International Journal of Advanced Trends in Engineering and Management
(ISSN 2583-7052)

pp. 53-56, April

On Solving Application of Non-Singular Matrices in Cryptography in Intuitionistic Fuzzy Pentagonal Number

S. Uma[1], S. Sathya[2]

[1]Department of Science and Humanities, A.V.C. College of Engineering, Mayiladuthurai, Tamil Nadu-609305, India.

[2]Department of Science and Humanities, A.V.C. College of Engineering, Mayiladuthurai, Tamil Nadu-609305, India.

Corresponding Author E-mail: umamurali100@gmail.com

ABSTRACT: Using pentagonal intuitionistic fuzzy numbers and assuming α and β cut values, the idea of modified arithmetic operations on interval valued intuitionistic fuzzy numbers is used to solve interval valued non-singular matrices in cryptography. Information protection has always depended on the study of cryptography, or the encoding of messages in secret codes. The basic idea behind cryptography is that data can be encrypted so that anyone who knows how to do so can decrypt it. Lastly, a numerical example was suggested.

Keywords: A Fuzzy number, Pentagonal intuitionistic fuzzy number, Value and Ambiguity indexes, Ranking method, Inverse, which means matrices, encryption, and cryptography.

1. Introduction

People from all around the world use the internet to communicate on a daily basis. It is essential to keep our sensitive data safe from unauthorized access. How to protect data from unauthorized change is the primary concern in data transfer. One of the most common and harmful kinds of attacks is unauthorized access to read, change, and delete data. Data transferred between systems over a public network can be protected via encryption. Every encryption creates a cipher text that can be decoded into plaintext. The lengthy and rich history of cryptology includes a number of fascinating basic cipher schemes that allow for a more thorough investigation of different mathematical problems. Several works use and improve matrix cryptography in an effort to address this security issue [11]. The key matrix and its inverse are required for encryption and decryption, respectively [1] [2]. But what happens if there is no inverse of the matrix? How does the decryption procedure operate otherwise? To get around all of the issues listed above, several non-singular matrices in orthogonal, Hilbert, and quadratic forms have been employed in the past. Fuzzy data must be handled and evaluated in order to make decisions in many real-world situations. Atanssov introduced fuzzy sets as a notation [3, 4]. Since its inception, the intuitionistic fuzzy set (IFS) has drawn increasing interest due to the fact that attribute value information is typically ambiguous or fuzzy. This work assumes interval valued intuitionistic fuzzy numbers [10] and pentagonal intuitionistic fuzzy numbers [PIFNS], as well as α and β cut values from non-singular matrices in the encryption and decryption literature of cryptography. The airthemetic procedure developed on interval valued intuitionistic fuzzy numbers (IVIFNS) has a significant impact. In 1951, Dwer [5] proposed interval arithmetic in the literature. In order to get the desired conclusion, we changed the identical procedures to interval valued intuitionistic fuzzy numbers in this work.

2. Premiliners

2.1 Definitions

1. An intuitionistic fuzzy sets $\tilde{A}$ in E is defined as an object of the form $\tilde{A} = \{\langle x, \mu_{\tilde{A}}(x), \nu_{\tilde{A}}(x)\rangle / x \in E\}$ where the functions $\mu_{\tilde{A}} : E \to [0,1]$ and $\nu_{\tilde{A}} : E \to [0,1]$ define the degree of membership and the degree of non membership of the element $x \in E$, respectively and for every $x \in E$:

$$0 \le \mu_{\tilde{A}}(x) + \nu_{\tilde{A}}(x) \le 1$$

2. An intuitionistic pentagonal number of intuitionistic fuzzy set A is defined as $A_{IP} = \{(a_1, b_1, c_1, d_1, e_1)(a_2, b_2, c_2, d_2, e_2)\}$ where all $(a_1, b_1, c_1, d_1, e_1)$ $(a_2, b_2, c_2, d_2, e_2)$ are real numbers and membership function $\mu_{A_{IP}}(x)$ is given by

