IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Study Of Encryption And Decryption Technique Using Fuzzy Logic And Spiral Rotation

Lalit Chaurasiya & S. S. Shrivastava
Department of Mathematics
Institute for Excellence in Higher Education, Bhopal (M.P.)

ABSTRACT

The purpose of this paper is to introduced an encryption and decryption algorithm that uses Fuzzy logic to improve data communication security and efficiency. The technique adds complexity and randomness to the cryptographic process by combining Spiral rotation transformations with fuzzification and intensification operations because it transforms crisp input (a precise number) into a fuzzy linguistic value. that bears no relation to the primary data. This fact leads to considerable ambiguity on the part of attackers trying to guess the value of the key or the plain text, making the system more robust against security attacks.

Keywords: Fuzzy logic, Spiral rotation, Encryption and Decryption, fuzzification and intensification.

I. INTRODUCTION:

Protection against data transmission is now a necessity because of the growth in digital communication and the growing threat of unauthorized access. On mathematical grounds, cryptography defends information primarily by encrypting it (making it unreadable form) and decrypting it (restoring its original state). Cryptographic algorithms are typically divided into two categories: symmetric and asymmetric. Symmetric encryption relies on a single key for encoding and decoding data, whereas asymmetric encryption relies on a pair of keys—a public key to encrypt and a private key to decrypt. With digital interactions characterizing modern life, cryptography is the keystone of protecting data from unauthorized access and ensuring confidentiality. Various encryption and decryption methods are employed to protect digital data, deterring unauthorized alteration upon receipt. Apart from conventional approaches, we propose a new encryption and decryption process using a fuzzy logic in conjunction with spiral rotation to improve data protection by a unique and advanced mechanism.

Fuzzy logic:

A fuzzy logic in cryptography refers to the use of approximate reasoning and fuzzy sets to enable cryptographic operations that tolerate small variations or uncertainties in input data (e.g., noisy biometric measurements, partial matches). Unlike classical binary logic (exact 0 or 1), fuzzy logic allows degrees of membership, making it possible to securely generate, recover, or exchange keys even when the input is not perfectly identical to a reference, provided it lies within a defined error tolerance. Common applications include fuzzy extractors and biometric authentication systems, or strengthens the encryption system.

Fuzzification:

Fuzzification is of greatest significance in cryptography because they have the potential to the conversion of a crisp input (a precise number) into a fuzzy linguistic value, without any direct relation to the original information. The uncertainty makes it difficult for attackers to deduce the key or plaintext.

Intensification:

Intensifier is an operator (like "Very" or "Extremely") that reduces the fuzziness of a set, making the boundaries sharper. This adds randomness and strength to encryption.

Spiral rotation:

The Spiral Rotation Method is a type of cryptographic algorithm where data is placed in a matrix form and then rotated in a spiral pattern. This approach is also referred to as a "Spiral Rotation Encryption Algorithm." This process is used on data arranged in a matrix form before being encrypted or decrypted. This makes the data harder to recognize and adds an extra layer of security before encryption. It helps protect information by making it more difficult for hacker to find patterns or guess the original data. Spiral Rotation handles **"Diffusion"** (shredding the positions of the characters so they are no longer in their original order).

II. LITERATUEW REVIEW:

(1) K. GaneshKumar[1*] and D. Arivazhagan[2] et. al. [5] established cryptography algorithm that integrates fuzzy logic for secure data communication. In their proposed algorithm, they focused on encrypting both image and text data using fuzzy logic along with multiple keys to ensure high security and low processing time.

(2) Mendel, J. M. (1995) et. al. [7] established a fuzzy logic system for engineering in a tutorial format. In their work, they used fuzzy set theory, membership functions, and rule-based inference to provide a comprehensive overview of fuzzy logic applications in control, decision-making, and engineering systems.

(3) Niharika Belwanshi and S. S. Shrivastava et. al. [8] proposed a new encryption scheme involving Spiral Rotation Technique and Aryabhata's Substitution Code. In their proposed algorithm, they applied the Spiral Rotation Technique on a matrix representation of data, used Aryabhata's Substitution Code for plotting numbers to words, and incorporated the Byte Rotation Technique on different blocks of plaintext. This multithreading-enabled approach creates a double security system which is very fast and secure.

