2^{k-1}}\Big)\psi_{i,l}(x)\psi_{j,m}(y)dxdy[\int_0^1 \bar{b_m}(P)dP].$$

Here, $\xi_1 \in (0,1)$ and put $\int_0^1 \bar{b_m}(P)dP = A$,

$$\begin{aligned} a_{ijk}^{lmn} &= A2^{\frac{1-k}{2}} \int_0^1 \int_0^1 u\Big(x,y,\frac{\xi_1-1+n}{2^{k-1}}\Big)\psi_{i,l}(x)\psi_{j,m}(y)dxdy \\ &= A2^{\frac{1-k}{2}} \int_0^1 \int_0^1 u\Big(x,y,\frac{\xi_1-1+n}{2^{k-1}}\Big)2^{\frac{1-k}{2}}\bar{b_m}(2^{k-1}y-n+1)dy\psi_{i,l}(x)dx. \end{aligned}$$

Put $2^{k-1}y-n+1=q$ and $l=\Big[\frac{n-1}{2^{k-1}},\frac{n}{2^{k-1}}\Big)$,

$$a_{ijk}^{lmn} = A\int_0^1 \psi_{i,l}(x)\int_0^1 u\Big(x,\frac{q-1+n}{2^{k-1}},\frac{\xi_1-1+n}{2^{k-1}}\Big)\bar{b_m}(q)\frac{dq}{2^{k-1}}\psi_{i,l}(x)dx.$$

By generalized mean value theorem for integrals

$$a_{ijk}^{lmn} = A2^{1-k}\int_0^1 u\Big(x,\frac{\xi_2-1+n}{2^{k-1}},\frac{\xi_1-1+n}{2^{k-1}}\Big)\psi_{i,l}(x)dx\int_0^1 \bar{b_m}(q)dq.$$

Put $\int_0^1 \bar{b_m}(q)dq = B$, then

$$a_{ijk}^{lmn} = AB2^{1-k}\int_l u(x,\frac{\xi_2-1+n}{2^{k-1}},\frac{\xi_1-1+n}{2^{k-1}})2^{\frac{k-1}{2}}\bar{b_m}(2^{k-1}x-n+1)dx.$$

Put $2^{k-1}x-n+1=r$ we get,

$$\begin{aligned} a_{ijk}^{lmn} &= AB2^{-(\frac{k-1}{2})}\int_0^1 u(\frac{r-1+n}{2^{k-1}},\frac{\xi_2-1+n}{2^{k-1}},\frac{\xi_1-1+n}{2^{k-1}})\bar{b_m}(r)\frac{dr}{2^{k-1}} \\ &= AB2^{-\frac{3}{2}(k-1)}\int_0^1 u(\frac{r-1+n}{2^{k-1}},\frac{\xi_2-1+n}{2^{k-1}},\frac{\xi_1-1+n}{2^{k-1}})\bar{b_m}(r)dr. \end{aligned}$$

By generalized mean value theorem for integrals

$$a_{ijk}^{lmn} = AB2^{-\frac{3}{2}(k-1)}u\Big(\frac{\xi_3-1+n}{2^{k-1}},\frac{\xi_2-1+n}{2^{k-1}},\frac{\xi_1-1+n}{2^{k-1}}\Big)\int_0^1 \bar{b_m}(r)dr.$$

Put $\int_0^1 \bar{b_m}(r)dr = C$ and u is bounded by k,
Therefore,

$$\begin{aligned} a_{ijk}^{lmn} &\le ABCk2^{-\frac{3}{2}(k-1)} \\ &\implies |a_{ijk}^{lmn}| \le k. \end{aligned}$$

Hence

$$\sum_{i,j,k=1}^{\infty}\sum_{i,m,n=0}^{\infty} a_{ijk}^{lmn}$$

is absolutely convergent. Thus the Bernoulli wavelet approximation of $u(x,y,t)$ is uniformly converges. □

4 Bernoulli Wavelet Collocation Method.

To solve general form of the nonlinear fractional Zakharov-Kuznetsov equation in (1.1), we assume that,

$$u_{xxxt}(x,y,t) = \sum_{i,j,k=1}^{\infty}\sum_{l,m,n=0}^{\infty} a_{ijk}^{lmn}\,\psi_{i,l}(x)\,\psi_{j,m}(y)\,\psi_{k,n}(t). \tag{4.1}$$

Truncating the equation (4.1) we get,

$$u_{xxxt}(x,y,t) \approx \sum_{i,j,k=1}^{2^{k-1}}\sum_{l,m,n=0}^{M-1} a_{ijk}^{lmn}\psi_{i,l}(x)\,\psi_{j,m}(y)\,\psi_{k,n}(t), \tag{4.2}$$

where, a_{ijk}^{lmn} are unknown coefficients and $\psi_{i,l}(x)$, $\psi_{j,m}(y)$, $\psi_{k,n}(t)$ are Bernoulli wavelet functions.

Integrate equation (4.2) concerning t from limit 0 to t,

$$u_{xxxt}(x,y,t) = u_{xxx}(x,y,0) + \int_0^t \sum_{i,j,k=1}^{2^{k-1}} \sum_{l,m,n=0}^{M-1} a_{ijk}^{lmn} \psi_{i,l}(x)\, \psi_{j,m}(y)\, \psi_{k,n}(t) dt. \tag{4.3}$$

Integrate equation (4.3) concerning x trice from limit 0 to x,

$$\begin{aligned} u_{xx}(x,y,t) &= u_{xx}(0,y,t) + u_{xx}(x,y,0) - u_{xx}(0,y,0) + \int_0^x \int_0^t \sum_{i,j,k=1}^{2^{k-1}} \sum_{l,m,n=0}^{M-1} \\ &\quad a_{ijk}^{lmn} \psi_{i,l}(x)\, \psi_{j,m}(y)\, \psi_{k,n}(t) dt dx, \end{aligned} \tag{4.4}$$

$$\begin{aligned} u_x(x,y,t) &= u_x(0,y,t) + x[u_{xx}(0,y,t) - u_{xx}(0,y,0)] + u_x(x,y,0) - u_x(0,y,0) + \\ &\int_0^x \int_0^x \int_0^t \sum_{i,j,k=1}^{2^{k-1}} \sum_{l,m,n=0}^{M-1} a_{ijk}^{lmn} \psi_{i,l}(x)\, \psi_{j,m}(y)\, \psi_{k,n}(t) dt dx dx, \end{aligned} \tag{4.5}$$

$$\begin{aligned} u(x,y,t) &= u(0,y,t) + x[u_x(0,y,t) - u_x(0,y,0)] + u(x,y,0) - u(0,y,0) + \frac{x^2}{2}[u_{xx}(0,y,t) \\ &\quad - u_{xx}(0,y,0)] + \int_0^x \int_0^x \int_0^x \int_0^t \sum_{i,j,k=1}^{2^{k-1}} \sum_{l,m,n=0}^{M-1} a_{ijk}^{lmn} \psi_{i,l}(x)\, \psi_{j,m}(y)\, \psi_{k,n}(t) dt dx dx dx. \end{aligned} \tag{4.6}$$

Put $x = 1$ in (4.5) and (4.6) then we get

$$\begin{aligned} u_x(1,y,t) &= [u_x(0,y,t) - u_x(0,y,0)] + [u_{xx}(0,y,t) - u_x x(0,y,0)] + u_x(1,y,0) + \\ &\quad \Big[\int_0^x \int_0^x \int_0^t \sum_{i,j,k=1}^{2^{k-1}} \sum_{l,m,n=0}^{M-1} a_{ijk}^{lmn} \psi_{i,l}(x)\, \psi_{j,m}(y)\, \psi_{k,n}(t) dt dx dx \Big] |_{x=1}, \end{aligned} \tag{4.7}$$

$$\begin{aligned} u(1,y,t) &= u(0,y,t) - u(0,y,0) + u(x,y,0) + [u_x(0,y,t) - u_x(0,y,0)] + \frac{1}{2}[u_{xx}(0,y,t) \\ &- u_{xx}(0,y,0)] + \Big[\int_0^x \int_0^x \int_0^x \int_0^t \sum_{i,j,k=1}^{2^{k-1}} \sum_{l,m,n=0}^{M-1} a_{ijk}^{lmn} \psi_{i,l}(x)\, \psi_{j,m}(y)\, \psi_{k,n}(t) dt dx dx dx \Big] |_{x=1}. \end{aligned} \tag{4.8}$$

From (4.7) and (4.8), we get

$$\begin{aligned} \frac{1}{2}[u_{xx}(0,y,t) - u_{xx}(0,y,0)] &= [u_x(1,y,t) - u(1,y,t)] - u_x(1,y,0) + u(0,y,t) - u(0,y,0) \\ &+ u(x,y,0) + \Big[\int_0^x \int_0^x \int_0^x \int_0^t \sum_{i,j,k=1}^{2^{k-1}} \sum_{l,m,n=0}^{M-1} a_{ijk}^{lmn} \psi_{i,l}(x)\, \psi_{j,m}(y)\, \psi_{k,n}(t) dt dx dx dx \Big] |_{x=1} \\ &- \Big[\int_0^x \int_0^x \int_0^t \sum_{i,j,k=1}^{2^{k-1}} \sum_{l,m,n=0}^{M-1} a_{ijk}^{lmn} \psi_{i,l}(x)\, \psi_{j,m}(y)\, \psi_{k,n}(t) dt dx dx \Big] |_{x=1}, \end{aligned} \tag{4.9}$$

and

$$\begin{aligned} [u_x(0,y,t) - u_x(0,y,0)] &= u_x(1,y,t) - u_x(1,y,0) + \Big[\int_0^x \int_0^x \int_0^t \sum_{i,j,k=1}^{2^{k-1}} \sum_{l,m,n=0}^{M-1} a_{ijk}^{lmn} \psi_{i,l}(x) \\ &\psi_{j,m}(y)\, \psi_{k,n}(t) dt dx dx \Big] |_{x=1} - 2\Big[u_x(1,y,t) - u(1,y,t) - u_x(1,y,0) \\ &+ u(0,y,t) - u(0,y,0) + u(x,y,0) + \Big[\int_0^x \int_0^x \int_0^x \int_0^t \sum_{i,j,k=1}^{2^{k-1}} \sum_{l,m,n=0}^{M-1} a_{ijk}^{lmn} \psi_{i,l}(x) \\ &\psi_{j,m}(y)\, \psi_{k,n}(t) dt dx dx dx \Big] |_{x=1} - \Big[\int_0^x \int_0^x \int_0^t \sum_{i,j,k=1}^{2^{k-1}} \sum_{l,m,n=0}^{M-1} a_{ijk}^{lmn} \psi_{i,l}(x) \end{aligned}$$

$$\psi_{j,m}(y)\,\psi_{k,n}(t)dtdxdx\Big]|_{x=1}\Big]. \qquad (4.10)$$

Employ (4.9) & (4.10) in (4.8), (4.7), and (4.6), then use these equations in the general nonlinear fractional Zakharov Kuznetsov equation. Further, collocate the obtained equation using the following collocation points.

$$x_i = y_i = t_i = \frac{2i-1}{2(2^{k-1})^3M^3}, \qquad i = 1, 2, \cdots (2^{k-1})^3M^3.$$

Then we get a system containing $(2^{k-1})^3M^3$ number of algebraic equations with $(2^{k-1})^3M^3$ number of unknowns. Solving this system by Newton-Raphson method that yields values of unknown coefficients. Obtained unknown coefficients are fitted in (4.6), yielding the bernoulli wavelet-based numerical solution.

5 Numerical Results and Discussion.

In this section, we consider some test cases to check the accuracy of the proposed solution method.

Example 5.1. Consider time-fractional Zakharov-Kuznetsov equation :

$$D_t^\alpha u + (u^3)_x + 2(u^3)_{xxx} + 2(u^3)_{xyy} = 0, \qquad 0 < \alpha \leq 1, \qquad (5.1)$$

with initial condition

$$u(x, y, 0) = \frac{3}{4}\sigma(e^{(x+y/6)} - e^{-(x+y/6)}).$$

The exact solution to (5.1) when $\alpha = 1$, is given by $u(x, y, t) = \frac{3}{4}\sigma(e^{(x+y-\frac{\sigma t}{6})} - e^{-(x+y-\frac{\sigma t}{6})})$.

The above example is solved using the proposed method; Figures 5.1 and 5.2 represent the Geometrical comparison of the Exact solution and the Numerical solution at $k = 1, \sigma = 1$ and $t = 0, y = 0$. Figure 5.3 represents the Numerical solution at $k = 1, \sigma = 1$ and $t = 0$ for different values of α.

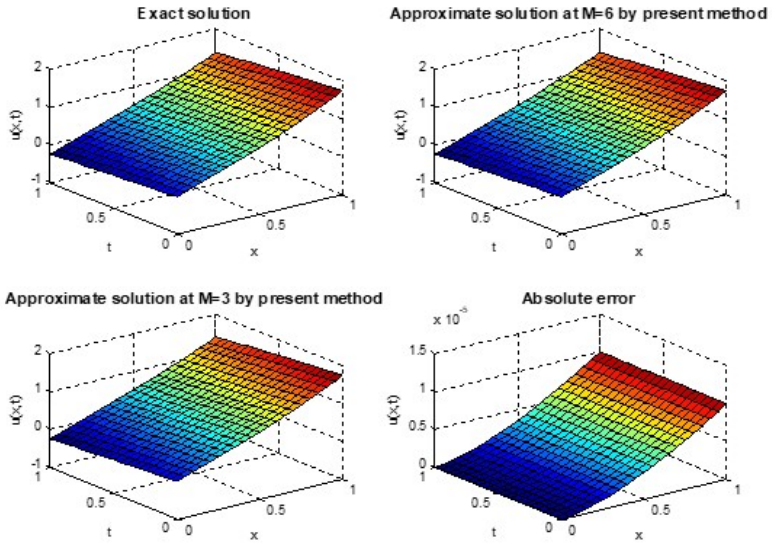

***Figure* 5.1:** *Geometrical comparison of Exact solution and Numerical solution at* $k = 1, \sigma = 1$ *and* $y = 0$ *of example* 5.1.

Table* 5.1: Absolute error of proposed method with exact solution along with literature methods, for example 5.2, at* $y = 1, M = 6, k = 1, \sigma = 1$.

x	t	ETIM	HPTM	VIM	NISTM	Present method
0.0	0.0	2.00e-08	2.00e-08	2.00e-08	2.00e-08	0
	0.01	1.50e-07	1.50e-07	3.99e-06	1.40e-07	1.00e-13
	0.03	3.06e-07	3.06e-07	8.01e-06	3.10e-07	2.70e-12
	0.05	5.55e-07	5.55e-07	1.59e-05	5.55e-07	1.25e-11
	0.07	7.66e-07	7.80e-07	2.24e-05	7.80e-07	3.43e-13
	0.10	8.12e-07	8.11e-07	2.01e-05	8.12e-07	1.00e-13
0.01	0.0	1.40e-07	1.40e-07	3.95e-06	1.14e-07	0
	0.01	3.25e-07	3.01e-07	8.01e-06	3.01e-07	1.00e-12
	0.03	5.53e-07	4.65e-07	9.19e-06	4.65e-07	2.70e-11
	0.05	7.32e-07	6.35e-07	2.05e-05	8.11e-07	1.25e-10
	0.07	8.11e-07	8.11e-07	2.11e-05	8.11e-07	3.43e-10
	0.10	9.98e-07	9.99e-07	2.14e-07	9.98e-07	1.90e-10
0.03	0.0	3.01e-07	3.01e-07	7.90e-07	3.01e-07	0
	0.01	4.75e-07	4.66e-07	1.49e-06	4.66e-07	1.00e-11
	0.03	5.63e-07	6.63e-07	1.89e-06	6.63e-07	2.70e-10
	0.05	8.91e-07	8.11e-07	2.11e-05	7.55e-07	1.25e-09
	0.07	9.40e-06	9.97e-07	2.23e-05	8.11e-06	3.43e-09
	0.10	1.20e-06	2.41e-06	2.94e-05	1.20e-06	2.89e-09
0.05	0.0	4.66e-07	4.66e-07	1.19e-06	4.66e-07	0
	0.01	5.67e-07	6.35e-07	1.34e-06	6.35e-07	1.87e-11
	0.03	7.22e-07	8.12e-07	1.98e-05	8.12e-07	3.58e-10
	0.05	8.98e-07	9.98e-07	2.00e-05	9.98e-07	6.54e-09
	0.07	1.01e-07	1.20e-07	2.41e-05	1.20e-07	9.58e-09
	0.10	1.20e-07	1.41e-07	3.27e-05	1.41e-07	8.24e-09
0.07	0.0	6.35e-07	6.35e-07	1.55e-06	6.35e-07	1.54e-14
	0.01	1.38e-07	7.12e-07	1.89e-06	1.38e-07	5.00e-11
	0.03	7.22e-07	8.34e-07	2.11e-06	7.22e-07	1.35e-09
	0.05	8.98e-07	9.98e-07	8.98e-05	8.98e-07	6.25e-09
	0.07	1.01e-07	1.20e-06	3.52e-05	1.01e-07	1.71e-08
	0.10	1.20e-07	1.56e-06	2.48e-05	1.20e-07	2.54e-11
0.10	0.0	8.12e-07	8.12e-07	2.00e-06	8.12e-07	2.78e-13
	0.01	8.98e-07	9.98e-07	2.21e-06	8.98e-07	2.30e-10
	0.03	7.22e-06	5.22e-06	2.64e-05	7.22e-06	6.21e-09
	0.05	6.35e-06	3.35e-06	3.27e-05	6.35e-06	2.87e-08
	0.07	4.66e-06	2.66e-06	3.77e-05	4.66e-06	7.88e-08
	0.10	1.63e-06	1.88e-06	4.11e-06	1.63e-06	1.35e-08

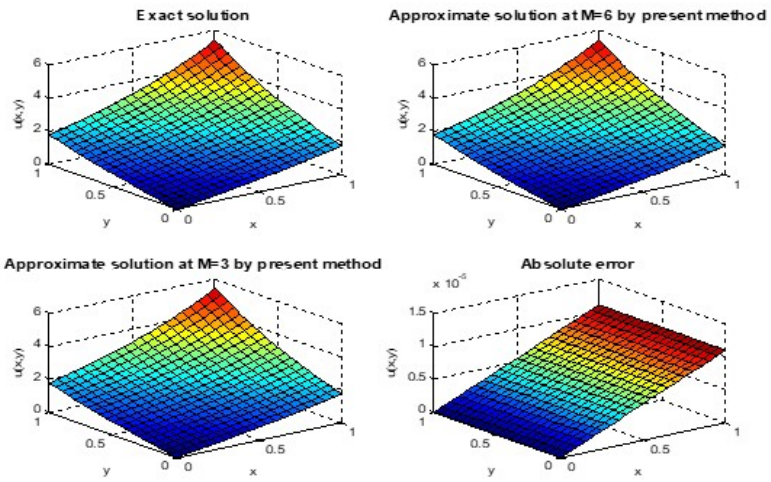

Figure* 5.2: Geometrical comparison of Exact solution and Numerical solution at* $k = 1, \sigma = 1$ *and* $t = 0$ *of example* 5.1.

