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

pp. 71-73, April

Utilizing Interval-Valued Fuzzy Integers to Apply Non-Singular Matrices in Cryptography

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

[1,2]Department of Science and Humanities, A.V.C. College of Engineering, Mayiladuthurai

Corresponding Author E-mail: sathyas@avccengg.net

ABSTRACT: This article explains a few matrix-based cryptography approaches. Although the method is straightforward and quick to use for confidential communication encryption, it is also difficult to crack if one does not know the key. In order to keep the text provided by the sender in the form of positions and their inverses for decoding, the encryption system uses various types of matrices. the idea of solving non-singular matrices in cryptography using modified arithmetic operations on interval-valued fuzzy values. Since ancient times, the science of encrypting messages in secret codes—known as cryptography—has been crucial to information security. The fundamental tenet of cryptography is that data can be encrypted using a system that anyone who is aware of the technique can decode. Lastly, a numerical example was suggested.

Keywords: Inverse, matrices, cryptography, encryption, fuzzy numbers, and fuzzy interval numbers.

1. Introduction

Numerical techniques that deal with optimization functions employ interval analysis. A more thorough analysis can be found in [11]. Numerous intriguing fundamental cipher schemes that enable a deeper exploration of various mathematical issues are part of the long and rich history of cryptology. Numerous studies attempt to address this security issue by utilizing and enhancing matrix cryptography. For encryption and decryption, respectively, the key matrix and its inverse are needed [1-6]. However, what occurs if the matrix's inverse is absent? If not, how does the decryption process work? Several non-singular matrices in orthogonal, Hilbert, and quadratic forms have been employed in the past to get around all of the issues mentioned above. The structure of the paper is as follows: The preliminary steps are covered in Section 2. In section 3, this approach is extended to unconstrained optimization problems involving two variables. Section 4 discusses a numerical example to confirm that the suggested approach is feasible. At the end, a few closing thoughts are shared.

2. Preliminaries

2.1 Definition

Let $\tilde{x}=[x_1,x_2]$, $\tilde{y}=[y_1,y_2]$

(i) Addition:

$\tilde{x}+\tilde{y}=[x_1+y_1, x_2+y_2]$

(ii) Subtraction

$\tilde{x}-\tilde{y}=[x_1-y_2, x_2-y_1]$

(iii)Multiplication

$\tilde{x}.\tilde{y}=[\min(x_1y_1,x_1y_2,x_2y_1,x_2y_2), \max(x_1y_1,x_1y_2,x_2y_1,x_2y_2)]$

(iv)Division

$\frac{[a,b]}{[c,d]}$= [a, b].$\left[\frac{1}{d},\frac{1}{c}\right]$ if 0∉[c,d]

(v) $\tilde{x}$=[λx$_1$, x$_2$] for ≥ 0

[λx$_2$, x$_1$] for < 0

(vi)Inverse

$[x_1, x_2]^{-1} = \left[\frac{1}{x_2},\frac{1}{x_1}\right]$, for 0∉[x$_1$,x$_2$]

(vii)$[x_1, x_2]^n = [{x_1}^n, {x_2}^n]$, if x$_1$≥0

$= [{x_2}^n, {x_1}^n]$, if x$_1$<0

$= [0, \max\{{x_1}^n, {x_2}^n\}]$, otherwise.

2.2 Basics

Matrix-based cryptography essentially employs a non-singular key matrix [10] for encryption and the key matrix's inverse for decryption.

Consider text message “SUNDAY”

Each letter will be given a number. The easiest way to do that is to assign 0 to a blank or space, 1 to A, 2 to B, etc. Consequently, our message string is

S	U	N	D	A	Y
19	21	14	4	1	25

And corresponding message matrix is $A =$ (19 21 14 4 1 25) of order 3×2 (n<m)

We encrypt this message by multiplying the message matrix by an encoding matrix or key (a randomly selected non-singular matrix) in order to secure it.

$$K = (5 \quad 2\ 6 \quad 4)$$

In interval valued fuzzy number

A
$= ([18,20]\ [20,22]\ [13,15]\ [3,5]\ [0,2]\ [24,26])$

and

$$K = ([4,6] \quad [1,3]\ [5,7] \quad [3,5])$$

The resulting matrix is

$X = AK$
$= ([82,260]\ [78,170]\ [67,125]\ [22,70]\ [120,194]\ [72,136])$

Now after receiving the encoded message, receiver can decode it if knows the key which is inverse of encoding matrix

K^{-1}
$= ([0.4,0.6]\ [-0.24,-0.26]\ [-0.74,-0.76]\ [0.624,0.626])$

So the encoded message is again decoded as

$M = XK^{-1}$
$= ([18,20]\ [20,22]\ [13,15]\ [3,5]\ [0,2]\ [24,26])$

The Original message is obtained as

S	U	N	D	A	Y
19	21	14	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. The concept of a one-to-one mapping matrix [8] is applied to encryption when a column vector is introduced and the matrix members are either 1 or 0. 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. Thus, 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. The instability makes it nearly impossible for anyone to retrieve the message without knowing the order because the size of the Hilbert matrix is kept secret (only the sender and the recipient are aware of it).

3. Conclusion

This paper introduces encryption approaches to familiarize readers with interval-valued fuzzy numbers. For the majority of engineering domains, such as computer programs and applied

thermodynamics, the interval analysis method is very practical and cost-effective in terms of time savings.

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. 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.

11. R. Sophia Porchelvi; S. Sathya, Year: 2015, "On Solving Bivariate Unconstrained Optimization Problems Using Interval Analysis", International Journal of Scientific & Engineering Research, Vol. 6, No. 2, pp. 842.