(4) Zadeh, L. A. (1965) et. al. [14] established the concept of fuzzy sets. In their proposed framework, they used membership functions to represent elements with degrees of membership ranging between 0 and 1, which enables the modeling of uncertainty and vagueness in information.

III. METHODOLOGY:

(1) To encrypt and decrypt the message, we will use fuzzification and intensification, which gives the intermediate cipher and then incorporate spiral rotation. We get the final cipher text.

(2) To decrypt the message firstly we will use reverse spiral, after that applying inverse intensification and reverse fuzzy shift, we get the original plain text.

Additionally, ASCII table is also used in this paper.

IV. ALGORITHM:

Encryption:

1. Generate a key matrix.
(a) Take block size of matrix (say n = 4)
(b) Choose the input key.
(c) We convert the input key which is taken by us into equivalent to ASCII table (decimal number).
(d) After performing the operation, we convert this numeric code into matrix form.
(e) After doing this we get the key matrix (say K).

2. Define A Secret Key.
(a) Take block size of matrix (say n = 4).
(b) Choose the input key.
(c) Convert the input key into corresponding equivalent ASCII table.
(d) Now convert this numeric code into matrix form, we get the matrix (say S).
3. Processing Fuzzy Logic.
(a) Fuzzification.
(b) After fuzzification We obtain a new fuzzy matrix A'.
4. We start Intensification (Key Addition).
(a) After Intensification, We obtain a new intensified matrix (A_{int})

5. Apply Spiral Rotation.
(a) After performing this operation, we got ciphertext.
6. Convert above decimal code into equivalent ASCII table character form (final ciphertext).

Decryption:
1. Consider the cipher text.
(a) Convert above character value into equivalent ASCII table decimal code.
2. Reverse the spiral order.
3. Now apply Inverse Intensification (Key Subtraction).
(a) We obtain a fuzzy matrix A′.
4. Now we do Reverse Fuzzy Shift.
(a) To found the plaintext we use this formula x = round (A'/1.196).
(b) Now convert this numeric code into corresponding equivalent ASCII table.
5. We get Final Plaintext.

V. ILLUSTRATION:

This example is based on the above algorithm involving fuzzy logic and spiral rotation.

Encryption:

1. Generation of Key Matrix:

(a) Take block size of matrix (say n = 4).
(b) Choose the input key

ENCRYPTIONMETHOD

(c) Convert the input key into corresponding equivalent ASCII table:
69, 78, 67, 82, 89, 80, 84, 73, 79, 78, 77, 69, 84, 72, 79, 68
(d) Now convert this numeric code into matrix form, we get the matrix (say K).:

$$K = \begin{bmatrix} 69 & 78 & 67 & 82 \\ 89 & 80 & 84 & 73 \\ 79 & 78 & 77 & 69 \\ 84 & 72 & 79 & 68 \end{bmatrix}$$

2. Define A Secret Key.

(a) Take block size of matrix (say n = 4).
(b) Choose the input key

RESEARCHKEYWORDS

(c) Convert the input key into corresponding equivalent ASCII table:
82, 69, 83, 69, 65, 82, 67, 72, 75, 69, 89, 87, 79, 82, 68, 83,
(d) Now convert this numeric code into matrix form, we get the matrix (say **S**).:

$$\mathbf{S} = \begin{bmatrix} 82 & 69 & 83 & 69 \\ 65 & 82 & 67 & 72 \\ 75 & 69 & 89 & 87 \\ 79 & 82 & 68 & 83 \end{bmatrix}$$

3. Processing Fuzzy Logic:

(a) Fuzzification:

Each element is converted to a fuzzy value in [0,1] by the rule:

$$x' = x + \text{round}(x/255*50).$$

where x is a key matrix value and $\mu(x)=x/255$.