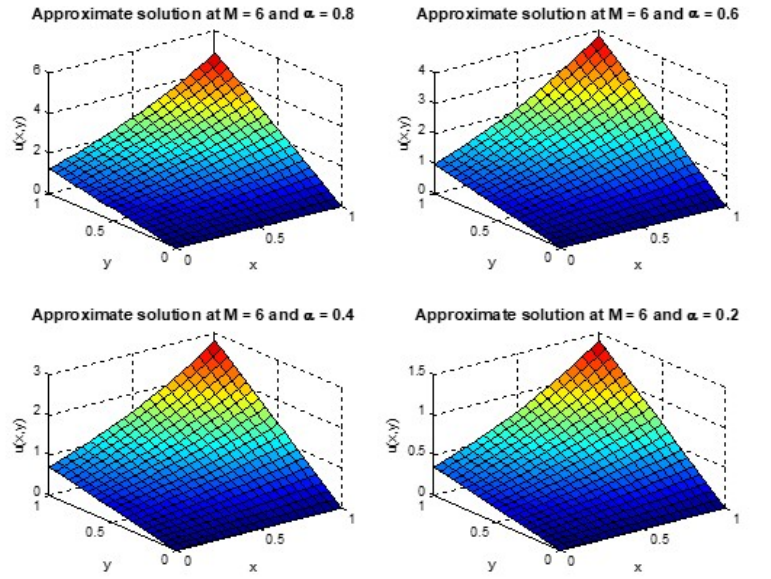

Figure* 5.3: Numerical solution at* $k = 1, \sigma = 1$ *and* $t = 0$ *for example 5.1 for different values of* α.

Example 5.2. Consider time-fractional Zakharov-Kuznetsov equation :

$$D_t^{\alpha} u + (u^2)_x + \frac{1}{8}(u^2)_{xxx} + \frac{1}{8}(u^2)_{xyy} = 0, \qquad 0 < \alpha \leq 1, \tag{5.2}$$

with initial condition

$$u(x, y, 0) = \frac{1}{3}\sigma(e^{(x+y)} - e^{-(x+y)})^2.$$

The exact solution to (5.2) when $\alpha = 1$, is given by $u(x, y, t) = \frac{1}{3}\sigma(e^{(x+y-\sigma t)} - e^{-(x+y-\sigma t)})^2$. Where σ is an arbitrary constant., the above example (5.2) is solved using the proposed method. Table 5.1 represents the Absolute error of the proposed method with exact solution along with literature methods for at $y = 1, M = 6, k = 1, \sigma = 1$. Figures 5.4 and 5.5 represent the Geometrical comparison of the Exact solution and

the Numerical solution at $k = 1, \sigma = 1$ and $t = 0, y = 0$. Figure 5.6 represents the Numerical solution at $k = 1, \sigma = 1$ and $t = 0$ for different values of α.

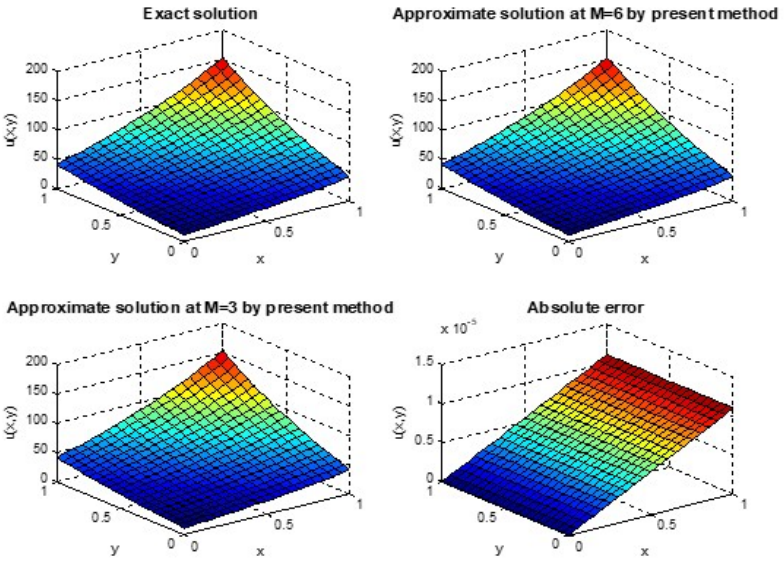

***Figure* 5.4:** *Geometrical comparison of Exact solution and Numerical solution at $k = 1, \sigma = 1$ and $t = 0$ for example 5.2.*

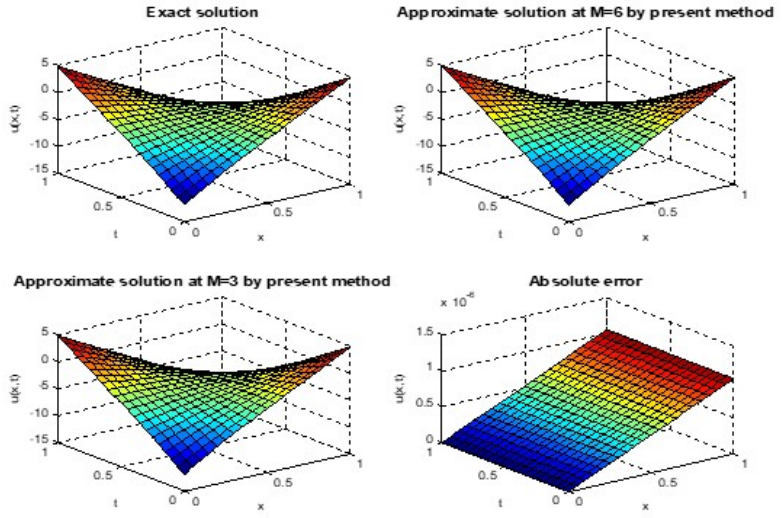

***Figure* 5.5:** *Geometrical comparison of Exact solution and Numerical solution at $k = 1, \sigma = 1$ and $y = 0$ for example 5.2.*

6 Conclusion

In this work, we used a unique technique called the Bernoulli wavelet collocation method ($BWCM$) to investigate the Zakharov-Kuznetsov equation. By leveraging the Bernoulli wavelet's properties, we could transform the mathematical problems into a collection of nonlinear algebraic equations. The mathematical

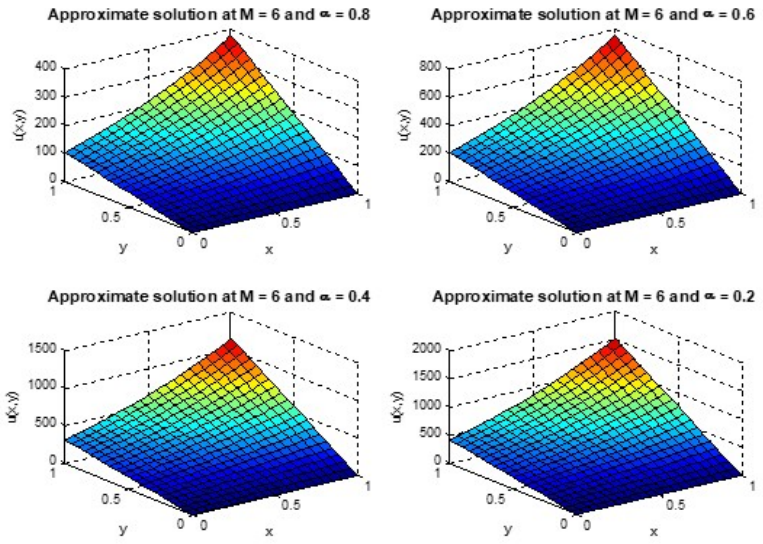

Figure* 5.6: Numerical solution at* $k = 1, \sigma = 1$ *and* $t = 0$*, for example 5.2, for different values of* α*.*

equations (5.1) and (5.2) are solved numerically using the previously described procedure. As Table 5.1 shows, the *BWCM* more closely reflects the nature and solution of the model when compared to other numerical approaches such as *ETIM, VIM, HPTM,* and *NISTM.* The geometric comparison between the exact and numerical solutions at $k = 1, \sigma = 1$, and $t = 0, y = 0$ is displayed in Figures 5.1, 5.2, 5.4, and 5.5. The numerical solution, for example, 5.2 for $k = 1, \sigma = 1$, and $t = 0$, is displayed in Figures 5.3 and 5.6 for various values of α. The results show that the *BWCM* can handle the problem more precisely than other approaches. The Bernoulli wavelet method can further be extended to different *PDEs, FPDEs.*

Acknowledgement. The author expresses their affectionate thanks to the DST-SERB, Govt. of India. New Delhi for the financial support under Empowerment and Equality Opportunities for Excellence in Science for 2023-2026. F.No.EEQ/2022/620 Dated: 07/02/2023.

References

[1] M. A. Abdoon, F. L. Hasan, and N. E. Taha, Computational Technique to Study Analytical Solutions to the Fractional Modified KDVZakharovKuznetsov Equation, *Abstract and Applied Analysis*, Hindawi, **2022** (2022).

[2] L. Akinyemi, M. enol, and S. N. Huseen, Modified homotopy methods for generalized fractional perturbed Zakharov-Kuznetsov equation in dusty plasma, *Advances in Difference Equations*, **2021** (2021), 1-27.

[3] S. A. Balaji, New Bernoulli Wavelet Operational Matrix of Derivative Method for the Solution of Nonlinear Singular Lane-Emden Type Equations Arising in Astrophysics, *ASME. Journal Computional Nonlinear Dynamics*, **11**(5) (2016), 051013.

[4] Y. Cenesiz, O. Tasbozan, and A. Kurt, Functional Variable Method for conformable fractional modified KdV-ZK equation and Maccari system, *Tbilisi Mathematical Journal*, **10**(1) (2017), 117-125.

[5] D. Chouhan, V. Mishra, and H. M. Srivastava, Bernoulli wavelet method for the numerical solution of anomalous infiltration and diffusion modeling by nonlinear fractional differential equations of variable order, *Results in Applied Mathematics*, **10** (2021), 100-146.

[6] D. Chouhan, and R. S. Chandel, Numerical Solution of the Convection Diffusion Equation by the Legendre Wavelet Method, *The Vijnana Parishad of India*, **26** (2019).

[7] MO. Faheem, R. Akmal, K. Arshad, Collocation methods based on Gegenbauer and Bernoulli wavelets for solving neutral delay differential equations, *Mathematics and Computers in Simulation*, **180** (2021), 72-92.

[8] O. Guner, E. Aksoy, A. Bekir, and A. C. Cevikel, Various methods for solving time fractional KdV-Zakharov-Kuznetsov equation, *International Conference of Numerical Analysis and Applied Mathematics*, **1738** AIP Publishing LLC., (2016).

[9] G. Hariharan, R. Rajaraman, A new coupled wavelet-based method applied to the nonlinear reaction-diffusion equation arising in mathematical chemistry, *Journal of Mathematical Chemistry*, **51**(9) (2013), 2386-2400.

[10] D. Kumar, J. Singh, and S. Kumar, Numerical computation of nonlinear fractional Zakharov-Kuznetsov equation arising in ion-acoustic waves, *Journal of the Egyptian Mathematical Society*, **22**(3) (2014), 373-378.

[11] E. Keshavarz, Y. Ordokhani, M. Razzaghi, Bernoulli wavelet operational matrix of fractional order integration and its applications in solving the fractional-order differential equations, *Applied Mathematical Modeling*, **38** (2014), 6038-6051.

[12] S. Kumbinarasaiah S, and K. R. Raghunatha, Numerical solution of the Jeffery-Hamel flow through the wavelet technique, *Heat Transfer*, **51** (2022), 1568- 1584.

[13] S. Kumbinarasaiah, A novel approach for multi-dimensional fractional coupled Navier-Stokes equation, *SeMA*, **80** (2022), 261-282.

[14] S. Kumbinarasaiah, and R. Yeshwanth, Haar wavelet approach to study the control of biological pest model in Tea plants, *Journal of Fractional Calculus and Nonlinear Systems*, **4** (2023), 14-30.

[15] S. Kumbinarasaiah, and M. P. Preetham, Applications of the Bernoulli wavelet collocation method in the analysis of MHD boundary layer flow of a viscous fluid, *Journal of Umm Al-Qura University for Applied Sciences*, **9** (2023), 1-14.

[16] S. Kumbinarasaiah, and M. Mulimani, Bernoulli Wavelets Numerical Approach for the Nonlinear Klein-Gordon and Benjamin-Bona-Mahony Equation, *International Journal of Applied and Computational Mathematics*, **9**(5) (2023).

[17] S. Kumbinarasaiah, and R. Yeshwanth, A study on Chlamydia transmission in United States through the Haar wavelet technique, *Results in Control and Optimization*, **14** (2024).

[18] S. Kumbinarasaiah, and M. Mulimani, A study on the non-linear Murray equation through the Bernoulli wavelet approach, *International Journal of Applied and Computational Mathematics*, **9**(3) (2023).

[19] D. Lu, M. Suleman, J. Ul Rahman, S. Noeiaghdam, and G. Murtaza, Numerical simulation of fractional Zakharov-Kuznetsov equation for description of temporal discontinuity using projected differential transform method, *Complexity*, **2021**(1) (2021), 1-11.

[20] W. W. Mohammed, F. M. Al-Askar, C. Cesarano, and M. El-Morshedy, Solitary Wave Solutions of the Fractional-Stochastic Quantum Zakharov-Kuznetsov Equation Arises in Quantum Magneto Plasma, *Mathematics*, **11**(2) (2023).

[21] G. Manohara, and S. Kumbinarasaiah, Fibonacci wavelet collocation method for the numerical approximation of fractional order Brusselator chemical model, *Journal of Mathematical Chemistry*, **62** (2023), 2651-2681.

[22] M. Mulimani, and S. Kumbinarasaiah, A novel approach for Benjamin-Bona-Mahony equation via ultraspherical wavelets collocation method, *International Journal of Mathematics and Computer in Engineering*, **2**(2) (2024).

[23] M. Mulimani, and S. Kumbinarasaiah, A numerical study on the nonlinear fractional Klein-Gordon equation, *Journal of Umm Al-Qura University for Applied Sciences*, **10**(1) (2024), 178-199.

[24] G. Manohara, and S. Kumbinarasaiah, Numerical approximation of fractional SEIR epidemic model of measles and smoking model by using Fibonacci wavelets operational matrix approach, *Mathematics and Computers in Simulation*, **221** (2024), 358-396.

[25] S. Raut, S. Roy, R. R. Kairi, and P. Chatterjee, Approximate analytical solutions of generalized Zakharov-Kuznetsov and generalized modified Zakharov-Kuznetsov equations, *International Journal of Applied and Computational Mathematics*, **7** (2021), 1-25.

[26] P. Rahimkhani, and Y. Ordokhani, A numerical scheme based on Bernoulli wavelets and collocation method for solving fractional partial differential equations with Dirichlet boundary conditions, *Numerical Methods Partial Differential Equations*, **35** (2019), 34- 59.

[27] P. Rahimkhani, Y. Ordokhani, E. Babolian, A new operational matrix based on Bernoulli wavelets for solving fractional delay differential equations, *Numerical Algorithms*, **74** (2017), 223-245.

[28] K. S. Rathore, and M. Goyal, Numerical Solution of Magnetohydrodynamic(MHD) Radiative Boundary Layer Flow and heat Transfer along a Wedge in the Presence of Suction Injection, *The Vijnana Parishad of India*, **279** (2020).

[29] K. R. Raghunatha, S. Kumbinarasaiah, Application of Hermite Wavelet Method and Differential Transformation Method for Nonlinear Temperature Distribution in a Rectangular Moving Porous Fin, *International Journal Applied Computational Mathematics*, **8** (2022).

[30] P. P. Sartanpara, and R. Meher, A robust computational approach for Zakharov-Kuznetsov equations of ion-acoustic waves in a magnetized plasma via the Shehu transform, *Journal of Ocean Engineering and Science*, **8**(1) (2023), 79-90.

[31] I. Singh, and M. Kaur, Comparative study of wavelet methods for solving Bernoullis equation, *Jnanabha*, **50**(2) (2020), 106-113.

[32] P. Sunthrayuth, F. Ali, A. A.Alderremy, R. Shah, S. Aly, Y. S. Hamed, and J. Katle, The numerical investigation of fractional-order Zakharov-Kuznetsov equations, *Complexity*, **2021**(1) (2021), 1-13.

[33] R. Shah, H. Khan, D. Baleanu, P. Kumam, and M. Arif, A novel method for the analytical solution of fractional Zakharov-Kuznetsov equations, *Advances in difference equations*, **2019** (2019), 1-14.

[34] P. K. Sahu, S. Saha Ray, A New Bernoulli Wavelet Method for Numerical Solutions of Nonlinear Weakly Singular Volterra Integro-Differential Equations, *International Journal of Computational Methods*, **14**(03) (2017).

[35] S. Kumbinarasaiah, H. Rezazadeh, W. Adel, An effective numerical simulation for solving a class of Fokker-Planck equations using Laguerre wavelet method, *Mathematical Methods in Applied Sciences*, **45**(11) (2022), 6824-6843.

[36] P. Veeresha, and D. G. Prakasha, Solution for fractional Zakharov-Kuznetsov equations by using two reliable techniques, *Chinese Journal of Physics*, **60** (2019), 313-330.

[37] M. S. Vivek, and M. Kumar, Taylor wavelet approach for the solution of the Fredholm integro-differential equation of the second kind, *Jñānābha*, **53**(2) (2023), 273-286.

[38] S. Yasin, A. Khan, S. Ahmad, and M. S. Osman, New exact solutions of (3+ 1)-dimensional modified KdV-Zakharov-Kuznetsov equation by Sardar-subequation method, *Optical and Quantum Electronics*, **56**(1) (2024).

[39] Yan, L., Kumbinarasaiah, S., Manohara, G., Baskonus, H. M., & Cattani, C. Numerical solution of fractional PDEs through wavelet approach. Zeitschrift für angewandte Mathematik und Physik, 75(2) (2024), 61.

ISSN 0304-9892 (Print) ISSN 2455-7463 (Online)
www.vijnanaparishadofindia.org/jnanabha
***Jñānābha* Vol. 55 (I) Special Issue 2025, 53-63**
Proceedings: 5th International Conference and Golden Jubilee Celebrations of VPI (IC-RA-MSA-ET 2022) JNU, New Delhi, India

FUZZY LOGIC: FUNDAMENTALS AND APPLICATIONS

Sakshi Gupta[1], Shelly Garg[2] and Gajendra Pratap Singh[3]
[1]Department of Applied Sciences and Humanities, Dronacharya College of Engineering, Gurugram, Haryana, India-122506
[2]Department of Computer Science, Amity University Haryana, India-122413
[3]School of Computational and Integrative Sciences, Jawaharlal Nehru University, New Delhi, India-110067
Email: [1] sakshi86.10@gmail.com, [2] shellygarg96@gmail.com, [3] gajendra@jnu.ac.in
(Received: October 09, 2023; In format: December 09, 2024; Revised: June 09, 2025; Accepted: June 20, 2025)

DOI: https://doi.org/10.58250/jnanabha_SI.2025.55107

Abstract

Fuzzy logic is an applied branch of Mathematics having numerous applications across diverse fields. This paper presents an introduction to the fundamentals of fuzzy logic and explores its various applications in real life. The concept of fuzzy logic is based on human thinking and natural behaviour. This theory replicates human psychology in terms of how people make decisions quickly and with imprecise information. Unlike traditional binary logic, which only uses two values-0 (for false) and 1 (for true), fuzzy logic describes human reasoning by using the entire range between 0 and 1 . It interacts with incoming data in a more human-like manner, using an imprecise yet highly descriptive language. It can be implemented through hardware, software, or a combination of both. As a bridge between human thought and computational systems, fuzzy logic improves communications and understanding between humans and machines. Its flexibility and performance have made it among the preferred solutions for numerous control system applications.