$$\mu_{\tilde{A}^I}(x) = \begin{cases} 0 & if \quad x < a_1 \\ \dfrac{x - a_1}{b_1 - a_1} & if \quad a_1 \le x \le b_1 \\ \left(\dfrac{x - b_1}{c_1 - b_1}\right) & if \quad b_1 \le x \le c_1 \\ 1 & if \quad x = c_1 \\ \left(\dfrac{d_1 - x}{d_1 - c_1}\right) & if \quad c_1 \le x \le d_1 \\ \dfrac{e_1 - x}{e_1 - d_1} & if \quad d_1 \le x \le e_1 \\ 0 & if \quad x > e_1 \end{cases}$$

Non membership function

$$\gamma_{A_{IP}}(x), \ \textit{is given by}$$

$$\gamma_{\tilde{A}^I}(x) = \begin{cases} 1 & if \quad x < a_2 \\ \dfrac{b - x}{b_2 - a_2} & if \quad a_2 \le x \le b_2 \\ \left(\dfrac{c_1 - x}{c_1 - b_2}\right) & if \quad b_2 \le x \le c_2 \\ 0 & if \quad x = c_1 \\ \left(\dfrac{x - c_1}{d_2 - c_1}\right) & if \quad c_2 \le x \le d_2 \\ \dfrac{x - d_2}{e_1 - d_2} & if \quad d_2 \le x \le e_2 \\ 1 & if \quad x > e_2 \end{cases}$$

2.2 Basics

In essence, matrix-based cryptography encrypts data using a non-singular key matrix and decrypts it using the inverse of the key matrix. Think about the text message

"WORKINGDAY."

We shall assign a number to each letter. Assigning 0 to a blank or space, 1 to A, 2 to B, etc., is the simplest method for doing that. Thus, our message string is

W	O	R	K	I	N	G	D	A	Y
23	15	18	11	9	14	7	4	1	25

And corresponding message matrix is

$$A = \begin{pmatrix} 23 & 15 \\ 18 & 11 \\ 9 & 14 \\ 7 & 4 \\ 1 & 25 \end{pmatrix}$$ of order 5×2 (n<m)

To secure this message, we encrypt it by multiplying the message matrix by an encoding matrix or key, which is a randomly chosen non-singular matrix.

$$K = \begin{pmatrix} 1 & 2 \\ 3 & 2 \end{pmatrix}$$

In pentagonal instutitionstic fuzzy number

$$A = \begin{pmatrix} 22,22.5,23,23.5,24,(1,0) & 14,14.5,15,15.5,16,(1,0) \\ 17,17.5,18,18.5,19,(1,0) & 10,10.5,11,11.5,12,(1,0) \\ 8,8.5,9,9.5,10,(1,0) & 13,13.5,14,14.5,15,(1,0) \\ 6,6.5,7,7.5,8,(1,0) & 3,3.5,4,4.5,5,(1,0) \\ 0,0.5,1,1.5,2,(1,0) & 24,24.5,25,25.5,26,(1,0) \end{pmatrix}$$

and

$$K = \begin{pmatrix} 0,0.5,1,1.5,2,(1,0) & 1,1.5,2,2.5,3(1,0) \\ 2,2.5,3,3.5,4,(1,0) & 1,1.5,2,2.5,3(1,0) \end{pmatrix}$$

Take $\alpha = 1, \beta = 0$

$$A = \begin{pmatrix} [23,23]\ [23,23] & [15,15]\ [15,15] \\ [18,18][18,18] & [11,11][11,11] \\ [9,9][9,9] & [14,14][14,14] \\ [7,7][7,7] & [4,4][4,4] \\ [1,1]\ [1,1] & [25,25]\ [25,25] \end{pmatrix}$$

$$K = \begin{pmatrix} [1,1][1,1] & [2,2][2,2] \\ [3,3][3,3] & [2,2][2,2] \end{pmatrix}$$