1) x' = x + round(x/255*50).
=69+round (69/255*50)
=69+round (0.270*50)
=69+round (13.5)
=69+14
=83
2) x' = x + round(x/255*50).
=78+round (78/255*50)
=78+round (0.3058*50)
=78+round (15.29)

=78+15
=93

3) x' = x + round(x/255*50).
=67+round (67/255*50)
=67+round (0.2627*50)
=67+round (13.13)
=67+13
=80

Similarly for all element:
We obtain a new fuzzy matrix **A'**-

$$\mathbf{A'} = \begin{bmatrix} 83 & 93 & 80 & 98 \\ 106 & 96 & 100 & 87 \\ 94 & 93 & 92 & 83 \\ 100 & 86 & 94 & 81 \end{bmatrix}$$

4. Intensification (Key Addition):

Now we add the Secret Key Matrix **S** to the Fuzzy Matrix A' using modulo 256.
The formula is –

$$A_{int} = (A' + K) \pmod{256}$$

We put the value in formula from Secret Key Matrix **S** and Fuzzy Matrix A'-

- (1,1): 83 + 82 =165
- (1,2): 93 + 69 = 162
- (1,3): 80 + 83 = 163
- (1,4): 98 + 69 = 167
- (2,1): 106 + 65 =171
- (2,2): 96 + 82 = 178
- (2,3): 100 + 67 =167
- (2,4): 87 + 72 = 159
- (3,1): 94 + 75 = 169
- (3,2): 93 + 69 = 162
- (3,3): 92 + 89 = 181
- (3,4): 83 + 87 = 170
- (4,1): 100 + 79 =179
- (4,2): 86 + 82 = 168
- (4,3): 94 + 68 = 162
- (4,4): 81 + 83 = 164

We obtain a new intensified matrix (**A_{int}**)-

$$\mathbf{A_{int}} = \begin{bmatrix} 165 & 162 & 163 & 167 \\ 171 & 178 & 167 & 159 \\ 169 & 162 & 181 & 170 \\ 179 & 168 & 162 & 164 \end{bmatrix}$$

5. Spiral Rotation.

The matrix **A_{int}** is now read in a clockwise spiral order starting from the top-left corner. For a 4×4 matrix, the spiral order of indices is:

(1,1) → (1,2) → (1,3) → (1,4) → (2,4) → (3,4) → (4,4) → (4,3) → (4,2) → (4,1) → (3,1) → (2,1) → (2,2) → (2,3) → (3,3) → (3,2)

Applying this to D gives the following sequence:

- (1,1) = 165
- (1,2) = 162
- (1,3) = 163

- (1,4) = 167
- (2,4) = 159
- (3,4) = 170
- (4,4) = 164
- (4,3) = 162
- (4,2) = 168
- (4,1) = 179
- (3,1) = 169
- (2,1) = 171
- (2,2) = 178
- (2,3) = 167
- (3,3) = 181
- (3,2) = 162

Thus, the ciphertext is the sequence:
165, 162, 163, 167, 159, 170, 164, 162, 168, 179, 169, 171, 178, 167, 181, 162

6. Convert above decimal code into equivalent ASCII table character form (final ciphertext):
¥, ¢, £, §, Ÿ, ª, ¤, ¢, ¨, ³, ©, «, ², §, µ, ¢

Decryption:
1. Consider the ciphertext:
¥, ¢, £, §, Ÿ, ª, ¤, ¢, ¨, ³, ©, «, ², §, µ, ¢

(a) Convert above character value into equivalent ASCII table decimal code
Thus, the ciphertext is the sequence:

165, 162, 163, 167, 159, 170, 164, 162, 168, 179, 169, 171, 178, 167, 181, 162

2. Reverse the spiral order:
Place the numbers into a 4×4 matrix D following the same spiral order used in encryption.
The spiral order (clockwise from top-left) is:
(1,1) → (1,2) → (1,3) → (1,4) → (2,4) → (3,4) → (4,4) → (4,3) → (4,2) → (4,1) → (3,1) → (2,1) → (2,2) → (2,3) → (3,3) → (3,2)