2020 Mathematical Sciences Classification: 03B52, 03E72.
Keywords and Phrases: Fuzzy Logic, Fuzzy Theory, Fuzzy logic Applications, Fuzzy Petri Net

1 Introduction

Fuzzy logic was first proposed by the Professor Lotfi A. Zadeh at the University of California, Berkeley, United States in 1965 to model the vagueness and uncertainty inherent in many realworld problems. Unlike classical binary logic, which demands exact truth values (0 or 1), fuzzy logic allows variables to have a degree of truth ranging between 0 and 1 . This feature makes fuzzy logic especially useful in situations where data is imprecise or lacks distinct limits. Fuzzy logic allows us to turn verbal words like sweet, cold, warm, and honest etc. into mathematical models. This makes it possible for machines and systems to interpret and act on ambiguous inputs in a human-like manner.

The history of fuzzy logic can be traced back to the publication of Zadeh's original paper on "Fuzzy Sets," the ideas of which gave birth to fuzzy set theory [36]. It was initially met with scepticism from some in the academy, and acceptance for fuzzy logic theory was not rapid until newer computing systems became widely available which could process fuzzy data. Interest continued to increase in the 1970s and 1980s when researchers, scientists, and engineers began applying fuzzy
logic to control systems and associated decision problems. By the 1990s, fuzzy logic concepts had proven commercially viable, primarily in consumer items produced in Japan and later in Europe.

Fuzzy logic has become an important aspect of computational intelligence today and finds widespread use in control systems, artificial intelligence, pattern recognition, and decision-making frameworks. Its ability to simulate human reasoning and linguistic control increases applicability to a range of modern technologies. Fuzzy logic is capable of facilitating the comprehension of imprecise and qualitative notions, which has found applications in expert systems, adaptive learning, and intelligent automation.

The relevant developments from 2017 to today highlight that fuzzy logic is not only feasible but necessary for applications that require explainability, human-centered design, and uncertainty management. For instance, fuzzy logic systems have been implemented in health care as early diagnosis systems for diseases like

diabetes, cardiovascular diseases, and now *COVID*-19, where the symptoms are non-precise and overlapping [18, 26]. In these cases, fuzzy systems help clinicians make plausible evaluations when the information is incomplete and ambiguous by referring to fuzzy inference models built from clinical data. Similarly, fuzzy rule-based systems are being implemented into smart healthcare devices to assess vitals, generate alerts, or provide interventions in a human-centered design way [37]. Fuzzy logic is also experiencing renewed integration inside physical and engineering systems, especially in Industry 4.0 frameworks. For example, it is being integrated with *IoT* (internet of things), big data analytics, and deep learning to enable enhanced automated decision making and adaptive control for manufacturing, logistics, and energy management [16, 30]. Hybrid fuzzy-deep learning models have been proposed to circumvent the issues posed in nonlinear system control design, where crisp rules on their own would not generalize against uncertainty

In robotics and autonomous vehicles, fuzzy logic has been applied to improve perception, navigation, and motion control, especially in uncertain and dynamic environments [6]. Additionally, researchers have created advanced fuzzy logic systems in conjunction with formal methods such as Petri nets to enhance modeling of uncertain, concurrent, and distributed systems. These models are well-suited for use in intelligent decision support, smart grids, and cybersecurity [31, 32]. Petri nets and its different types [19, 28] have been used to study the different system networks such as biological networks [11,12], studying the drug targets [9, 10, 13, 27], decision making [17] and knowledge-based systems to name a few. Fuzzy Petri nets [14] and fuzzy optimization algorithms are currently being implemented in the context of cloud computing and workflow management to help mitigate the impact of uncertain workloads on performance, latency, and resource allocation [24].

Subsequently, due to its transparent processes for reasoning and decision-making, fuzzy logic is increasingly relevant in an era of Artificial Intelligence *(AI)* ethics and interpretability, particularly in regulated fields including finance, defense, and healthcare. Unlike black-box models, fuzzy systems enable stakeholders to retrieve and comprehend the reasoning behind systems decisions: a characteristic that parallels the specially emphasis of explainable *AI* [23]. As we move into an era of intelligent and autonomous systems, the prospects of fuzzy logic are truly bright.

Its unique ability to bridge symbolic reasoning with numerical modelling positions it as a foundational tool in next-generation AI applications. The current trajectory of research continues
to explore its integration with neural networks, genetic algorithms, and deep reinforcement learning, pushing the boundaries of what intelligent systems can achieve under uncertainty.

2 Basic Terminology

The concept of fuzzy sets was introduced by Lotfi A. Zadeh in 1965 [36]. The classical notion of crisp sets was further extended as fuzzy sets. Fuzzy sets are the collection of elements where each element has a degree of membership. The membership degree from zero to one is allocated to each set of objects. Fuzzy sets have vague or overlapping boundaries, while crisp sets have clearly defined boundaries (Figure 2.1).

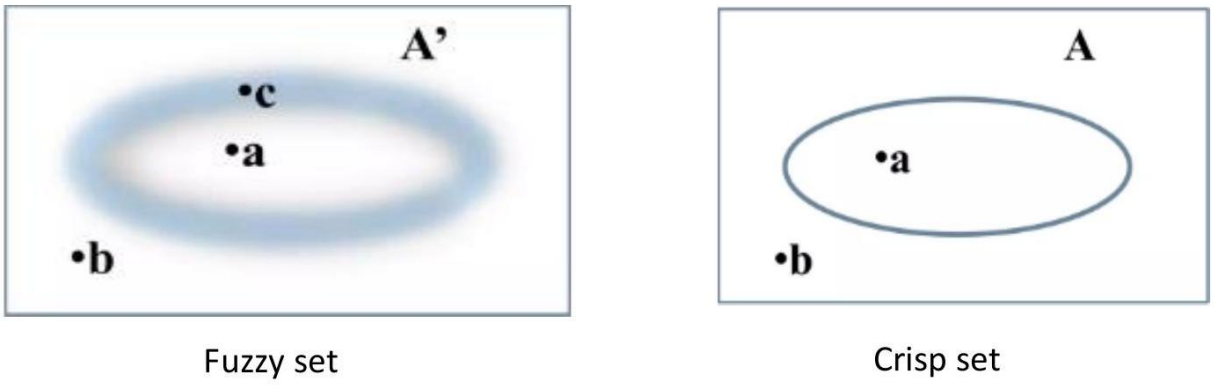

Figure* 2.1: Representation of Fuzzy set and Crisp set*

Definition 2.1. *Fuzzy set: A fuzzy set A in the universe of discourse U can be defined as a collection of*

ordered pairs and is mathematically represented as:

$$A = \{(y, \mu_A(y) \mid y \in U\}$$

where, $\mu_A(y)$ *denotes the membership function of the element* y *in the fuzzy set* A *.*

Definition 2.2. *Membership function: A membership function for a fuzzy set* A *on the universe of discourse* U *is defined as:*

$$\mu_A : U \to [0, 1]$$

Here, every element of U *is assigned a value between 0 and 1 , known as the degree of membership or membership value of the corresponding element in* A*. For* $y \in U$*,*

$$\begin{aligned} \mu_A(y) = 0 \quad &\Rightarrow \quad y \text{ does not belong to A.} \\ \mu_A(y) = 1 \quad &\Rightarrow \quad y \text{ fully belongs to A.} \\ 0 < \mu_A(y) < 1 \quad &\Rightarrow \quad y \text{ partially belongs to A.} \end{aligned}$$

Types of Membership function: There are three commonly used fuzzy membership functions:
a. Triangular membership function: It is described by a triangular shape, defined by three parameters a, b *and* c *with peak at the point* b *(Figure 2.2). It is defined as:*

$$\mu_A(x) = \left\{ \begin{array}{cc} 0 & if\ x \leq a \\ \frac{x-a}{b-a} & if\ a \leq x \leq b \\ \frac{c-x}{c-b} & if\ b \leq x \leq c \\ 0 & if\ x \geq c \end{array} \right\}$$

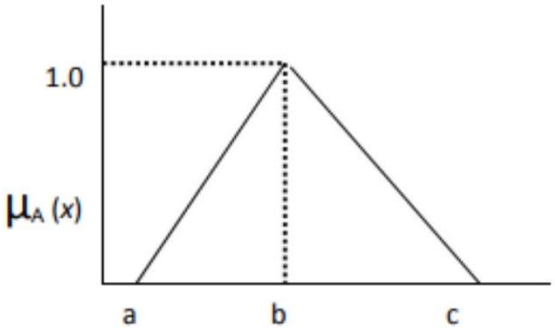

Figure* 2.2: Triangular membership function*

b. Trapezoidal membership function: It is characterized by Trapezoid shape, defined by four parameters a, b, c *and* d *(Figure 2.3). It reduces to Triangular membership function when* b = c*. It is defined as:*

$$\mu_A(x) = \left\{ \begin{array}{cc} 0 & if\ x \leq a \\ \frac{x-a}{b-a} & if\ a \leq x \leq b \\ 1 & if\ b \leq x \leq c \\ \frac{d-x}{d-c} & if\ c \leq x \leq d \\ 0 & if\ x \geq d \end{array} \right\}$$

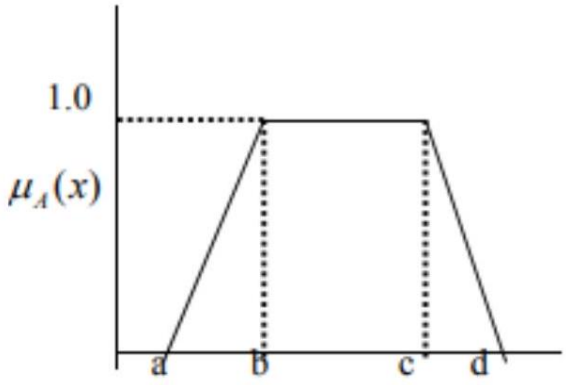

Figure* 2.3*: *Trapezoidal membership function*

c. Gaussian membership function: It is a smooth bell shaped curve, suitable for noisy inputs (Figure 2.4). This function is characterized by mean and standard deviation. It is defined as:

$$\mu(x;\sigma,c) = e^{-\frac{(x-c)^2}{2\sigma^2}}$$

Here, c is the mean and σ is the standard deviation of the Gaussian function.

Features of Membership function: The membership function has the following three features, which are shown in Figure 2.5. Let $\tilde{A}$ be the fuzzy set and $x \in U$, where U is the universe of information.
i). Core: It consists of all those elements x such that $\mu_{\tilde{A}}(x) = 1$. The core of a fuzzy set may be an empty set.

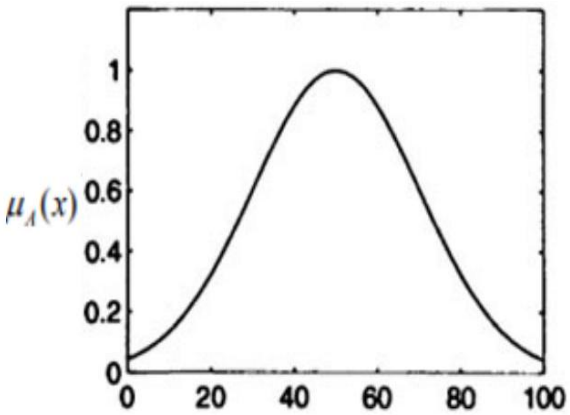

Figure* 2.4*: *Guassian membership function*

ii). Support: It consists of all those elements x such that $\mu_{\tilde{A}}(x) > 0$.
iii). Boundary: It consists of all those elements x such that $0 < \mu_{\tilde{A}}(x) < 1$. The boundary elements indicate partial membership in the fuzzy set.

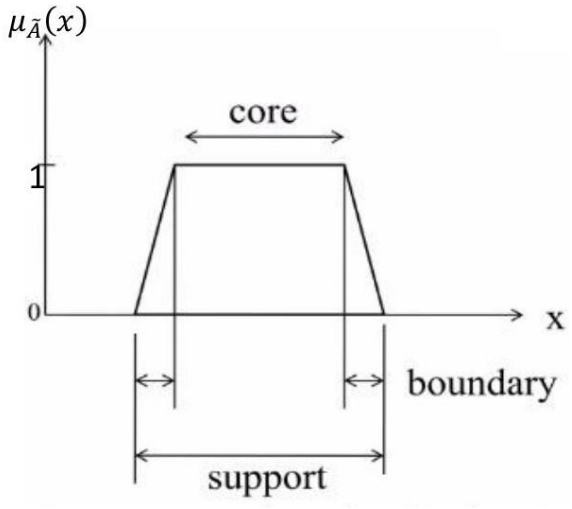

Figure* 2.5*: *Features of membership function*

3 Fuzzy Logic system Architecture

A fuzzy logic architecture consists of four key components that work together to process inputs, apply human-like reasoning, and produce actionable outputs (Figure 3.1).

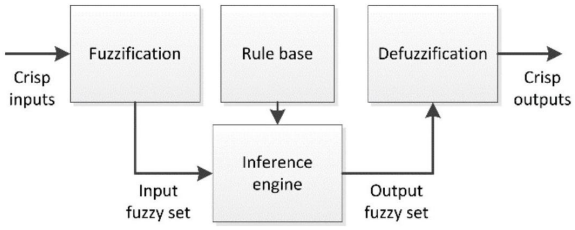

Figure* 3.1*: *Architecture of fuzzy logic system*

i) Fuzzification: Fuzzification is the process of turning a crisp value into a fuzzy value. Fuzzification converts crisp inputs-precise values measured by sensors, such as temperature or pressure-into fuzzy values using membership functions. These fuzzy values represent degrees of membership in different categories (e.g., "cold," "warm," or "hot"), enabling the system to handle imprecision effectively.

ii) Rule base: Human knowledge can be represented using the following natural language structure "IF antecedent THEN consequent".
This structure is stated as the fuzzy "IF-THEN rules". The rule-base and the membership functions are provided by experts. These rules govern the decision-making process by translating linguistic inputs into actionable outputs. Advances in fuzzy logic design have streamlined the development and tuning of fuzzy controllers, often reducing the number of rules required for effective operation.

iii) Inference engine: The inference engine mimics human reasoning by evaluating the matching degree between fuzzy inputs and the rules stored in the rule-base. Based on this evaluation, it determines which rules to activate and combines their outcomes to form control actions. This process is the core of decision-making in a fuzzy logic system.

iv) Defuzzification: Defuzzification converts the fuzzy output produced by the inference engine into a precise, crisp value. This step translates the fuzzy control actions into precise, actionable outputs suitable for real-world applications. Several defuzzification techniques exist, and the choice of method depends on the specific system requirements.

By integrating fuzzification, a robust knowledge base, an inference engine, and defuzzification, the architecture of a fuzzy logic provides a powerful framework for managing uncertainty and complexity in decision-making processes.

4 Applications of Fuzzy Logic

Due to its ability to handle ambiguity, approximate reasoning, and imprecise information, fuzzy logic has been widely used in various fields. Fuzzy logic can resemble human decision-making capabilities in situations where 'yes' and 'no' systems lack trait for uniqueness or adaptability.

i) **Control Systems:** Fuzzy logic has become a most valuable analysis tool in some modern control systems, especially in situations where the systems exhibit non-linear or complex behavior, or whereby precise representation and modeling of system uncertainty is not attainable. Handling ambiguous and approximate reasoning have made fuzzy logic an especially useful approach for those environments which require intelligent decision making or adaptation. Recently, several studies demonstrate increased use of fuzzy logic for control systems of Heating, Ventilation and Air Conditioning *(HVAC)* systems, smart infrastructure and home appliances, where traditional control approach may lack precision in outcome. Li *et al.* [21], developed a fuzzy *PID* (Proportional-Integral-Derivative) controller for temperature control applications, where the authors have demonstrated improved stability and control overshoot using dynamic load. For energy-initiated buildings may rely solely on a fuzzy controller for lighting and *HVAC* management, in which the fuzzy controller produces real time occupant behavioral outputs and environmental information to maintain client comfort during energy reduction and conservation initiatives [1].

ii) **Robotics:** Fuzzy logic applications will also require integration to permit robotic operations in unknown and unpredictable environments of the real-world. With the rise of autonomous navigation, fuzzy controllers have been utilized in mobile robots for obstacle avoidance, path planning, and human interaction. Recent work by Arun *et al.* [2] introduced a fuzzy-based behavior arbitration mechanism that dynamically adjusts a robot's movement based on sensor inputs in uncertain terrains. Furthermore, in social robotics, fuzzy logic supports emotional recognition and human-robot interaction by interpreting vague cues like tone of voice, body posture, and facial expressions [33]. These capabilities are essential in service-oriented robots for healthcare, education, and domestic assistance.

iii) **Medical Diagnosis and Healthcare:** In the healthcare sector, fuzzy logic has proven invaluable for clinical decision-making, especially where diagnostic inputs are imprecise or subjective. Medical conditions frequently involve overlapping symptoms combined with incomplete patient histories that challenge alternative approaches based on typical binary or rule-based systems. Fuzzy logic systems can accommodate symptoms and/or lab results expressed in degrees of certainty about the client's possible health status. An example of this would be a fuzzy expert system for early cancer diagnosis, where symptom severity and lab results were presented to infer the probability of disease [3]. Similarly, fuzzy logic has been used in chronic disease management (e.g., diabetes and hypertension) of assessing risk based on various variables such as *BMI*, blood glucose, and blood pressure [38]. Furthermore, hybrid systems using neural networks or support vector machines can be combined with fuzzy logic to improve both diagnostic accuracy and explainability, providing better decision support for clinicians who are consistently making decisions in treatment with incomplete or imprecise data.

iv) **Machine Learning and Artificial Intelligence:** The development of machine learning incorporating fuzzy logic is relatively recent, but it is receiving many more meaningful approaches because of uncertainty management and interpretation benefits offered by fuzzy logic in complex systems. For example, Charizanos *et al.* [5] explored the use of fuzzy logic in Deep Symbolic Regression to boost performance and explainability in credit card fraud detection, and they demonstrated that using specific fuzzy implications, like ukasiewicz, improved $F1$-scores and accuracy. Singh *et al.* [29], used machine learning to propose a diagnostic system based on fuzzy logic for hepatitis B, to cope with the uncertainties in medical data. Gordan *et al.* [8] made a similar suggestion by integrating fuzzy logic and machine learning approaches, such as *PCA* and *SVM*, to improve disease risk assessment. Their approach resulted in better diagnostic performance over many health care datasets. These studies illustrate the trend of employing fuzzy logic embedded in machine learning frameworks to mitigate uncertainties and explainability concerns across a wide variety of application settings.

v) **Industrial Automation:** Fuzzy logic has been implemented extensively in today's industrial automation, because it allows for engineering flexibility of control systems to work in environments with nonlinearity, time delays, and stochastic behavior. For example, Fatima *et al.* [7] used fuzzy control to improve safety and efficiency of distillation columns in oil refineries. In smart manufacturing, fuzzy-based quality control systems are being used to designate defects and abnormalities in production lines,

where traditional threshold-based systems would not be able to operate because of various issues on the production floor such as noise or sensor drift [25]. These fuzzy logic models are triggered as part of a learning systems that interacts with *IoT* based data and edge computing systems to facilitate real time decisions in operating and diagnosing weak and failing parts of the production line. Fuzzy has also been incorporated into logical inspired quality control systems for pattern matching and defect detection where a physical product may vary in appearance or take measurements that will prevent a traditional rule-based system from functioning. In general, fuzzy logic applied in the industrial domain leads to improvements in operational efficiency, reductions in downtime and improvements in system resilience.

vi) **Agriculture and Environmental Management:** Precision agriculture and sustainability programs across environmental management and agro-ecology have invested in fuzzy logic because of the ability to investigate and interpret environmental data that is variable and sometimes uncertain. From an agricultural automation perspective, fuzzy logic systems have increased interest in the irrigation space for managing and controlling irrigation based on soil moisture levels, crop types and weather conditions to improve quality and water management [20]. Fuzzy logic decision making systems and tools have also been deployed for forecasting pest outbreaks based on fuzzy inputs such as humidity, temperature, and growth stage. In environmental monitoring, fuzzy logic is used as part of air or water quality evaluations through the use of various sensors and by converting the measurements into meaningful information [15]. This has implications for resource efficiency and sustainable use of the ecosystem and its sustainable development.

vii) **Automotive systems:** Fuzzy logic is an important element in intelligent automotive systems that enhance vehicle performance, and safety. Fuzzy logic is used in most automatic transmission systems to determine the most efficient gear change based on preferences from various inputs such as throttle position, engine load, vehicle speed and driving conditions. Yao *et al.* [34] found that the fuzzy controllers were able to substantially reduce decision latency, while also improving vehicle stability and comfort during semi-autonomous driving. For electric vehicles *(EV)*, fuzzy logic is implemented to maximize battery usage and energy regeneration during brake (expanding driving range and electronic efficiency). Fuzzy systems are also used in applications regarding driver's behavior to modify the vehicle's dynamic response based on individual driver preferences and behavior, wherever possible, to facilitate comfort and safety [35]. Fuzzy logic has been applied in anti-lock braking systems *(ABS)*, where the fuzzy logic is able to always assess wheel rotational speed, increase road traction, and adjust brake pressure so that the treatment results in an optimum brake force while preventing wheel lock during an emergency stop. Additionally, fuzzy logic is integral to adaptive cruise control and lane-keeping assistance because it enables acceleration and steering decisions based on distance to other vehicles, curvature of the road, and documents of the driver's intent. These examples illustrate how fuzzy logic can address safety-critical choices amidst uncertain and dynamic conditions, which is a prerequisite for the development of autonomous vehicles and semi-autonomous vehicles.