The resulting matrix is

$$X = AK = \begin{pmatrix} 68 & 76 \\ 51 & 58 \\ 51 & 46 \\ 19 & 22 \\ 76 & 52 \end{pmatrix}$$

If the receiver knows the key, which is the inverse of the encoding matrix, they can now decode the message after it has been encoded.

$$K^{-1} = \begin{pmatrix} -0.5 & 0.5 \\ 0.75 & -0.25 \end{pmatrix}$$

So the encoded message is again decoded as

$$M = XK^{-1} = \begin{pmatrix} 23 & 15 \\ 18 & 11 \\ 9 & 14 \\ 7 & 4 \\ 1 & 25 \end{pmatrix}$$

The Original message is obtained as

W	O	R	K	I	N	G	D	A	Y
23	15	18	11	9	14	7	4	1	25

Orthogonal matrices are also used to produce the key matrix of the traditional Hill cipher, which increases the security of communication texts [7]. The ciphertext improvisation is relatively safer when an orthogonal matrix is used. When a column vector is added and the matrix members are either 1 or 0, the idea of a one-to-one mapping matrix [8] is used in encryption. The basic principle of this method is to change row 1 to row n, row 2 to row n-1, row n to row 1, and so on. Consequently, the one-to-one mapping matrix can be used to encrypt and decode the secret data. Raja and Chakravarthy used Hilbert matrices to encrypt the confidential communications [9]. The Hilbert matrices were selected due to their constant invertibility and integer inverses. The inverse is easy to find if the order is known; it is difficult to find if the order is unknown. Because the size of the Hilbert matrix is kept secret (only the sender and the recipient know it), the instability makes it nearly impossible for anyone to extract the message without knowing the order.

3. Conclusion

In order to familiarize readers with pentagonal intuitionistic fuzzy numbers in the many encryption strategies used to encrypt the data using different matrices, this study has covered several of the key encryption techniques.. Although we can extend these operations into hexagonal intuitionistic fuzzy numbers.

References

1. http://www.richland.edu/james/lecture/.../matrices/applications.html

2. http://aix1.uottawa.ca/~jkhoury/cryptography.htm

3. Saeid Abbasbandy, Year: 2009, “Ranking of fuzzy numbers, some recent and new formulas”, INIFSA-EUSFLAT2009, pp. 642- 646.

4. Krassimir T Atanassov, Year: 1986, “Intuitionistic fuzzy sets and sytems”, Vol. 20, pp. 87-96.

5. Paul S Dwyer, Year: 1951, “Linear Computation”, (New York, 1951).

6. Paul S Dwyer, Year: 1964, “Matrix Inversion with the Square Root Method”, Technometrices, Vol: 6, No: 2, pp. 197-213.

7. Fozia Hanif Khan; Rehan Shams; Farheen Qazi; D. Agha, Year: 2015, “Hill Cipher Key Generation Algorithm By Using Orthogonal Matrix”, International Journal Of Innovative Science And Modern Engineering (IJISME), Vol: 3, No: 3, pp. 5-7.

8. Tzong-Mou Wu, Year: 2005, Applied Mathematics and Computation, Vol: 169, No: 2, pp. 963-70.

9. Penmetsa V. Krishna Raja; A. S. N. Chakravarthy; P. S. Avadhani, Year: 2011, “A Cryptosystem Based On Hilbert Matrix Using Cipher Block Chaining Mode”, International Journal Of Mathematics Trends And Technology.

10. Sophia Porchelvi; Rukmani Thiagarajan, Year: 2017, “On Solving Multi-Objective Linear Programming Problem with Pentagonal Intuitionstic Fuzzy Numbers (Ivifns)”, Global Journal of Pure and Applied Mathematics, Vol. 13, No. 2.

11. Babita Bist Ramola, Year: 2016, “Application of Non-Singular Matrices in Encryption and Decryption text of Cryptography” International Journal for Research in Applied Science & Engineering Technology (IJRASET), Vol. 4, Issue IV, April 2016 IC Value: 13.98 ISSN: 2321-9653.