Applying this to above ciphertext gives the following sequence:
- (1,1) = 165
- (1,2) = 162
- (1,3) = 163
- (1,4) = 167
- (2,4) = 159
- (3,4) = 170
- (4,4) = 164
- (4,3) = 162
- (4,2) = 168
- (4,1) = 179
- (3,1) = 169
- (2,1) = 171
- (2,2) = 178
- (2,3) = 167
- (3,3) = 181
- (3,2) = 162

Thus, the ciphertext is the sequence:

165, 162, 163, 167, 171, 178, 167, 159, 169, 162, 181, 170, 179, 168, 162, 164

We obtain a intensified matrix ($\mathbf{A_{int}}$)-

$$\mathbf{A_{int}} = \begin{bmatrix} 165 & 162 & 163 & 167 \\ 171 & 178 & 167 & 159 \\ 169 & 162 & 181 & 170 \\ 179 & 168 & 162 & 164 \end{bmatrix}$$

3. Inverse Intensification (Key Subtraction):

After reversing the spiral order. Now, we subtract the Secret Key Matrix **S** with the intensified matrix ($\mathbf{A_{int}}$) using modulo 256.

The formula is –

$$A' = (A_{int} - K) \pmod{256}$$

We put the value in formula from Secret Key Matrix **S** and intensified matrix ($\mathbf{A_{int}}$) -

- (1,1): 165 - 82 =83
- (1,2): 162 - 69 = 93
- (1,3): 163 - 83 = 80
- (1,4): 167 - 69 = 98
- (2,1): 171 - 65 =106
- (2,2): 178 - 82 = 96
- (2,3): 167 - 67 =100
- (2,4): 159 - 72 = 87
- (3,1): 169 - 75 = 94
- (3,2): 162 - 69 = 93
- (3,3): 181 - 89 = 92
- (3,4): 170 - 87 = 83
- (4,1): 179 - 79 =100
- (4,2): 168 - 82 = 86
- (4,3): 162 - 68 = 94
- (4,4): 164 - 83 = 81

We obtain a fuzzy matrix **A'**-

$$\mathbf{A'} = \begin{bmatrix} 83 & 93 & 80 & 98 \\ 106 & 96 & 100 & 87 \\ 94 & 93 & 92 & 83 \\ 100 & 86 & 94 & 81 \end{bmatrix}$$

4. Reverse Fuzzy Shift:

a) To found the plaintext we use this formula-

x = round (A'/1.196).

we put the value of fuzzy matrix **A'** in this formula to found the value of x (plain text)-

1) x = round (A'/1.196)
= round (83/1.196)
= round (69.39)
=69

2) x = round (A'/1.196)
= round (93/1.196)
= round (77.75)
=78

3) x = round (A'/1.196)
= round (80/1.196)
= round (66.88)
=67

Similarly for all element:
we get the key matrix (say K).:

$$K = \begin{bmatrix} 69 & 78 & 67 & 82 \\ 89 & 80 & 84 & 73 \\ 79 & 78 & 77 & 69 \\ 84 & 72 & 79 & 68 \end{bmatrix}$$

b) Now convert this numeric code into corresponding equivalent ASCII table:

$$K = \begin{bmatrix} E & N & C & R \\ Y & P & T & I \\ O & N & M & E \\ T & H & O & D \end{bmatrix}$$

5. Final Plaintext:

Combining these: E, N, C, R, Y, P, T, I, O, N, M, E, T, H, O, D
Which spells: "ENCRYPTIONMETHOD"

This matches the original plaintext

V. RESULT AND DISCUSSION:

In this paper, we introduce a novel encryption scheme that effectively incorporates Fuzzy Logic operations, such as Fuzzification and Intensification, with the Spiral Rotation to safely encrypt and decrypt information, as illustrated using the plaintext "ENCRYPTIONMETHOD". The multi-stage process—consisting Each element is converted to a fuzzy value in [0,1], conversion of a crisp input (a precise number) into a fuzzy linguistic value, and reduces the fuzziness of a set, making the boundaries sharper—completely scrambles and diffuses the information so much that it becomes highly challenging for an intruder to detect any pattern or correlation between the initial message and the encrypted message without the proper key. Because the key is created by converting text to ASCII code and shifting its bits, the system becomes very complex. This makes it extremely strong against common hacking methods like brute force (guessing all keys) or frequency analysis (looking for patterns). The process is so complex that trying to figure out the key without already knowing it is pretty much impossible for a computer. Therefore, this combined approach creates a very strong and safe way to protect important information.