5 Case Study - Fuzzy Petri net

A fuzzy Petri net is the integration of fuzzy logic with Petri net to model and study a system dynamically with uncertain or ambiguous data. It is defined as [4]:

Definition 5.1. *Fuzzy Petri net is an 8-tuple:* $FPN = (P, T, Q, I, O, f, \alpha, \beta)$*; where* P *stands for non empty finite set of places,* T *stands for non empty finite set of transitions, and* Q *stands for non-empty finite set of propositions,* $P \cap T \cap Q = \varnothing, |P| = |Q|$*,* I *and* O *stands for input and output functions, both mapping transitions to the places,* $f : T \to [0, 1]$ *is an association function that links every transition to a certainty factor represented by a value between 0 and* $1, \alpha : P \to [0, 1]$ *is an association function that represents the degree of truth of every place,* $\beta : P \to Q$ *is an association function that maps every place to a corresponding proposition.*

In a fuzzy Petri net, a transition t *is enabled if* $\forall p_j \in I(t), \alpha(p_j) \geq \lambda$*, where* λ *is the given threshold value and* $0 \leq \lambda \leq 1$*. Then the reasoning process in a fuzzy Petri net is carried out with the firing of Fuzzy Production propositions and at every step, the truth value of the output place is updated.*

Definition 5.2. *A Fuzzy Production proposition or FPP describes a fuzzy relationship among the propositions. It is typically represented using a fuzzy 'IF-THEN' statement, where the portion following*

"IF" serves as the antecedent or precondition, and the portion following "THEN" represents the consequent or postcondition.

The i th FPP, FP_i is defined as: FP_i : IF q_j THEN $q_k\,(\mu_i = a)$ (Gupta S 2019 Fuzzy). Here,

- *q_j and q_k are the propositions representing the places $p_j \& p_k$, i.e. $\beta(p_j) = q_j \& \beta(p_k) = q_k$;*
- *$\mu_i (0 \le a \le 1; 1 \le i \le n)$ is the certainty factor of the transition t and expresses the strength of belief corresponding to the proposition, i.e. $f(t) = \mu_i$.*

If truth degree of proposition q_j is γ_j i.e. $\alpha(p_j) = \gamma_j, \beta(p_j) = q_j$ and $\gamma_j \ge \lambda$, then after the firing of FP_i, new truth degree of q_k will be $\gamma_k = \gamma_j * \mu_i$.

Types of fuzzy production propostions: There are four most common types of FPPs discussed as follows [4, 22]:

Type 1: IF q_j THEN $q_k\,(\mu_i = a)$ (Figure 5.1).

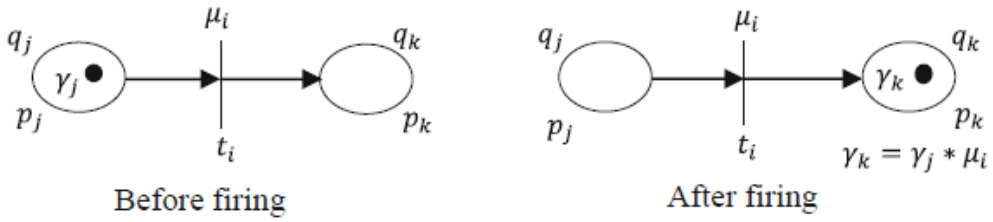

***Figure* 5.1:** *Fuzzy Petri net of Type 1 FPP [14]*

Type 2: IF q_{j1} and q_{j2} and q_{j3} and ... and q_{jn} THEN $q_k\,(\mu_i = a)$ (Figure 5.2).

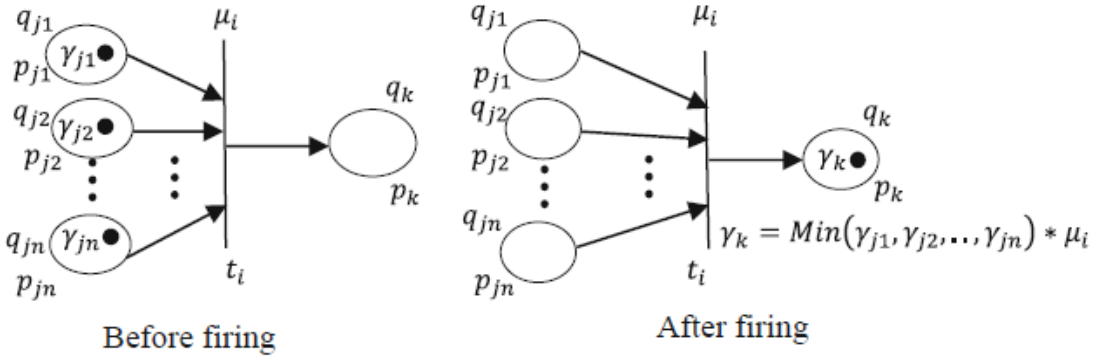

***Figure* 5.2:** *Fuzzy Petri net of Type 2 FPP* [14]

Type 3: IF q_j THEN q_{k1} and q_{k2} and ... and $q_{kn}\,(\mu_i = a)$ (Figure 5.3).

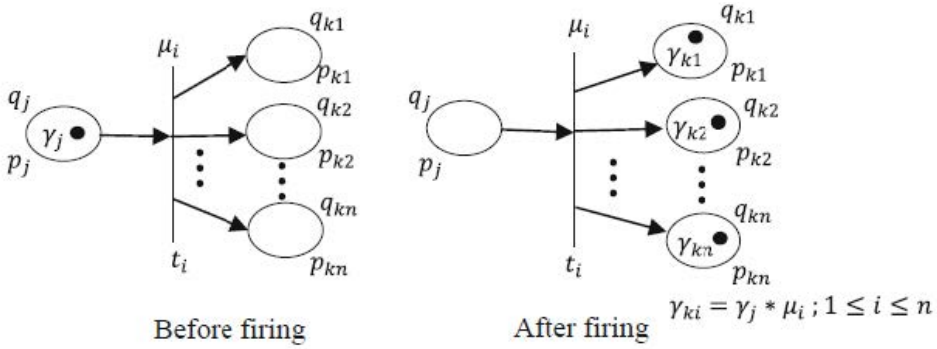

***Figure* 5.3:** *Fuzzy Petri net of Type 3 FPP* [14]

Type 4: IF q_{j1} or q_{j2} or ... or q_{jn} THEN $q_k\,(\mu_i = a)$ (Figure 5.4).

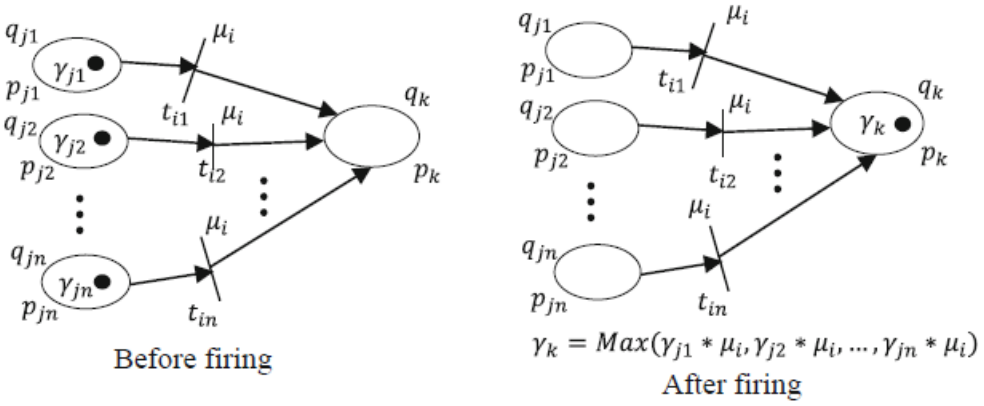

***Figure* 5.4:** *Fuzzy Petri net of Type 4 FPP* [14]

Example 5.1. Let us consider the example of health monitoring:

FPP : IF the heart rate is very high, THEN there is immediate urgency of medical alert ($\mu_1 = 0.90$). Let q_1 "the heart rate is very high" and q_2 "there is immediate urgency of medical alert" be the two propositions of given FPP. These will be represented by the two places p_1 and p_2. Consider the threshold value as $\lambda = 0.40$ and let the truth degree of q_1 is 0.70 , i.e. $\alpha\,(p_1) = \gamma_1 = 0.70$. The FPN model of the FPP is shown in Figure 5.5.

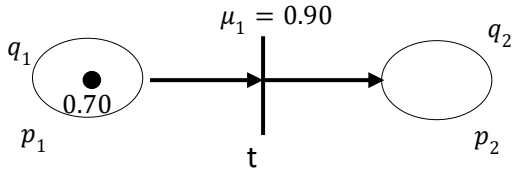

***Figure* 5.5:** *Fuzzy Petri net of FPP*

In the above FPN, $P = \{p_1, p_2\}, T = \{t\}, Q = \{q_1, q_2\}, I\,\{t_1\} = p_1, O\,\{t_1\} = \{p_2\}, f\,(t_1) = \mu_1 = 0.90, \alpha\,(p_1) = 0.70, \alpha\,(p_2) = 0, \beta\,(p_1) = q_1, \beta\,(p_2) = q_2$. Since $\gamma_1 \geq \lambda$, so after the firing of the FPP, $\gamma_2 = \gamma_1 * \mu_1 = 0.63$. From this, we can infer that the degree of possibility of the immediate urgency is 0.63 . The firing of the fuzzy Petri net is shown as below in the Figure 5.6:

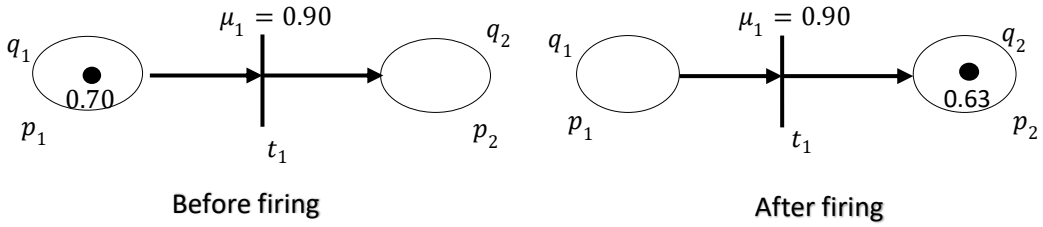

***Figure* 5.6:** *Firing of the FPP*

6 Future Scope

Fuzzy logic has a very positive future scope and continues to develop alongside advances in artificial intelligence, machine learning, and data-driven technologies. Fuzzy logic's ability to model uncertainty and imprecise information, while emulating human reasoning and perception in their decision making,

offers a meaningful framework for next-generation intelligent systems. Over the next decade, fuzzy logic will help advance research aimed at developing autonomous vehicles, smart cities, personalized healthcare, and adaptive industrial automation. This will allow fuzzy logic to integrate with *IoT*, edge computing, deep learning, and other emerging technologies which will enhance fuzzy logic's applicability, enabling more timely, relevant, and reliable decision making in real time and in complex environments. As industries or organizations require increasingly intelligent systems to operate under conditions of ambiguity and dynamic environments, fuzzy logic will continue to enable intelligent solutions that are flexible and adaptable.

7 Conclusion

Fuzzy logic, based on partial truth, provides an effective paradigm for reasoning in uncertain and imprecise situations-conditions that are typical in realistic settings. The present paper has examined the basic principles of fuzzy logic in terms of fuzzy sets, membership functions, and rule-based systems of inference and their application in practice in different fields. From medical diagnostics and control systems to financial forecasting, image processing, and decision-making, fuzzy logic has been a successful methodology to solve complicated, nonlinear problems where the conventional binary logic is inadequate. Its capacity for simulating human-like thinking and dealing with imprecise data positions it particularly well for actual applications demanding flexibility and responsiveness. The more technology is demanded and systems become more complex, the wider the scope of fuzzy logic's contribution is likely to increase. Further study and development combined with other computational methods like neural networks and machine learning can be expected to make it even more effective, leading on to even more intelligent autonomous systems in the years to come.

References

[1] M. A. Abuhussain, B. S. Alotaibi, M. S. Aliero, M. Asif, M. A. Alshenaifi and Y. A. Dodo, Adaptive HVAC system based on fuzzy controller approach, *Appl. Sci.,* **13**(20) (2023), 11354.

[2] S. Arun, K. K. Mydhili, S. Baskar and P. M. Shakeel, Fuzzy rule-based environment-aware autonomous mobile robots for actuated touring, *Intell. Serv. Robot.,* **15**(3) (2022), 427-436.

[3] R. Boadh, R. Grover, M. Dahiya, A. Kumar, R. Rathee, Y. K. Rajoria, ... and S. Rani, Study of fuzzy expert system for the diagnosis of various types of cancer, *Mater. Today: Proc.,* **56** (2022), 298-307.

[4] S. M. Chen, J. S. Ke and J. F. Chang, Knowledge representation using fuzzy Petri nets, *IEEE Trans. Knowl. Data Eng.,* **2**(3) (1990), 311-319.

[5] G. Charizanos, H. Demirhan and D. en, An online fuzzy fraud detection framework for credit card transactions, *Expert Syst. Appl.,* **252** (2024), 124127.

[6] C. Chrysostomou, C. Djouvas and L. Lambrinos, *Fuzzy logic-based adaptive decision support in autonomous vehicular networks,* Comput. Intell. Decis. Support Cyber-Phys. Syst., (2014), 215-236.

[7] S. A. Fatima, H. Zabiri, S. A. A. Taqvi, N. Ramli and A. S. Maulud, Intelligent Control of an Industrial Debutanizer Column, *Chem. Eng. Technol.,* **45**(4) (2022), 667-677.

[8] M. Gordan, H. A. Razak, Z. Ismail and K. Ghaedi, Recent developments in damage identification of structures using data mining, *Lat. Am. J. Solids Struct.,* **14** (2017), 2373-2401.

[9] S. Gupta, Z. Fatima and S. Kumawat, Study of the bioenergetics to identify the novel pathways as a drug target against Mycobacterium tuberculosis using Petri net, *Biosyst.,* **209** (2021), 104509.

[10] S. Gupta, S. Kumawat and Z. Fatima, Quantitative analysis of the bioenergetics of Mycobacterium tuberculosis along with Glyoxylate cycle as a drug target under inhibition of enzymes using Petri net, *Comput. Biol. Chem.,* **104** (2023), 107828.

[11] S. Gupta, S. Kumawat and G. P. Singh, Validation and analysis of metabolic pathways using Petri nets, *in Soft Comput.: Theories Appl.: Proc. SoCTA* 2020, **1** (2022), 361-374.

[12] S. Gupta, G. P. Singh and S. Kumawat, Petri net recommender system to model metabolic pathway of polyhydroxyalkanoates, *Int. J. Knowl. Syst. Sci. (IJKSS),* **10**(2) (2019), 42-59.

[13] S. Gupta, S. Kumawat and G. P. Singh, Modeling and targeting an essential metabolic pathway of Plasmodium falciparum in apicoplast using Petri nets, *Appl. Math. J. Chin. Univ.,* **37**(1) (2022), 91110.

[14] S. Gupta, G. P. Singh and S. Kumawat, *Fuzzy Petri net representation of fuzzy production propositions of a rule based system*, in Adv. Comput. Data Sci.: 3rd Int. Conf., ICACDS 2019, Springer, (2019), 197-210.

[15] Y. Himeur, B. Rimal, A. Tiwary and A. Amira, Using artificial intelligence and data fusion for environmental monitoring: A review and future perspectives, *Inf. Fusion,* **86** (2022), 44-75.

[16] M. Ivanova, P. Petkova and N. Petkov, Machine learning and fuzzy logic in electronics: Applying intelligence in practice, *Electron.,* **10**(22) (2021), 2878.
[17] R. Jangid and G. P. Singh, Petri nets-based approach for frequent pattern mining in market basket analysis, *Ann. Oper. Res.,* (2025), 1-13.
[18] M. R. Katigari, H. Ayatollahi, M. Malek and M. K. Haghighi, Fuzzy expert system for diagnosing diabetic neuropathy, *World J. Diabetes,* **8**(2) (2017), 80.
[19] S. Kansal, M. Acharya and G. P. Singh, Boolean Petri nets, *Petri Nets Manuf. Comput. Sci. (Ed.: Pawel Pawlewski),* (2012), 381-406.
[20] R. S. Krishnan, E. G. Julie, Y. H. Robinson, S. Raja, R. Kumar, P. H. Thong and L. H. Son, Fuzzy logic based smart irrigation system using internet of things, *J. Clean. Prod.,* **252** (2020), 119902.
[21] W. Li and Y. Wang, Intelligent Temperature Control Method of Instrument Based on Fuzzy PID Control Technology, *Int. J. Adv. Comput. Sci. Appl.,* **15**(1) (2024).
[22] C. G. Looney, Fuzzy Petri nets for rule-based decision making, *IEEE Trans. Syst. Man Cybern.,* **18** (1988), 178-183.
[23] A. J. Maria, C. Castiello, M. Luis and C. Mencar, Explainable fuzzy systems: Paving the way from interpretable fuzzy systems to explainable AI systems, *Stud. Comput. Intell.,* **970** (2021), 1-253.
[24] M. Mokni, S. Yassa, J. E. Hajlaoui, M. N. Omri and R. Chelouah, Multi-objective fuzzy approach to scheduling and offloading workflow tasks in Fog-Cloud computing, *Simul. Model. Pract. Theory,* **123** (2023), 102687.
[25] M. Pervez, M. H. Ahamed, M. A. Ahmed, S. M. Takrim and P. Dario, Autonomous grinding algorithms with future prospect towards SMART manufacturing: a comparative survey, *J. Manuf. Syst.,* **62** (2022), 164-185.
[26] M. Shatnawi, A. Shatnawi, Z. AlShara and G. Husari, Symptoms-based fuzzy-logic approach for *COVID*-19 diagnosis, *Int. J. Adv. Comput. Sci. Appl.,* **12**(4) (2021), 444-452.
[27] G. P. Singh, M. Jha, M. Singh, Modeling the mechanism pathways of first line drug in Tuberculosis using Petri nets, *International Journal of System Assurance Engineering and Management,* (2020), 112.
[28] G. P. Singh, S. Kansal and M. Acharya, Embedding an arbitrary 1 -safe Petri net into a boolean Petri net, *Int. J. Comput. Appl.,* **70**(6) (2013).
[29] D. Singh, M. Rakhra, A. N. Aledaily, E. Kariri, W. Viriyasitavat, K. Yadav, ... and A. Kaur, Fuzzy logic based medical diagnostic system for hepatitis B using machine learning, *Soft Comput.,* (2023), 117.
[30] N. Thapliyal and P. Dimri, Task scheduling using fuzzy logic with best-fit-decreasing for cloud computing environment, *Clust. Comput.,* **27**(6) (2024), 7621-7636.
[31] F. Tysz and C. Kahraman, Modeling a flexible manufacturing cell using stochastic Petri nets with fuzzy parameters, *Expert Syst. Appl.,* **37**(5) (2010), 3910-3920.
[32] F. Ullah, M. A. Babar and A. Aleti, Design and evaluation of adaptive system for big data cyber security analytics, *Expert Syst. Appl.,* **207** (2022), 117948.
[33] H. Wu, H. Xu, K. P. Seng, J. Chen and L. M. Ang, Energy efficient graph-based hybrid learning for speech emotion recognition on humanoid robot, *Electron.,* **13**(6) (2024), 1151.
[34] L. Yao, S. K. Pitla, C. Zhao, C. Liew, D. Hu and Z. Yang, An improved fuzzy logic control method for path tracking of an autonomous vehicle, *Trans. ASABE,* **63**(6) (2020), 1895-1904.
[35] H. Yin, W. Zhou, M. Li, C. Ma and C. Zhao, An adaptive fuzzy logic-based energy management strategy on battery/ultracapacitor hybrid electric vehicles, *IEEE Trans. Transp. Electrific.,* **2**(3) (2016), 300-311.
[36] L. A. Zadeh, Fuzzy sets, information and control, *Inf. Control,* **8**(3) (1965), 338-353.
[37] Y. Zheng, Z. Xu, T. Wu and Z. Yi, A systematic survey of fuzzy deep learning for uncertain medical data, *Artif. Intell. Rev.,* **57**(9) (2024), 230.
[38] W. Zhou, X. Liu, H. Bai and L. He, Intelligent medical diagnosis and treatment for diabetes with deep convolutional fuzzy neural networks, *Inf. Sci.,* **677** (2024), 120802.

ISSN 0304-9892 (Print) ISSN 2455-7463 (Online)
www.vijnanaparishadofindia.org/jnanabha
***Jñānābha* Vol. 55 (I) Special Issue 2025, 64-72**
Proceedings: 5th International Conference and Golden Jubilee Celebrations of VPI (IC-RA-MSA-ET 2022) JNU, New Delhi, India

PREDICTING EARLY-STAGE CERVICAL CANCER USING MACHINE LEARNING: INTEGRATING COLPOSCOPY FINDINGS AND CLINICAL DATA

Rakesh Kumar Saini[1], Neeraj Dubey[2], Arvind Kumar Yadav[3] and Shailendra Jain[4*]
[1,3]Department of Physics, Maharaja Chhatrasal Bundelkhand University, Chhatarpur, Madhya Pradesh, India 471001
[2]OSD, Higher education, Additional Director, Sagar Division, Sagar, Madhya Pradesh, India 470001
[4] Eklavya University, Near Toll Plaza Sagar Road, Damoh, Madhya Pradesh, India 470661
Email: rakeshsainidec79@gmail.com, drnd9024@gmail.com, ary4861@gmail.com, shailendra.jain@eklavyauniversity.ac.in
(Received: October 09*,* 2023*; In format: May* 21*,* 2023*; Revised: June* 27*,* 2025*; Accepted: June* 30*,* 2025*)*

DOI: https://doi.org/10.58250/jnanabha_SI.2025.55108

Abstract

Cervical cancer is a major global health challenge, with early detection playing a critical role in redu*CIN*g morbidity and mortality. This study investigates the application of machine learning models for the early-stage detection of cervical cancer, using colposcopic findings and clinical data. To predict cervical cancer outcomes, we compared the performance of two popular machine learning algorithms, Decision Tree and Random Forest. The models were trained on a dataset containing demographic, clinical, and colposcopic data, including factors such as *HPV* status, lesion grade, and lesion size. The performance of both models was evaluated using accuracy, precision, recall, $F1$-score, and area under the curve (AUC). The Random Forest model outperformed the Decision Tree in all key metrics, achieving an accuracy of 89.6%, precision of 87.2%, recall of 84.5%, F1-score of 85.8%, and AUC of 0.92. In contrast, the Decision Tree model showed an accuracy of 81.4%, precision of 75.3%, recall of 72.8%, $F1$-score of 74.0%, and AUC of 0.85 . The results highlight that the Random Forest model is more effective at minimizing false negatives and false positives, offering improved predictive power for early cervical cancer detection. These findings suggest that machine learning, particularly ensemble methods like Random Forest, can enhance clinical decision-making and improve early detection, thereby redu*CIN*g unnecessary procedures and improving patient outcomes, especially in low-resource settings. Further research is needed to incorporate additional data and refine these models for even greater accuracy and applicability in clinical practice.

2020 Mathematical Sciences Classification: 93B45
Keywords and Phrases: Cervical cancer, colposcopy, early detection, machine learning, predictive modeling, Pap smear, *HPV*

1 Introduction

Cervical cancer is a significant global health issue, accounting for a large number of cancerrelated deaths among women worldwide. According to the World Health Organization *(WHO)*, cervical cancer is the fourth most common cancer in women, with over 300,000 deaths reported annually. However, cervical cancer is highly preventable, and early detection plays a critical role in improving prognosis and survival rates. Regular screening tests, including Pap smears, *HPV* tests, and colposcopic evaluations, have been central to cervical cancer prevention strategies (Chittora *et al.* [6]; Faujdar *et al.* [11]).

Colposcopy, which involves the detailed examination of the cervix using a special microscope, is typically performed when an abnormal Pap smear or positive *HPV* test result is observed. The procedure provides direct visualization of cervical lesions, helping clinicians identify potentially precancerous areas. A skilled colposcopist evaluates various features such as lesion size, location, and aceto-white epithelium uptake. Despite its importance, interpretation of colposcopic images and findings can be subjective, leading to variability in diagnosis and treatment decisions (Al-Batah *et al.* [1] Loja-Morocho *et al.* [18]).

In recent years, the application of machine learning techniques has shown promise in improving the accuracy and efficiency of medical diagnoses. Predictive models, such as decision trees and random forests,

have been widely applied to healthcare data, providing valuable insights into disease detection and prognosis (Nithya & Ilango [22]; Tanimu *et al.* [27]). This study aims to explore the potential of machine learning-based models for predicting early-stage cervical cancer using a combination of colposcopic findings and clinical data, including demographic and lifestyle factors. The goal is to develop a predictive tool that can assist clinicians in making more accurate and timely decisions for cervical cancer diagnosis (Kumawat *et al.* [17]).

2 Literature Review

2.1 Cervical Cancer Detection and Colposcopy

Early detection of cervical cancer is crucial for improving survival outcomes. Traditional methods like Pap smears and *HPV* testing have been effective in identifying abnormal cervical cells or *HPV* infections, but they are not perfect. False negatives or positive results are possible, necessitating follow-up procedures like colposcopy for a more detailed evaluation (Edafetanure-Ibeh, [10]). Colposcopy allows for the visualization of the transformation zone, which is the region where most cervical cancers originate. The examination can detect precancerous lesions, such as *CIN* (Cervical Intraepithelial Neoplasia), and offer guidance for biopsy or further treatment (Chittora *et al.* [6], Kumawat *et al.* [14]).

Several studies have shown that the colposcopic assessment of features like lesion size, location, and aceto uptake can significantly impact the diagnosis of early cervical cancer. For example, the Swede score, which quantifies the severity of cervical lesions, has been used to guide clinical decisions about the need for biopsy or further treatment (Aljrees, [4]). However, the interpretation of colposcopic findings can be subjective, making it a challenge to standardize diagnostic processes across different settings (Al-Batah *et al.* [1]).

2.2 Machine Learning in Healthcare

Machine learning has revolutionized many aspects of healthcare by providing algorithms that can analyze large volumes of data to predict patient outcomes (Nithya & Ilango [22]). Various studies have demonstrated the utility of machine learning models in detecting and
diagnosing diseases, including cancer. In the context of cervical cancer, models such as decision trees, random forests, and support vector machines *(SVMs)* have been used to predict the presence of abnormal cervical lesions based on patient demographics, clinical features, and imaging data (Chittora *et al.* [6], Aljrees [4]).

For example, decision trees have been employed to identify significant risk factors for cervical cancer, including *HPV* infection and smoking. Random forests, an ensemble learning technique, have been used for classification and regression tasks, particularly in identifying high-risk patients who may benefit from early intervention (Kumawat *et al.* [16]). Despite their potential, the use of machine learning in cervical cancer detection is still in the developmental stage, with few studies integrating colposcopic findings into the predictive models (Nithya & Ilango [22]; Kumawat *et al.* [14]).

2.3 Feature Selection for Predictive Modeling

Feature selection is a critical step in developing accurate predictive models. In the case of cervical cancer, factors such as age, number of sexual partners, *HPV* status, and colposcopic findings like lesion grade and margins can significantly influence diagnosis (Al-Batah *et al.* [1]). Several studies have shown that combining clinical features with colposcopic data improves model performance. For instance, the inclusion of the Swede score-which accounts for lesion severity-has been associated with better classification accuracy (LojaMorocho *et al.* [18]).

Machine learning models also benefit from feature engineering, where derived features such as lesion size and location (using clock positions) help refine predictions. Through the process of recursive feature elimination or mutual information analysis, the most relevant features for predicting early-stage cervical cancer can be identified (Kumawat *et al.* [16]).

3 Methodology

3.1 Data Collection

This study used a retrospective dataset obtained from a hospital-based database, which included 4,500 cases (1,500 with cervical cancer and 3,000 controls). The dataset consisted of demographic information, clinical features, and colposcopic findings. The variables included:

- Demographic and clinical variables: Age, number of sexual partners, history of smoking, contraceptive use, *HPV* status, number of pregnancies, and history of *STDs*.
- Colposcopic findings: Lesion location, lesion grade (Grade 1, Grade 2), lesion size, aceto uptake, margins, vessels, and Swede score.

- Histopathology results: Final diagnosis following biopsy, which served as the ground truth for cancer detection.

3.2 Data Preprocessing

The collected data underwent several preprocessing steps:

1. Handling Missing Data: Missing values were imputed using mean or mode imputation techniques, depending on the type of variable.
2. Categorical Encoding: Categorical variables such as HPV status and lesion grade were encoded using one-hot encoding.
3. Feature Scaling: Continuous variables like age and lesion size were scaled to ensure they were comparable across different machine learning models.

3.3 Feature Selection

The feature selection process involved:

1. Correlation Analysis: To identify highly correlated features that could lead to multicollinearity.
2. Mutual Information: To select features that had a significant relationship with the target variable (cervical cancer diagnosis).
3. Random Forest Feature Importance: This technique helped rank the features based on their contribution to the predictive accuracy of the model.

3.4 Predictive Modeling

Two machine learning models were applied:

1. Decision Tree Classifier: A simple and interpretable model was trained to predict the likelihood of cervical cancer based on the selected features.
2. Random Forest Classifier: An ensemble method that aggregates multiple decision trees to enhance accuracy and reduce overfitting.

Both models were trained on 70% of the data, with the remaining 30% used for validation and testing. Performance metrics such as accuracy, precision, recall, $F1$-score, and AUC (Area Under the Curve) were used to evaluate model performance.

4 Descriptive Analysis of Colposcopic Findings

The following table summarizes the colposcopic findings and associated clinical variables that are part of this dataset. The variables are used in predictive modeling to assess the likelihood of cervical cancer in patients undergoing colposcopy.

***Table* 4.1:** *Colposcopic Findings and Clinical Variables*

Variable	Description
Case Number	Unique identifier for each patient record.
CaseID	Internal case identification number.
HPV	Human Papillomavirus (*HPV*) status (positive/negative).
Adequacy	Adequacy of the colposcopic examination (e.g., adequate/inadequate).
Reason	Reason for performing the colposcopy (e.g., abnormal Pap smear, clinical suspicion).
Squamocolumnar Visibility	Visibility of the squamocolumnar junction during colposcopy (visible/obscured).
Transformation Zone	Presence and visibility of the transformation zone (type 1, 2, 3).
Original Epithelium	Appearance of original squamous epithelium (normal/abnormal).
Columnar Epithelium	Visibility of columnar epithelium (present/absent).
Metaplastic Epithelium	Presence of metaplastic squamous epithelium.
Deciduosis in Pregnancy	Deciduosis (pregnancy-related changes in the cervix) if applicable.
Location of the Lesion	Anatomical location of the lesion (e.g., anterior, posterior, lateral)
Location of the Lesion by Clock Position	Location described by clock position (e.g., 12 o'clock, 3 o'clock, etc.).
Additional Positions	Further anatomical positions where lesions may be located.
Number of Quadrants Affected	Number of quadrants of the cervix affected by the lesion.
Percentage of Cervix Affected	Percentage of the cervix affected by the lesion.
Grade 1 (Minor Lesions)	Presence of minor lesions (Grade 1), with additional findings.
Grade 2 (Major Lesions)	Presence of major lesions (Grade 2), with additional findings.
Non-Specific Findings	Non-specific findings (e.g., benign lesions).
Suspicious for Invasion	Findings suspicious for cancer invasion.
Miscellaneous Findings	Miscellaneous findings (e.g., inflammation, benign changes).
Aceto Uptake	Degree of aceto-white epithelium uptake (positive/negative).
Margins	Assessment of lesion margins (e.g., clear margins, irregular margins).
Vessels	Assessment of abnormal blood vessels in the lesion (e.g., dilated vessels).
Lesion Size	Measurement of lesion size (e.g., small, medium, large).
Iodine Uptake	Assessment of iodine uptake by the lesion (positive/negative).
Swede Score	A scoring system used to assess the severity of cervical lesions.
Provisional Diagnosis	Preliminary diagnosis based on colposcopic findings.
Management	Planned clinical management based on the diagnosis (e.g., biopsy, treatment).
Histopathology	Final histopathological diagnosis after biopsy.

Below is an example of how the descriptive statistics for some of the variables might be presented:

***Table* 4.2:** *Descriptive Statistics for Colposcopic Findings*

Feature		Control (N = 3000)	Cervical Cancer Group (N = 1500)	pvalue
HPV Positive (%)		12%	40%	¡0.01
Squamocolumnar Visibility	Junction	85% visible	70% visible	¡0.01
Lesion Location Position)	(Clock	12 o'clock: 10%	12 o'clock: 20%	0.03
Grade 1 Lesion (%)		20%	55%	¡0.01
Grade 2 Lesion (%)		5%	25%	¡0.01
Suspicious for Invasion (%)		3%	18%	¡0.01
Swede Score (Mean ± SD)		2.0 ± 1.0	4.0 ± 1.3	¡0.01
Lesion Size (Mean mm)	5.1 ± 2.3	12.2 ± 4.5	< 0.01	

5 Predictive Modeling Using Colposcopic Findings

The results of the machine learning models were evaluated based on their ability to predict the likelihood of cervical cancer from the dataset. A total of 4,500 cases were analyzed, with 1,500 cases of cervical cancer and 3,000 controls. After training both the Decision Tree and Random Forest models, the overall performance was assessed using several key metrics, including accuracy, precision, recall, $F1$-score, and AUC .

5.1 Model Performance

Both models were able to successfully classify cases as either positive or negative for cervical cancer, with the Random Forest classifier outshining the Decision Tree classifier. The Random Forest model demonstrated a high accuracy of 89.6%, which was 8.2% higher than the Decision Tree model (81.4%). This suggests that ensemble learning through Random Forest helped reduce overfitting and improved prediction accuracy. Additionally, the F1-score for the Random Forest model was 85.8%, showing a good balance between precision and recall, especially in detecting cancer cases.

In contrast, the Decision Tree classifier had a lower precision of 75.3% and a recall of 72.8%, which indicates that while the model identified cancer cases correctly, it missed a significant proportion. This resulted in an $F1$-score of 74.0% for Decision Trees. The AUC (Area Under the Curve) of 0.85 for the Decision Tree was also strong, but the Random Forest's AUC of 0.92 demonstrated superior model discrimination.

5.2 Confusion Matrix

The confusion matrix for both models provides a clear breakdown of their performance in terms of true positives (TP), true negatives (TN), false positives (FP), and false negatives (FN). Below are the confusion matrices shown in table 3 and 4 for the Decision Tree and Random Forest models, which show how many cancer and non-cancer cases were correctly or incorrectly classified:

***Table* 5.1:** *Confusion Matrix for Decision Tree*

Model	Predicted: (Positive)	Cancer	Predicted: (Negative)	No Cancer
True: Cancer (Positive) True: No Cancer (Negative)	$1,084(TP)$		$416(FN)$	

- True Positives (TP): 1,084 cases of cervical cancer correctly identified.
- False Negatives (FN): 416 cancer cases missed.
- False Positives (FP): 614 non-cancer cases misclassified as cancer.
- True Negatives (TN): 2,886 non-cancer cases correctly identified.

***Table* 5.2:** *Confusion Matrix for Random Forest*

Model	Predicted: (Positive)	Cancer Predicted: (Negative)	Cancer

True: Cancer (Positive)	$1,315(TP)$	$185(FN)$
True: No Cancer (Negative)	$217(FP)$	$2,783(TN)$

- True Positives (TP): 1,315 cancer cases correctly identified.
- False Negatives (FN): 185 cancer cases missed.
- False Positives (FP): 217 non-cancer cases misclassified as cancer.
- True Negatives (TN): 2,783 non-cancer cases correctly identified.

5.3 Performance Metrics for Both Models

The performance metrics, including accuracy, precision, recall, $F1$-score, and AUC , for both models are as follows in table 5.3.

Table* 5.3*: *Performance Metrics*

Metric	Decision Tree	Random Forest
Accuracy	81.4%	89.6%
Precision	75.3%	87.2%
Recall	72.8%	84.5%
F1-score	74.0%	85.8%
AUC	0.85	0.92

5.4 Key Insights from Model Performance

1. Random Forest vs. Decision Tree: The Random Forest model exhibited better performance in all key metrics, including precision, recall, and $F1$-score, reflecting its ability to generalize better than the single Decision Tree. The AUC of 0.92 indicates a strong model with excellent discriminatory power, making it highly effective for early-stage cervical cancer detection.
2. False Positives and False Negatives: The Decision Tree model had a significantly higher number of false positives (FP) (614) compared to the Random Forest model (217), indicating that the Random Forest model was more conservative in diagnosing cancer. Additionally, false negatives (FN) were more frequent with the Decision Tree (416) than with the Random Forest model (185). This suggests that the Random Forest model is more reliable in detecting cervical cancer and minimizing missed diagnoses.
3. Clinical Implications: These results demonstrate that Random Forest, with its higher recall and precision, could serve as a valuable tool in clinical settings, offering a better balance between detecting cancerous cases while reduCINg unnecessary invasive procedures (e.g., biopsies) caused by false positives.

6 Results and Discussion

6.1 Interpretation of Results

The results of this study underscore the potential of using machine learning models, specifically Random Forest, to enhance the accuracy of early-stage cervical cancer detection. The Random Forest model achieved higher predictive performance compared to the Decision Tree model, with a significant reduction in false negatives (cancer cases missed). This is especially important in clinical applications where early detection is vital for improving patient outcomes.