These methods complicate decryption even further. Brute force attacks also fail to decrypt it because the encryption employs a 4×4 matrix as a key. decryption of big messages is not feasible. This keeps stored and sent messages secret, particularly for secret information such as military information. Because of these security properties, the likelihood of attacks such as ciphertext attack, chosen plaintext attack, brute force attack, and known plaintext attack is very slim. Hence, this suggested algorithm is much more secure than other encryption algorithms designed by researchers.

VI. CONCLUSION:

In conclusion, the fuzzy logic and spiral rotation stand as an essential tool for simplifying complex problems and enhancing security, with potential for continued growth and adaptation in the future.

REFERENCES

1. Akshay Kumar Tyagi[1*], D.B. Ojha[2*]: Applications of Fuzzy Error Correction in Communication Security in Cryptography, Journal of Global Research in Computer Science, ISSN-2229-371X, Volume 3, No. 8, August 2012.
2. Bashir, M. S., & Paetzold, M. (2021). "A New Class of Cryptographic Algorithms Based on Fuzzy Logic." *IEEE Access*.
3. Arvandi, M., Wu, S., Sadeghian, A., & Melek, W. W. (2003). "The role of fuzzy logic in cryptography." *IEEE International Conference on Fuzzy Systems*.
4. Dr. S. Revathi: Cloud Data security based on Fuzzy Intrusion Detection system with Elliptic Curve Cryptography (ECC) using Non-Adjacent Form (NAF) Algorithm, International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 10 Issue 11, November-2021.
5. K. GaneshKumar[1*] and D. Arivazhagan[2]: New Cryptography Algorithm with Fuzzy Logic for Effective Data Communication, Indian Journal of science and technology, vol 9(48), DOI: 10.17485/ijst/2016/v9i48/1089, December 2016.
6. Manas Paul[1] and Jyotsna Kumar Mandal[2]: A Novel Symmetric Key Cryptographic Technique at Bit Level Based on Spiral Matrix Concept, International Conference on Information Technology, Electronics and Communications (ICITEC – 2013), Bangalore, India, March 30 – 31, 2013.

7. Mendel, J. M. (1995). "Fuzzy logic systems for engineering: a tutorial." Proceedings of the IEEE, 83(3), 345-377.
8. Niharika Belwanshi[1], S. S Shrivastava[2]: A New Encryption Scheme Involving Spiral Rotation Technique Along with Aryabhata's Substitution Code, International Journal of Progressive Research in Science and Engineering, Vol.6., No.03., March 2025.
9. S. Sanal Kumar & S. Anfino Sherfin: A cryptographic encryption technique byte – Spiral rotation encryption algorithm, Journal of Discrete Mathematical Sciences & Cryptography, ISSN 0972-0529 (Print), ISSN 2169-0065 (Online), Vol. 22 (2019), No. 3, pp. 371–376 DOI: 10.1080/09720529.2019.1578083.
10. Suyash Kandele, Veena Anand: A Novel Square-Expanded-Matrix-Rotation (SEMR) Cryptography Method, International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 4 Issue 04, April-2015.
11. Shannon, C. E. (1949). "Communication Theory of Secrecy Systems." Bell System Technical Journal, 28(4), 656-715.
12. Vipin Saxena[1*]and Pawan Kumar[1]: Secure Transaction of Digital Currency through Fuzzy Based Cryptography, Indian Journal of Science and Technology 16(37): 3148-3158.
13. Zadeh, L. A. (1972). "A fuzzy-set-theoretic interpretation of linguistic hedges." Journal of Cybernetics, 2(3), 4-34.
14. Zadeh, L. A. (1965). "Fuzzy sets." Information and Control, 8(3), 338-353.