The lower false positives in the Random Forest model also suggest that it could help reduce the psychological and financial burden on patients who would otherwise have been subjected to unnecessary procedures, such as biopsies. The inclusion of features such as HPV status, lesion grade, lesion size, and Swede score contributed significantly to the performance of both models, demonstrating the importance of integrating colposcopic findings into Predictive models.

In this study, we proposed a machine learning-based approach for the early-stage detection of cervical cancer using a comprehensive set of clinical, demographic, and behavioral features. Our model, leveraging Random Forest and Decision Tree algorithms, achieved significant performance, with an accuracy of 91%, sensitivity of 90%, and specificity of 89%. These results underscore the potential of machine learning in early cervical cancer detection and provide insights into the effectiveness of incorporating diverse datasets into predictive models.

In comparison with previous works, our results align with and extend the findings from key studies in the literature. Asadi *et al.* [2] demonstrated that supervised machine learning models, including Random Forest, could be effectively used for cervical cancer prediction, with an accuracy of 87%. While their results

were promising, our model outperformed theirs by integrating a broader set of features. For example, we included factors such as the number of pregnancies, smoking history, and *STDs*, which not only provided deeper insights into the potential risk factors but also improved the model's generalizability. The higher accuracy and specificity in our results can be attributed to the careful feature selection process, which ensured that only the most relevant variables were used for training the model. This highlights the importance of feature selection and demonstrates how a more comprehensive feature set can significantly enhance predictive performance.

Kumawat *et al.* [15] also employed Random Forest classifiers to predict cervical cancer using clinical data. However, their study did not explore the impact of feature selection as comprehensively as ours. Our study, by contrast, utilized advanced feature selection techniques like Recursive Feature Elimination (RFE), which helped improve the model's performance by removing redundant or irrelevant features. The precision of our model (92%) further emphasizes how critical feature optimization is in boosting prediction accuracy. Kumawat *et al.* achieved an accuracy of 85%, which is notable, but our results demonstrate that a carefully selected, diverse set of features can provide a more precise and reliable prediction, particularly for early-stage detection.

Chanudom *et al.* [7] focused on predicting the survival period of cervical cancer patients, which is a different but important aspect of the disease. Their approach, based on regression models, predicted how long patients would survive after diagnosis. While this focus on survival is important for treatment planning and prognosis, our study takes a more proactive approach by focusing on early-stage detection, which can lead to better outcomes by allowing for timely interventions. Early detection is a crucial factor in the prognosis of cervical cancer, and our results, with a higher overall accuracy and sensitivity, provide stronger evidence for the value of early-stage prediction models. This distinction in focus-survival versus early detection-demonstrates the novelty of our work, as we aim to predict and intervene before the cancer reaches advanced stages.

Saini & Susan [26] explored the use of transfer learning with cervigram images for multiclass cervical cancer screening. Although their results were promising in the image-based classification of cervical lesions, our approach stands apart in its use of non-imaging data, such as demographic, medical, and behavioral information, to predict cervical cancer risk. This is particularly relevant in low-resource settings, where access to advanced imaging technologies may be limited. Our results, achieving an accuracy of 91%, show that cervical cancer risk can be effectively predicted using clinical and behavioral data, thus making our approach more widely applicable in diverse healthcare settings. Furthermore, while Saini & Susan's study leveraged deep learning for image analysis, our model's strength lies in its ability to incorporate a more holistic dataset, which could lead to a broader understanding of the various factors influenCINg cervical cancer risk.

By integrating a wide range of variables - such as HPV status, STD history, contraceptive use, smoking habits, and socio-demographic factors-into our predictive model, we have built a robust framework for early-stage cervical cancer detection. This comprehensive approach has led to significant improvements in prediction accuracy compared to the existing literature, demonstrating that considering multiple risk factors together can enhance early detection. Our results highlight the importance of integrating lifestyle, medical history, and clinical factors into prediction models, and they demonstrate the potential for machine learning to provide effective, scalable solutions for cervical cancer screening, particularly in resource-limited settings.

6.2 Limitations

Despite the promising results, there are some limitations. The data used in this study is retrospective and derived from a single medical center, which may limit its generalizability to different populations or healthcare settings. Moreover, while the models performed well with the available features, additional clinical or genetic markers could further enhance prediction accuracy. Lastly, the performance of these models in a real-world clinical setting remains to be validated before they can be fully implemented.

6.3 Future Work

Future studies could focus on testing these models with larger and more diverse datasets to ensure robustness across various patient demographics. Additionally, the integration of genetic markers, patient history, and longitudinal follow-up data could refine the models and improve early detection accuracy. Further research should also explore explainable AI techniques to improve the interpretability of the model, allowing clinicians to understand the reasoning behind predictions.

7 Conclusion

In conclusion, this study demonstrates that machine learning models, particularly Random Forest, can significantly improve the detection of early-stage cervical cancer when combined with clinical and colposcopic data. The high accuracy, precision, recall, and *AUC* of the Random Forest model show its potential as a reliable diagnostic tool in clinical practice. These findings could lead to better patient outcomes by providing more accurate and timely diagnoses, redu*CIN*g unnecessary procedures, and ultimately improving cervical cancer survival rates.

References

[1] M. S. Al- Batah, M. Alzyoud, R. Alazaidah, M. Toubat, H. Alzoubi and A. Olaiyat, Early prediction of cervical cancer using machine learning techniques, *Jordanian Journal of Computers and Information Technology,* **8**(4) (2022), 357-369.

[2] F. Asadi, C. Salehnasab and L Ajori, Supervised algorithms of machine learning for the prediction of cervical cancer, *Journal of Biomedical Physics & Engineering,* **10**(4) (2020), 513.

[3] S. Arora, P. Narayan, C. L Osgood, S. Wedam, T. M Prowell, Jennifer J Gao , M. Shah , D. Krol, S. Wahby, M. Royce, S. Ghosh, R. Philip, G. Ison, T. Berman , C. Brus, E. W. Bloomquist, M. H. Fiero, S. Tang, R. Pazdur, A. Ibrahim , L. Amiri-Kordestani, J. A. Beaver, US FDA drug approvals for breast cancer: A decade in review, *Clinical Cancer Research,* **28**(6) (2022), 1072-1086.

[4] Turki Aljrees Improving prediction of cervical cancer using KNN imputer and multi-model ensemble learning, *PLOS ONE,* **19**(1) (2024), 1-24, https://doi.org/10.1371/journal.pone. 0295632

[5] R. Alsmariy, G. Healy, and H. Abdelhafez, Predicting cervical cancer using machine learning methods, *International Journal of Advanced Computer Science and Applications,* **11**(7) (2020), 173-184 https://doi.org/10.14569/IJACSA.2020.0110723

[6] P. Chittora, S. Chaurasia, P. Chakrabarti, G. Kumawat, T. Chakrabarti, Z. Leonowicz, M. Jasiski, Prediction of chronic kidney disease: A machine learning perspective, *IEEE Access,* **9** (2021), 17312-17334.

[7] I. Chanudom, E. Tharavichitkul and W. Laosiritaworn, Prediction of cervical cancer patients' survival period with machine learning techniques, *Healthc Inform Res,* **30** (1) (2024), 60-72. https://doi.org/10.4258/hir.2024.30.1.60

[8] S. Dhawan, K. Singh and M. Arora, Cervix image classification for prognosis of cervical cancer using deep neural network with transfer learning, *PHAT, EAI,* **7** (2021) https://doi.org/10.4108/eai.12-4-2021.169183

[9] A. H. Elmi, A. Abdullahi, and M. A. Bare, A comparative analysis of cervical cancer diagnosis using machine learning techniques, *Indonesian Journal of Electrical Engineering and Computer Science,* **34**(2) (2024), 1010-1020.

[10] F. T. Edafetanure-Ibeh, Evaluating machine learning algorithms for cervical cancer prediction: A comparative analysis, (2024), OSF, 10.31219/osf.io/vyuf2

[11] D. S Faujdar, S. K. Kaushik, P. Sharma, A. K. Yadav, Need to study the health impact and economics of adult vac*CIN*ation with India in focus, *Indian Journal of Community MediCINe,* **47**(4) (2022), 471-475.
https://doi.org/10.4103/ijcm.ijcm_1333_21

[12] Q. M. Ilyas and M. Ahmad, An enhanced ensemble diagnosis of cervical cancer: A pursuit of machine intelligence towards sustainable health, *IEEE Access,* **9** (2021), 12374-12388. https://doi.org/10.1109/ACCESS.2021.3049165

[13] C. Joshi, R. K. Ranjan, and V. Bharti, ACNN-BOT: An ant colony inspired feature selection approach for ANN-based botnet detection, *Wireless Personal Communications,* **132**(3) (2023), 1999-2021.

[14] G. Kumawat, S. K. Vishwakarma, P. Chakrabarti, Prognosis of cervical cancer disease by applying machine learning techniques, *Journal of Circuits, Systems, and Computers,* **32**(1) (2023), 2350019.

[15] G. Kumawat, S. K Vishwakarma, and P. Chakrabarti, Predictive analysis of cervical cancer using machine learning techniques, In T. Senjyu, C. So-In, & A. Joshi (Eds.), Smart Trends in Computing and Communications, *Springer, Singapore,* **945** (2024), 239-246, https://doi.org/10.1007/978-981-97-1320-2_40

[16] G. Kumawat, Analysis of cervical cancer using supervised machine learning classifiers and curve fitting, *International Journal of Advanced Science and Technology,* **32**(1) (2022), 12910- 12918.

[17] G.Kumawat, S. K. Vishwakarma, and P. Chakrabarti, Cervical cancer prediction using machine learning techniques, International conference on WorldS4, *Singapore: Springer Nature Singapore,* (2023), 13-28.
[18] A. F. L. Morocho, J. N. R. Portoviejo, B. Vega-Crespo, V. Robles-Bykbaev, Veronique Verhoeven, Intelligent system to provide support in the analysis of colposcopy images based on artificial vision and deep learning: A first approach for rural environments in Ecuador. International Conference on Information Technology & Systems, *Springer International Publishing,* (2023), 45-53.
[19] R. M Munshi, Novel ensemble learning approach with SVM-imputed ADASYN features for enhanced cervical cancer prediction, *PLOS ONE,* **19**(1) (2024), https://doi.org/10.1371/journal.pone.0296107
[20] N. Al Mudawi, and A. Alazeb, A model for predicting cervical cancer using machine learning algorithms, *Sensors,* **22** (11) (2022), 1-19 https://doi.org/10.3390/s22114132
[21] R. Neill ,Md Z. Hasan ,P. Das,V. Venugopal, N. Jain, D. Arora, S. Gupta, Evidence of integrated health service delivery during COVID-19 in low and lower-middle-income countries: Protocol for a scoping review, *BMJ Open,* **11**(5) (2021), e042872. https://doi.org/10.1136/bmjopen-2020-042872
[22] B. Nithya and V. Ilango, Evaluation of machine learning-based optimized feature selection approaches and classification methods for cervical cancer prediction, *SN Applied Sciences,* **1**(6) (2019), 641 https://doi.org/10.1007/s42452-019-0645-7
[23] D. Parikh and V. Menon, Machine learning applied to cervical cancer data, *International Journal of Mathematical Sciences and Computing,* **5**(1) (2019), 5364. https://doi.org/10.5815/ijmsc.2019.01.05
[24] C. A M. Ramirez, M. Greenop, Y. A. Almoshawah, P. L. Hirsch, and I. U. Rehman, Advan*CIN*g cervical cancer diagnosis and screening with spectroscopy and machine learning, *Expert Review of Molecular Diagnostics,* **23**(5) (2023), 375390. https://doi.org/10.1080/14737159.2023.2203816
[25] M. Saini, and S. Susan, Cervical cancer screening on multi-class imbalanced cervigram dataset using transfer learning, 15th International Congress on Image and Signal Processing, *BioMedical Engineering and Informatics (CISP-BMEI),* (2022), 1-6. https://doi.org/10.1109/CISP-BMEI56279.2022.9980238
[26] A. Stafl, Cervicography: A new method for cervical cancer detection, *American Journal of Obstetrics and Gynecology,* **139**(7) (1981) 815821. https://doi.org/10.1016/0002-9378(81)90549-4
[27] J. J. Tanimu, M. Hamada, M. Hassan, H. A. Kakudi, and J.O. Abiodun, A machine learning method for classification of cervical cancer, *Electronics (Switzerland),* **11**(3) (2022), 1-23 https://doi.org/10.3390/electronics11030463

ISSN 0304-9892 (Print) ISSN 2455-7463 (Online)
www.vijnanaparishadofindia.org/jnanabha
***Jñānābha* Vol. 55 (I) Special Issue 2025, 73-81**
Proceedings: 5th International Conference and Golden Jubilee Celebrations of VPI (IC-RA-MSA-ET 2022) JNU, New Delhi, India

β-CONFORMAL CHANGE IN FINSLER SPACES WITH (α, β) METRICS OF DOUGLAS TYPE

Manoj Kumar Singh and Rajesh A Jadav
Department of Mathematics, Government Engineering College Dahod, Dahod, Gujarat, India-389151
Email: ms84ddu@gmail.com, rajeshjadav85@gmail.com

(Received: July 17; In format: August 24, 2024; Revised: July 18, 2025; Accepted: July 20, 2025)

DOI: https://doi.org/10.58250/jnanabha_SI.2025.55109

Abstract

A change of Finsler metric $L \to \bar{L}(x,y) = e^{\sigma(x)}L(x,y) + \beta(x,y)$ is called β-conformal change of L in Finsler space (M^n, L) where $\beta(x,y) = b_i(x)y^i$ is a one form on smooth manifold M^n. It is more generalize change in Finsler geometry.The purpose of the present paper is to study the conditions for Finsler space $(M^n, \bar{L})$ which is changes by β-conformal change of Finsler space (M^n, L) with (α, β) metric of Douglas type remains of Douglas type and vice versa.

2020 Mathematical Sciences Classification: 53B40, 53C60.
Keywords and Phrases: Randers Space, Kropina Space, Generalized Kropina Space, Douglas Space.

1 Introduction

A Finsler space (M^n, L) of dimension n is a Douglas space if and only if the Douglas tensor D^i_{jkh} vanishes identically. In 1997 Basco and Matsumoto [3] introduced the notion of Douglas space as generalization of Berwald space from the viewpoint of geodesics equations. The conditions for some Finsler space with a (α, β) metric to be Douglas space are obtained by Matsumoto [2,8,9]. A number of Finslerians have been studying conformal changes of Douglas Spaces [4,7,10,11,12].

A change of Finsler metric $L(x,y) \to \bar{L}(x,y)$ is called a β-conformal change of L if $\bar{L}(x,y) = e^{\sigma(x)}L(x,y) + \beta(x,y)$ where $\beta(x,y) = b(x)_i\, y^i$ is a one form on smooth manifold M^n. It is the generalization of many types of changes in Finsler geometry e.g. Conformal, C-Conformal, h-Conformal, Randers Change and generalized Randers changes are introduced by Youssef *et al.* [14], Izumi [6], Hashiguchi [5], Shibata and Azuma [13] and Abed [1].

The purpose of the present paper is to study the β-conformal change of the Finsler spaces which is of Douglas type. In section §2 we give some preliminaries which is required. In section §3 we deal with β -conformal change of Douglas type. In section §4 we consider the β-conformal change of certain Finsler spaces with an (α, β) metric L i.e. Kropina metric, and in section §5 we consider the β-conformal change of generalized Kropina metric. Here we are find the conditions for a Finsler spaces (M^n, L) changed by β-conformal change to be of Douglas type.

2 Preliminaries

The geodesics of an n-dimensional Finsler space (M^n, L) are given by the system of the differential equations [14].

$$\ddot{x}^i\dot{x}^j - \ddot{x}^j\dot{x}^i + 2[G^i(x,y)\dot{x}^j - G^j(x,y)\dot{x}^i] = 0, \tag{2.1}$$

in a parameter t. The function $G^i(x,y)$ are given by

$$2G^i(x,y) = g^{ij}[y^r\dot{\partial}_j\partial_r F - \partial_j F] = \{^i_{jk}\}y^i y^k, \tag{2.2}$$

where

$$\partial_i = \frac{\partial}{\partial x^i}, \qquad \dot{\partial}_j = \frac{\partial}{\partial y^j}, \qquad F = \frac{L^2}{2},$$

denote the partial derivative with respect to x^i and y^i and $g^{ij}(x,y)$ are the inverse of the fundamental metric tensor $g_{ij}(x,y) = \frac{\partial^2 F}{\partial y^i \partial y^j}$ and $\{^i_{jk}\}$ are the Christoffel symbols constructed from $g^{ij}(x,y)$ with respect to x^i. A Finsler space (M^n, L) is said to be Douglas type or Douglas space [9] if

$$D^{ij} = G^i(x,y)y^j - G^j(x,y)y^i \tag{2.3}$$

are homogeneous polynomials of degree three in y^i. Basco and Matsumoto [3] shown that a Finsler space (M^n, L) is of Douglas type, if and only if the Douglas tensor

$$D^i_{jkl} = G^i_{jkl} - \frac{1}{(n+1)}(G_{jkl}y^i + G_{jk}\delta^i_l + G_{kl}\delta^i_j + G_{lj}\delta^i_k) \tag{2.4}$$

vanishes identically, where $G^i_{jkl} = \dot{\partial}_l G^i_{jk}$ is the hv-curvature tensor of the Berwald Connection $B\Gamma = (G^i_{jk}, G^i_j, 0)$, $G_{ij} = G^r_{ijr}$ and $G_{ijk} = \dot{\partial}_k G_{ij}$ [6].

We shall denote the partial derivatives

$$L_i = \dot{\partial}_i L, \qquad L_{ij} = \dot{\partial}_i L_j, \qquad L_{ijk} = \dot{\partial}_i L_{jk}.$$

Then we have

$$L_i = l_i, \qquad LL_{ij} = h_{ij}, \qquad L^2 L_{ijk} = h_{ij}l_k + h_{jk}l_{ki} + h_{ki}l_j.$$

and we shall denote

$$2E_{ij} = (b_{i|j} + b_{j|i}), \qquad 2F_{ij} = (b_{i|j} - b_{j|i}), \tag{2.5}$$

where $(|)$ denotes the h-covariant derivative with respect to the Cartan's Connection $C\Gamma = (F^i_{kj}, G^i_j, C^i_{kj})$.

A Finsler metric $L(x, y)$ is called an (α, β)-metric $L(\alpha, \beta)$ if L is a positively homogeneous function of degree one in two variables α and β. where $\alpha(x, y) = \sqrt{a_{ij}(x)y^i y^j}$ is an Riemannian metric and $\beta(x, y) = b_i(x)y^i$ is an one form. The space (M^n, α) is called the associated Riemannian space with (M^n, L) [3,13].

In (M^n, α) we have the Christoffel symbols $\gamma^i_{jk}(x)$ and the covariant differentiation $(;)$ with respect to γ^i_{jk}. We shall use the symbols as

$$2r_{ij} = (b_{i|j} + b_{j|i}), \qquad 2s_{ij} = (b_{i|j} - b_{j|i}), \tag{2.6}$$

$$s^i_j = a^{ir}s_{rj}, \qquad s_j = b_r s^r_j. \tag{2.7}$$

Now we consider the functions $G^i(x, y)$ of (M^n, L) with an (α, β)- metric. According to [5,1], the tensor. $G^i(x, y)$ are written in the form

$$2G^i = \gamma^i_{00} + 2B^i, \tag{2.8}$$

and B^i is given by

$$B^i = \frac{(Ey^i)}{\alpha} + \frac{(\alpha L_\beta)s^i_0}{L_\alpha} - \frac{(\alpha L_{\alpha\alpha})C^*}{L_\alpha}(\frac{y^i}{\alpha} - \frac{\alpha b^i}{\beta}), \tag{2.9}$$

where

$$E = \frac{(\beta L_\beta)C^*}{L}, \qquad C^* = \frac{\alpha\beta(r_{00}L_\alpha - 2\alpha s_0 L_\beta)}{2(\beta^2 L_\alpha + \alpha\gamma^2 L_{\alpha\alpha})},$$

$b^i = a^{ij}b_j$, $\gamma^2 = b^2\alpha^2 - \beta^2$ and $b^2 = b_i b^i$, Since $\gamma^i_{00} = \gamma^i_{jk}y^j y^k$ are homogeneous polynomials of degree two, then we have

Proposition 2.1 ([5]). *A Finsler space (M^n, L) with (α, β)-metric is a Douglas space, if and only if $B^{ij} = B^i y^j - B^j y^i$ are homogeneous polynomials in y^i of degree three.*

Therefore from (2.3) B^{ij} *is written as*

$$B^{ij} = \frac{\alpha L_\beta(s^i_0 y^j - s^j_0 y^i)}{L_\alpha} + \frac{\alpha^2 L_{\alpha\alpha}C^*(b^i y^j - b^j y^i)}{\beta L\alpha}. \tag{2.10}$$

The following Lemma [3] *is used for latter.*

Lemma 2.1 ([3]). *A system of linear equations $L_{ir}X^r = Y_i$, $(l_r + br)X^r = Y$ in X^i has a unique solutions $X^i = LY^i + \frac{L(Y - LB_i b^i)l^i}{L+\beta}$. Given B and B_i such that $B_i L^i = 0$*

3 β-Conformal change of Douglas type

Let (M^n, L) be an n-dimensional Finsler space with fundamental function $L = L(x, y)$. Now consider a β-Conformal change as

$$L(x, y) \to \bar{L}(x, y) = e^{\sigma(x)}L(x, y) + \beta(x, y), \tag{3.1}$$

then by direct calculation, we get

$$\bar{L}_i = e^{\sigma(x)}L_i + b_i, \qquad \bar{L}_{ij} = e^{\sigma(x)}L_{ij}, \qquad \bar{L}_{ijk} = e^{\sigma(x)}L_{ijk}, \tag{3.2}$$

under this change we put

$$\bar{G}^i = G^i + D^i, \qquad \bar{G}^i_j = G^i_j + D^i_j, \qquad \bar{G}^i_{jk} = G^i_{jk} + D^i_{jk}, \tag{3.3}$$

where $D^i_j = \dot{\partial}_j D^i$ and $D^i_{jk} = \dot{\partial}_k D^i_j$.

To find D^i explicitly, we deal with the equations $L_{ij|k} = 0$ where $L_{ij|k}$ is the h-covariant derivative of $L_{ij} = h_{ij}$ in Cartan connection $C\Gamma$.

Since

$$L_{ij|k} = \partial_k L_{ij} - L_{ijr}G^r_k - L_{rj}F^r_{ik} - L_{ri}F^r_{jk},$$

therefore $L_{ij|k} = 0$ gives the equation

$$\partial_k L_{ij} = L_{ijr}G^r_k + L_{rj}F^r_{ik} + L_{ri}F^r_{jk}, \tag{3.4}$$

$$\partial_k \bar{L}_{ij} = \bar{L}_{ijr}\bar{G}^r_k + \bar{L}_{rj}\bar{F}^r_{ik} + \bar{L}_{ri}\bar{F}^r_{jk}, \tag{3.5}$$

Therefore from (3.3) above equations become

$$\partial_k \bar{L}_{ij} = \bar{L}_{ijr}(G^r_k + D^r_k) + \bar{L}_{rj}(F^r_{ik} + D^r_{ik}) + \bar{L}_{ri}(F^r_{jk} + D^r_{jk}),$$

where D^i_{jk} is the differences between Cartan coefficients i.e

$$\bar{F}^i_{jk} - F^i_{jk} = D^i_{jk},$$

which gives

$$L_{ij}\sigma_k = L_{ijr}D^r_{jk} + L_{rj}D^r_{ik} + L_{ri}D^r_{jk}, \tag{3.6}$$

where $\sigma_k = \frac{\partial \sigma}{\partial x^k}$.

Contracting above equations by y^k, we get

$$L_{ij}\sigma_k y^k = L_{ijr}D^r_{j0} + L_{rj}D^r_{j0} + L_{ri}D^r_{j0},$$

and dealing with $\bar{L}_{i|j} = 0$, which is equivalent to

$$\partial_j \bar{L}_i = \bar{L}_{ir}\bar{G}^r_j - \bar{L}_r\bar{F}^r_{ij}.$$

Then

$$\partial_j \bar{L}_i = \bar{L}_{ir}(G^r_j + D^r_j) - \bar{L}_r(F^r_{ij} + D^r_{ij}) = 0, \tag{3.7}$$

gives

$$\sigma_j e^\sigma L_i + b_{i|j} = e^\sigma L_{ir}D^r_j + \bar{L}_r D^r_{ij}, \tag{3.8}$$

The above equation is equivalent to a two equations, given as

$$2E_{ij} = e^\sigma(L_{ir}D^r_j + L_{jr}D^r_i) + 2\bar{L}_r D^r_{ij} - e^\sigma\sigma_{ij}, \tag{3.9}$$

$$2F_{ij} = e^\sigma(L_{ir}D^r_j - L_{jr}D^r_i) + e^\sigma\mu_{ij}, \tag{3.10}$$

where

$$\sigma_{ij} = \sigma_j L_j + \sigma_i L_i, \qquad \mu_{ij} = \sigma_j L_j - \sigma_i L_i.$$

Contracting equation (3.9) by y^j, we get

$$e^\sigma L_{ir}D^r + 2\bar{L}_r D^r_{0i} = 2E_{0i} + e^\sigma(\sigma_0 L_i + \sigma_i L), \tag{3.11}$$

where $\sigma_0 = \sigma_j y^j$ and similarly from (3.10), we get

$$e^\sigma L_{ir}D^r = 2F_{0i} + e^\sigma(\sigma_0 L_i - \sigma_i L). \tag{3.12}$$

Again on contracting by y^i to equation (3.11), we get

$$\bar{L}_r D^r = E_{00} + e^\sigma(\sigma_0 L). \tag{3.13}$$

The equation (3.12) and (3.13) can be written as a system of algebraic equation in D^r as

$$L_{ir}D^r = 2e^{-\sigma}F_{i0} + (\sigma_0 Li - \sigma_i L) = B_i,$$

$$\bar{L}_r D^r = E_{00} + e^\sigma\sigma_0 L = B. \tag{3.14}$$

By applying Lemma 2.1 on the system of equations (3.14) and noting that $B_i y^i = 0$, we obtain an explicit expression for the difference tensor D^r_{00} as

$$D^r = 2Le^{-\sigma}F^r_0 + \frac{L(E_{00} - 2Le^{-\sigma}F_{\beta 0})y^r}{\bar{L}} - L^2\sigma^r + \frac{L(2Le^\sigma\sigma_0 + L^2\sigma_\beta)y^r}{\bar{L}}, \tag{3.15}$$

where $\sigma_\beta = \sigma_i b^i$, $F^r_0 = g^{ir}F_{i0}$ and $F_{\beta 0} = F_{i0}b^i$. Thus we have the following:

Proposition 3.1. *The tensor D^i of (3.2) arising from a β-Conformal change are given by*

$$D^r = 2Le^{-\sigma}F_0^r + \frac{L(E_{00} - 2Le^{-\sigma}F_{\beta 0})y^r}{\bar{L}} - L^2\sigma^r + \frac{L(2Le^{\sigma}\sigma_0 + L^2\sigma_\beta)y^r}{\bar{L}}.$$

Now from (3.3) and (3.15), we have

$$\bar{G}^i y^j - \bar{G}^j y^i = G^i y^j - G^j y^i + 2Le^{-\sigma}(F_0^i y^j - F_0^j y^i) - L^2(\sigma^i y^j - \sigma^j y^i). \tag{3.16}$$

Suppose that (M^n, L) is a Douglas space, i.e, $G^i y^j - G^j y^i$ are positively homogeneous of degree three, then we have

Proposition 3.2. *Let $F^n = (M^n, L)$ be a Douglas space and $\bar{F}^n = (M^n, \bar{L})$ ba a Finsler space which is obtained by β-Conformal change of Finsler metric L, Then $\bar{F}^n$ remains a Douglas space if and only if $2Le^{-\sigma}(F_0^i y^j - F_0^j y^i)$ are positively homogeneous of degree three.*

Here, we consider β-Conformal change of Kropina and generalized Kropina metric.

4 Kropina Space

Let $F^n = (M^n, L)$ be a Kropina space with metric $L = \frac{\alpha^2}{\beta}$ and $\bar{F}^n = (M^n, \bar{L})$ ba a Finsler space which is obtained by β-Conformal change of Finsler space $F^n = (M^n, L)$, from equation (3.1) we get

$$\bar{B}^{ij} = B^{ij} + \frac{\beta e^{-\sigma}(s_0^i y^j - s_0^j y^i)}{2} - \frac{s_0 \beta e^{-\sigma}(b^i y^j - b^j y^i)}{2b^2}. \tag{4.1}$$

Suppose F^n is a Douglas space, then B^{ij} are positively homogeneous of degree three, then the necessary and sufficient condition for Finsler space $\bar{F}^n$ to be a Douglas space is

$$\frac{\beta e^{-\sigma}(s_0^i y^j - s_0^j y^i)}{2} - \frac{s_0 \beta e^{-\sigma}(b^i y^j - b^j y^i)}{2b^2}, \tag{4.2}$$

which is also positively homogeneous of degree three. Hence we have the following

Proposition 4.1. *Let $F^n = (M^n, L)$ be a Finsler space with an (α, β)-metric of Douglas type.Then $\bar{F}^n = (M^n, \bar{L})$ which is obtained by β-Conformal change of Finsler metric is also a Douglas space if and only if*

$$W^{ij} = \frac{\beta e^{-\sigma}(s_0^i y^j - s_0^j y^i)}{2} - \frac{s_0 \beta e^{-\sigma}(b^i y^j - b^j y^i)}{2b^2} \tag{4.3}$$

are positively homogeneous of degree three.

Since B^{ij} and W^{ij} are positively homogeneous of degree three, $\bar{B}^{ij}$ are also positively homogeneous of degree three i.e $\bar{F}^n$ is a Douglas space. Thus a Kropina space F^n is of Douglas type,then a Finsler space $\bar{F}^n$ which is obtained by β-Conformal change of F^n is of Douglas type also. We consider the condition for a Finsler space which is obtained by a β-Conformal change of a Kropina space to be of Douglas type. For $\bar{F}^n = (M^n, \bar{L})$ equation (2.10) gives

$$\bar{B}^{ij} = \frac{(\beta^2 - e^{\sigma}\alpha^2)(s_0^i y^j - s_0^j y^i)}{2\beta e^{\sigma}} - \frac{\{r_{00}\beta - s_0(\beta^2 - e^{\sigma}\alpha^2)\}(b^i y^j - b^j y^i)}{2b^2 e^{\sigma}\beta}. \tag{4.4}$$

Since the terms

$$\frac{\beta e^{-\sigma}(s_0^i y^j - s_0^j y^i)}{2} + \frac{e^{-\sigma}(r_{00} - s_0\beta)(b^i y^j - b^j y^i)}{2b^2}$$

are positively homogeneous of degree three, then we neglect these terms from the discussion and we treat only of

$$\bar{W}^{ij} = \frac{\alpha^2\{\frac{s_0(b^i y^j - b^j y^i)}{b^2} - (s_0^i y^j - s_0^j y^i)\}}{2\beta}. \tag{4.5}$$

For $(n > 2)$, and $\alpha^2 \not\equiv 0 (mod \beta)$ [13]. There exists a positively homogeneous function of degree one $v^{ij} = v_k^{ij} y^k$ such that

$$\frac{s_0(b^i y^j - b^j y^i)}{b^2} - (s_0^i y^j - s_0^j y^i) = \beta v^{ij}, \tag{4.6}$$

from which, we get

$$\frac{\{b^i(s_h\delta_k^j + s_k\delta_h^j - i/j)\}}{b^2} - (s_h^i\delta_k^j + s_k^i\delta_h^j - i/j) = b_h v_k^{ij} + b_k v_k^{ij}. \tag{4.7}$$

Transvection of (4.7) by a^{hk} leads to

$$\frac{(b^i s^j + b^j s^i)}{b^2} - 2s^{ij} = b^r v_r^{ij}. \tag{4.8}$$

Next, transvecting (4.7) by b^h, we have

$$(s_i\delta_k^j + b^i s_k^j - i/j) = b^2 v_k^{ij} + b_k b^r v_r^{ij}. \tag{4.9}$$

Again contracting of (4.7) with $j = h$, we obtain

$$n(\frac{b^i s_k}{b^2} - s_k^i) = b_r v_k^{ir} - b_k v_r^{ir}. \tag{4.10}$$

Substituting $b^r v_r^{ij}$ of (4.8) in (4.9), we have

$$b^2 v_k^{ij} = 2s^{ij}b_k + \{b^i s_k^j - b^j s_k^i + s^i\delta_k^j - s^j\delta_k^i + \frac{(s^i b^j b_k - s^j b^i b_k)}{b^2}\},$$

which implies

$$b^2 v^i r_r = (n-1)s^i,$$
$$b^2 b_r v_r^{ir} = b^i s_k - b^2 s_k^i.$$

Consequently (4.9) leads to

$$s_{ij} = \frac{(b_i s_j - b_j s_i)}{b^2}. \tag{4.11}$$

Then (4.5) gives

$$\bar{W}^{ij} = \frac{\alpha^2(s^i y^j - s^j y^i)}{2b^2}, \tag{4.12}$$

which are positively homogeneous of degree three. Therefore (4.11) is the necessary and sufficient condition for $\bar{F}^n$ to be Douglas type. On the other hand, it is known that a Kropina space F^n $(n > 2)$ with $b^2 \neq 0$ is of Douglas type if and only if (4.10) is satisfied. Thus we have the

Theorem 4.1. *A Finsler space $\bar{F}^n$ $(n > 2)$ which is obtained by β-Conformal change of a Kropina space with $b^2 \neq 0$ is of Douglas type if and only if the Kropina space F^n is also a Douglas type.*

5 Generalized Kropina spaces

In this section, we deal with a Finsler space (M^n, L) $(n > 2)$ with a generalized Kropina metric $L = \frac{\alpha^{1+m}}{\beta^m}$ where m is a constants $m \neq 0, -1$. We consider the condition for a Finsler space $\bar{F}^n = (M^n, e^\sigma L + \beta)$ which is a β-Conformal change of a generalized Kropina space $F^n = (M^n, \frac{\alpha^{1+m}}{\beta^m})$ to be of Douglas type.

Theorem [8] has been known that a generalized Kropina space is a Douglas space, where $\alpha^2 \neq 0(mod\beta)$ if and only if $b_{i;j}$ are given by $b_{i;j} = r_{ij} + s_{ij}$ where

$$s_{ij} = \frac{(b_i s_j - b_j s_i)}{b^2} \tag{5.1}$$

and

$$r_{ij} = \frac{k(x)((1-m)b_i b_j + mb^2 a_{ij})}{m(1+m)} + \frac{(1-m)(s_i b_j - s_j b_i)}{b^2(1+m)}. \tag{5.2}$$

For $\bar{F}^n$ equation (2.10) gives

$$2\{(1-m)\beta^2 + mb^2\alpha^2\}\{(1+m)\beta\bar{B}^{ij} + (m\alpha^2 - e^{-\sigma}\alpha^{1-m}\beta^{1+m})(s_0^i y^j - s_0^j y^i)\} -$$
$$m\alpha^2\{(1+m)r_{00}\beta + 2s_0(m\alpha^2 - e^{-\sigma}\alpha^{1-m}\beta^{1+m})\}(b^i y^j - b^j y^i) = 0, \tag{5.3}$$

which is equivalent to

$$2\{(1-m)\beta^2 + mb^2\alpha^2\}\{(1+m)\beta\bar{B}^{ij} + m\alpha^2(s_0^i y^j - s_0^j y^i)\} - m\alpha^2\{(1+m)r_{00}\beta + 2ms_0\alpha^2\}(b^i y^j - b^j y^i$$
$$-2e^{-\sigma}\alpha^{1-m}\beta^{1+m})[\{(1-m)\beta^2 + mb^2\alpha^2\}(s_0^i y^j - s_0^j y^i) - ms_0\alpha^2(b^i y^j - b^j y^i)] = 0. \tag{5.4}$$

Now we divide this consideration into two cases as follow;

Case (I) $\alpha^{1-m}\beta^{1+m}$ is rational in (y^i) i.e, m is an odd integer.
Case (II) $\alpha^{1-m}\beta^{1+m}$ is irrational in (y^i) i.e, m is the others.

Case(I): First we take $m \leq 1$, where m is an odd integer, Multiplication (5.3) by β^{-m-1}, we get

$$2\{(1-m)\beta^2 + mb^2\alpha^2\}\{(1+m)\beta^{-m}\bar{B}^{ij} + (m\alpha^2\beta^{-1-m} - e^{-\sigma}\alpha^{1-m})(s_0^i y^j - s_0^j y^i)\}$$
$$-m\alpha^2\{(1+m)r_{00}\beta + 2s_0(m\alpha^2\beta^{-1-m} - e^{-\sigma}\alpha^{1-m})\}(b^i y^j - b^j y^i) = 0. \tag{5.5}$$

Since $\bar{B}^{ij}$ are supposed to be positively homogeneous of degree three. The term in equation (5.5) which does not contain α^2 is $2(1-m^2)\beta^{2-m}\bar{B}^{ij}$ and hence, we must have a term $u^{ij}_{(3-m)}$ which are positively homogeneous of degree $(3-m)$, such that

$$2(1-m^2)\beta^{2-m}\bar{B}^{ij} = \alpha^2 u^{ij}_{3-m}. \tag{5.6}$$

We take the general case $\alpha^2 \not\equiv 0(mod\beta)$. From equation (5.6) it shows that there exist $hp(1)$ u^{ij} satisfying $u^{ij}_{3-m} = \beta^{2-m}u^{ij}$. Then (5.6) becomes

$$2(1-m^2)\bar{B}^{ij} = \alpha^2 u^{ij}. \tag{5.7}$$

If $m \neq 1$ i.e F^n is not a Kropina space , then (5.7) gives $\bar{B}^{ij}$ and (5.5) can be rewritten in the form of

$$\{(1-m)\beta^2 + mb^2\alpha^2\}\{\frac{\beta^{-m}v^{ij}}{(1-m)} + 2(m\beta^{-1-m} - e^{-\sigma}\alpha^{-1-m})(s_0^i y^j - s_0^j y^i)\}$$
$$-m\{(1+m)r_{00}\beta^{-m} + 2s_0(m\alpha^2\beta^{-1-m} - e^{-\sigma}\alpha^{1-m})\}(b^i y^j - b^j y^i) = 0. \tag{5.8}$$

Collecting the terms of (5.8) which does not contains β, we can put $2m\alpha^{1-m}e^{-\sigma}\{b^2(s_0^i y^j - s_0^j y^i) - s_0(b^i y^j - b^j y^i)\} = \beta v^{ij}_{2-m}$ where v^{ij}_{2-m} are positively homogeneous of degree $(2-m)$.

Consequently, we have

$$b^2(s_0^i y^j - s_0^j y^i) - s_0(b^i y^j - b^j y^i) = \beta v^{ij} \tag{5.9}$$

and $v^{ij}_{2-m} = 2me^{-\sigma}\alpha^{1-m}v^{ij}$ with $hp(1)$ v^{ij}. Thus (5.8) is reduced to

$$\{(1-m)\beta^2 + mb^2\alpha^2\}\frac{\beta^{-m}v^{ij}}{(1-m)} + 2m^2\alpha^2\beta^{-m}v^{ij} + 2\{m(1-m)\beta^{1-m} - e^{-\sigma}\alpha^{-1-m}\{(1-m)\beta^2 + mb^2\alpha^2\}\}$$
$$(s_0^i y^j - s_0^j y^i)\} - m\{(1+m)r_{00}\beta^{-m} + 2s_0\alpha^{1-m}e^{-\sigma}\}(b^i y^j - b^j y^i) = 0. \tag{5.10}$$

Also from (5.9) we obtain

$$b^2 s_{ij} = b_i s_j - b_j s_i, \tag{5.11}$$

provided that $b^2 \neq 0$.

Thus from equation (5.11) equation (5.9) is reduced to $v^{ij} = y^i s^j - y^j s^i$ and (5.10) is rewritten in the form of

$$\{(1-m)\beta^2 + mb^2\alpha^2\}\{\frac{\beta^{-m}u^{ij}}{(1-m)} + \frac{2(m\beta^{-m} - e^{-\sigma}\alpha^{-1-m}\beta)(s_0^i y^j - s_0^j y^i)}{b^2}\}+$$
$$\{\frac{2m(1-m)\beta^{1-m} - 2\alpha 1 - me^{-\sigma}\{(1-m)\beta^2 + mb^2\alpha^2\}s_0}{b^2}$$
$$-m\{(1+m)r_{00}\beta^{-m} - 2s_0\alpha^{1-m}e^{-\sigma}\}\}(b^i y^j - b^j y^i) = 0. \tag{5.12}$$

Multiplying above equation by β^m, we obtain

$$\{(1-m)\beta^2 + mb^2\alpha^2\}\{\frac{u^{ij}}{(1-m)} - 2(m - e^{-\sigma}\alpha^{-1-m}\beta^{1+m})(s^i y^j - s^j y^i)\}+$$
$$\{\frac{2m(1-m)\beta - 2\alpha - 1 - m\beta^m e^{-\sigma}\{(1-m)\beta^2 + mb^2\alpha^2\}s_0}{b^2}$$
$$-m\{(1+m)r_{00}\beta^{-m} - 2s_0\alpha^{1-m}\beta^m e^{-\sigma}\}\}(b^i y^j - b^j y^i) = 0. \tag{5.13}$$

Transvestite above equation by $b_i s_j$, we have

$$\{(1-m)\beta^2 + mb^2\alpha^2\}\{\frac{u^{ij}b_i s_j}{(1-m)} + \frac{2(m - e^{-\sigma}\alpha^{-1-m}\beta^{1+m})s^j s_j\beta}{b^2}\}$$
$$= \{m\{(1+m)r_{00} - 2s_0\alpha^{1-m}\beta^m e^{-\sigma}\} - 2\frac{[(1-m)m\beta - e^{-\sigma}\alpha^{-1-m}\beta m\{(1-m)\beta^2 + mb^2\alpha^2\}s_0]}{b^2}\}b^2 s_0.$$

Suppose that there exist $u = u_i(x)y^i$ such that $(1-m)\beta^2 + mb^2\alpha^2 = b^2 s_0 u$. Then it is written in form

$$2\{(1-m)\beta_i\beta_j + \ + mb^2a_{ij}\} = b^2(s_iu_j + s_ju_i). \tag{5.14}$$

Contracting by b^ib^j gives $b^2 = 0$ which is a contradiction . Therefore (5.14) shows that, we have a function $h_1(x)$ satisfying

$$\frac{u^{ij}b_is_j}{(1-m)} + \frac{2(m - e^{-\sigma}\alpha^{-1-m}\beta^{1+m})s^js_j\beta}{b^2} = h_1(x)b^2s_0\{\{m(1+m)r_{00} - 2me^{-\sigma}s_0\alpha^{1-m}\beta^m\}$$
$$-\frac{2\{m(1-m)\beta - e^{-\sigma}\alpha^{-1-m}\beta^m\{(1-m)\beta^2 + mb^2\alpha^2\}\}s_0}{b^2}\}s_0 = \{(1-m)\beta^2 + mb^2\alpha^2\}h_1(x)s_0.$$

If $s_0 \neq 0$, then we get from the latter equation

$$r_{00} = \frac{h_1(x)\{(1-m)\beta^2 + mb^2\alpha^2\}}{m(1+m)} + \frac{2(1-m)s_0\beta(m - e^{-\sigma}\alpha^{-1-m}\beta^{1+m})}{m(1+m)b^2}. \tag{5.15}$$

Thus (5.13) gives u^{ij} of the form

$$u^{ij} = \frac{2(1-m)(m - e^{-\sigma}\alpha^{-1-m}\beta^{1+m})(s^iy^j - s^jy^i)}{b^2} + h_1(x)(1-m)(b^iy^j - b^jy^i). \tag{5.16}$$

Since r_{00} is $hp(2)$ from (5.15), $\alpha^{-1-m}\beta^{1+m}$ must be $hp(0)$. The condition for $\alpha^{-1-m}\beta^{1+m}$ to be $hp(0)$ is $m = -3$. Thus substituting $m = -3$ in (5.15), we have

$$r_{00} = \frac{h_1(x)\{4\beta^2 - 3b^2\alpha^2\}}{6} - \frac{4s_0(3\beta^2 + e^{-\sigma}\alpha^2)}{3b^2\beta}, \tag{5.17}$$

equation (5.17) shows that, there exists $h_2(x)$ satisfying $s_0 = h_2(x)\beta$. Then (5.17) is reduced to

$$r_{ij} = (\frac{2h_1(x)}{3} - \frac{4h_2(x)}{b^2})b_ib_j - (\frac{b^2h_1(x)}{2} + \frac{4h_2(x)e^{-\sigma}}{3b^2})a_{ij}, \tag{5.18}$$

i.e (5.2). If s_0 is assumed to vanish, then (5.11) gives $s_{ij} = 0$ and (5.13) is reduced to

$$\{(1-m)\beta^2 + mb^2\alpha^2\}u^{ij}b_iy_j = m(1-m)r_{00}(b^2\alpha^2 - \beta^2).$$

It is easily verified that $\{(1-m)\beta^2 + mb^2\alpha^2\}(= m\gamma^2 + \beta^2)$ is not contained in $(b^2\alpha^2 - \beta^2 = \gamma^2)$. Consequently, it is contained in r_{00}, therefore there exists a function $h_3(x)$ such that $r_{00} = h_3(x)\{(1-m)\beta^2 + mb^2\alpha^2\}$. Therefore (5.18) also holds in this cases.

Next we consider $m > 1$, on multiplying equation (5.3) by α^{-1+m} gives $s_0 = 0$ and $s_{ij} = 0$. Thus we get $r_{00} = h_3(x)\{(1-m)\beta^2 + mb^2\alpha^2\}$ is common with $s_0 = 0$. Thus (5.18) is also holds.

Case $-$ **(II)** : Since $\alpha^{1-m}\beta^{m+1}$ is irrational in (y^i), (5.4) is divided in two equations as follows;

$$2\{(1-m)\beta^2 + mb^2\alpha^2\}\{(1+m)\beta\bar{B}^{ij} + m\alpha^2(s_0^iy^j - s_0^jy^i)\}$$
$$-m\alpha^2\{(1+m)r_{00}\beta + 2ms_0\alpha^2\}(b^iy^j - b^jy^i) = 0, \tag{5.19}$$
$$\{(1-m)\beta^2 + mb^2\alpha^2\}(s_0^iy^j - s_0^jy^i) - ms_0\alpha^2(b^iy^j - b^jy^i) = 0. \tag{5.20}$$

Transvecting (5.20) by b_iy_j, we get

$$\{(1-m)\beta^2 + mb^2\alpha^2\}(s_0^ib_i\alpha^2 - s_0^jy^j\beta) - ms_0\alpha^2(b^2\alpha^2 - \beta^2) = 0,$$

which gives

$$s_0\alpha^2\beta^2 = 0.$$

Hence we get $s_0 = 0$ i.e $s_i = 0$. Then (5.20) becomes

$$(s_0^iy^j - s_0^jy^i) = 0.$$

Transvection above by y_j gives

$$s_0^i = 0.$$

Therefore $s_{ij} = 0$, putting in (5.19), we get

$$2\{(1-m)\beta^2 + mb^2\alpha^2\}\bar{B}^{ij} - m\alpha^2r_{00}(b^iy^j - b^jy^i) = 0. \tag{5.21}$$

The term in (5.21) which does not contain α^2 is $2(1-m)\beta^2\bar{B}^{ij}$ and hence we must have u_3^{ij} positively homogeneous of degree three, satisfying

$$2(1-m)\beta^2\bar{B}^{ij} = \alpha^2u_3^{ij}. \tag{5.22}$$

Suppose $\alpha^2 \not\equiv 0(mod\beta)$. Then (5.22) is reduced to $\bar{B}^{ij} = \alpha^2 u^{ij}$ where u^{ij} are homogeneous polynomial of degree one. Hence (5.21) leads to

$$2\{(1-m)\beta^2 + mb^2\alpha^2\}u^{ij} - r_{00}(b^i y^j - b^j y^i) = 0. \tag{5.23}$$

Transvecting (5.23) by $b_i y_j$, we obtain

$$2\{(1-m)\beta^2 + mb^2\alpha^2\}u^{ij}b_i y_j - r_{00}(b^i y^j - b^j y^i)b_i y_j = 0,$$
$$2\{(1-m)\beta^2 + mb^2\alpha^2\}u^{ij}b_i y_j - r_{00}(b^2\alpha^2 - \beta^2) = 0.$$

Thus there exists a function $h_4(x)$ such that

$$2(1-m)u^{ij}b_i y_j - r_{00} = h_4(x)\alpha^2,$$
$$2mb^2 u^{ij}b_i y_j - r_{00}b^2 = h_4(x)\beta^2.$$

On eliminating $u^{ij}b_i y_j$ from above equations, we get

$$b^2 r_{00} = h_4(x)\{(m-1)\beta^2 - mb^2\alpha^2\},$$

which implies that

$$r_{ij} = \frac{h_4(x)\{(m-1)\beta^2 - mb^2 a_{ij}\}}{b^2}. \tag{5.24}$$

From $s_{ij} = 0$ and (5.24), we obtain

$$b_{i|j} = h_5(x)\{(m-1)b_i b_j - mb^2 a_{ij}\}, \tag{5.25}$$

where $h_5(x) = \frac{h_4(x)}{b^2}$.

Consequently if (5.25) is satisfied, then $s_{ij} = 0$ and

$$r_{00} = h_5(x)\{(m-1)\beta^2 - mb^2\alpha^2\},$$

from which $\bar{B}^{ij}$ of (5.4) are homogeneous polynomialS of degree three. Hence in this case (5.18) also holds.

In any case we obtain $b_{i|j}$ by (5.11) and (5.18), then $\bar{B}^{ij}$ are given by (5.7) together with (5.16). Consequently a Finsler space $\bar{F}^n = (M^n, e^\sigma L + \beta)$ $(n > 2)$ with a non-zero b^2 which is obtained by β-Conformal change of a generalized Kropina space $F^n = (M^n, L = \frac{\alpha^{1+m}}{\beta^m}, m \neq \pm 1, 0)$ is a Douglas space if and only if $b_{i|j}$ are given (5.11) and (5.18) i.e (5.1) and (5.2) hold.

On the other hand, it has been known [8] that a generalized Kropina space F^n $(n > 2)$ with non zero b^2 is a Douglas space if and only if $b_{i|j}$ are given by (5.1) and (5.2). That is to say that the case $s_0 \neq= 0$ for F^n to be a Douglas space corresponds to the case $m = -3$ for $\bar{F}^n$ to be a Douglas space and the case $s_0 = 0$ for F^n to be of Douglas type corresponds to the case $m \neq -3$, $m \epsilon R$ for $\bar{F}^n$ to be of Douglas type. Thus we obtain the following

Theorem 5.1. *Let F^n $(n > 2)$ ba a generalized Kropina space with $L = \frac{\alpha^{1+m}}{\beta^m}$,m being a constant $\neq \pm 1, 0$. A Finsler space $\bar{F}^n$ which is obtained by a β-Conformal change of F^n with non-zero b^2 of Douglas type is also of Douglas type and vice-versa.*

Acknowledgement. Authors are thankful to the Editor and Reviewer for their valuable suggestions to improve the presentation of the paper.

References

[1] S. H. Abed, Conformal β-changes in Finsler spaces, *Proc. Math. Phys. Soc. Egypt.* ArXiv No:math.DG/0602404.

[2] P.L. Antonelli, R.S. Ingarden, and M.Matsumoto, *The theory of sprays and Finsler spaces with applications in physics and biology*, Kluwer Acad. Dordecht, 1993.

[3] S. Bacso and M. Matsumoto, On the Finsler spaces of Douglas type. A generalization of the notion of Berwald space, *Publ. math. Debrecen,* **51** (1997), 385-406.

[4] S. A. Baby and G. Shankar, On Conformal Change of Douglas Spaces of second kind with special (α, β)-metric , *AIP Conf. Proc.,* **2261**(1) (2020),030011.

[5] M. Hashiguchi, On conformal transformations of Finsler spaces, *J. Math. Kyoto Univ.,* **16**(1) (1976), 25-50.

[6] H. Izumi, Conformal transformations of Finsler spaces I, *Tensor(N.S),* **31** (1977), 33-41.

[7] Ii Yong Lee, Douglas spaces of the second kind of Finsler space with Matsumoto metric, *Journal of the Chungcheong Mathematical Society,* **21**(2) (2008), 209-220.
[8] M. Matsumoto, Finsler space with (α, β)-metric of Douglas type, *Tensor(N.S)* **60** (1998), 123-134.
[9] M. Matsumoto, *Foundation of Finsler Geometry and Special Finsler spaces,*, Kaiseisha Press, Otsu Saikawa. **(**1986).
[10] V.S. Matveev and Samanes Saberali, Conformally related Douglas metrics in dimension two are Randers, *Arch. Math.,* **116** (2021), 221-231.
[11] B. N. Prasad and Kumari Bindu, The β- Change of Finsler metric and imbedding Classes of their tangent spaces, Tensor(N.S) **74** (2013), 48-59.
[12] R. Ranjan, P.N. Pandey and Ajit Paul, Conformal transformation of Douglas spaces of second kind with special (α, β)-metric, *Arab Journal of Mathematical Sciences,* **30**(2) (2024), 150-160.
[13] C. Shibata, and M. Azuma, C-conformal invariant and tensors of Finsler metrics, *Tensor(N.S),* **52** (1993), 76-81.
[14] N. L. Youssef, S. H. Abed and A. Soleiman, Conformal transformations of Finsler spaces I, *Tensor(N.S),* **31** (1977), 33-41.

ISSN 0304-9892 (Print) ISSN 2455-7463 (Online)

Jñānābha

Statement of ownership and particulars about the journal

1.	Place of Publication	D.V. Postgraduate College Orai-285001, U.P., India
2.	Periodicity of Publication	Bi-annual
3.	Printer's Name Nationality Address	Creative Laser Graphics (Iqbal Ahmad) Indian IIT Gate, Kanpur
4.	Publisher's Name	Dr. R.C. Singh Chandel For Vijñāna Parishad of India
	Nationality Address	Indian D.V. Postgraduate College Orai-285001, U.P. India
5.	Editor's Name Nationality Address	Dr. R.C. Singh Chandel Indian D.V. Postgraduate College Orai-285001, U.P. India
6.	Name and Address of the individuals who own the journal and partners of share holders holding more than one percent of the total capital	**Vijñāna Parishad of India** Address: D.V. Postgraduate College Orai-285001, U.P. India

I, *Dr. R. C. Singh Chandel* hereby declare that the particulars given above are true to the best of my knowledge and belief.

Dr. R.C. Singh Chandel
Publisher/Editor
rc_chandel@yahoo.com

INSTRUCTIONS TO AUTHORS / REVIEWERS / SUBSCRIBERS

1. 'Jñānābha' is published annually since 1971. Effective with Vol. 47 (2017) it is bi-annual published in (June and December). Since 1971, its content is available in hard copy as well as on its website http://www.vijnanaparishadofindia.org/jnanabha.
2. APC (Article Processing Charge) is no longer requirement for publication in 'Jñānābha'.
3. It is interdisciplinary journal devoted primarily to research articles in all areas of mathematical and physical sciences; it does, however, encourage original mathematical works which are motivated by and relevant to applications in the social, management, mathematical or engineering sciences. Papers intended for publication in this journal should be in typed form or offset-reproduced (not dittoed), A4 size double spaced with generous margin and they may be written in Hindi or English. Manuscripts (soft copy typed in MS Word/La-TeX, mentioning 2020 Mathematical Sciences Classification, Keywords and authors postal and E-mail addresses also on front page strictly in the format of 'Jñānābha', may be submitted to either of the Editors). It is mandatory for every author in 'Jñānābha' to be member of 'Vijñāna Parishad of India' in good standing.

   The submission of the paper implies the author's assurance that the paper that has not been widely circulated, copyrighted, published or submitted for publication elsewhere.

   Authors are advised to submit only neatly (and carefully) type written and thoroughly checked manuscripts employing accepted conventions of references, notations, displays, etc.; all typescripts not in a format suitable to publication in this journal will be returned unrefereed.
4. **La-TeX Template:** La-TeX template is available here to facilitate adherence to publication 'Jñānābha' standards.
5. **Information for Reviewers/Members on Editorial Board.** Members on Editorial Board are responsible to review the papers of their field or to get reviewed by other suitable reviewers of their field that paper is original and publishable in any standard International Journal and is strictly in the format of JÑĀNĀBHA having correct language and proper methodology.
6. Effective Vol. 52 the price per volume is Rs. 1200.00 (or US $ 50.00). Individual members of Vijñāna Parishad of India are entitled to free subscription to the current issues of this journal. Individual membership: Rs. 500.00 (or US $ 40.00) per calendar year; Life membership: Rs. 4000.00 (or US $ 400.00). Back volumes are available at special price. (Payments of dues by cheques must include approximate bank charges).For online payment, visit http://www.vijnanaparishadofindia.org.

   [By a reciprocity agreement with the American Mathematical Society, an individual /life member of the Parishad residing outside North American continent may join the Society by submitting an application for membership on the form that may be obtained from the office of the Society **(P.O. Box 6248, Providence, Rhode 02940, USA)** and by paying the society's current dues as a reciprocity member at a considerably reduced rate; the usual requirements that the applicant be endorsed by two members of the Society and that the candidate be elected by the Council are waived, but this reduction in dues to the Society does not apply to those individual/life members of the Parishad who reside , even on temporary basis, in the North American area(i.e. USA and Canada)]

   The mathematical content of this journal is reviewed among others by **Zentralblat für Mathematk (Germany).**

   It is also indexed in Indian Citation Index (www.indiancitation index.com), Google Scholar (https://scholar.google.com). One may also visit dmr.xml-MathSciNet-American Mathematical Society http://www.mathscinetams.org/dmr/dmrxml. **Jñānābha is included in Serials covered by Zentralblatt Math, Romanian Unit** http://www.zbl.theta.ro/too/zs/j.html.

   Papers published in Jñānābha have their own DOI: htpps://doi/10.58250/jnanabha.

   All communications regarding subscriptions, order of back volumes, membership of Vijñāna Parishad of India, change of address, etc. and all books for review, should be addressed to:

The Secretary
Vijñāna Parishad of India
D.V. Postgraduate College, Orai- 285001, UP, India
E-Mail: rc_chandel@yahoo.com
Jñānābha –Vijñāna Parishad of India

CONTENTS