IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

DEVICING A FUZZY SOFT MATRIX FOR CRYPTOSYSTEM

[1]Agnes Jenifa.A,[2]Dr.A.Sahaya Sudha
[1]Research Scholar, [2]Assistant Professor
[1]Department of Mathematics,
Nirmala College ForWomen, Coimbatore, India
[2]Department of Mathematics,
Nirmala College ForWomen, Coimbatore, India

Abstract: To deal with the uncertainties, the recently known and developed topic was fuzzy soft set. Fuzzy soft set structures are very useful in many areas of applied mathematics and computer science. In this paper, we introduce a new operation of Hadamard product on fuzzy soft matrix. To evaluate the efficiency of these new proposed product of fuzzy soft matrix, a fuzzy soft matrix cryptosystem has been explained. Nowadays our life is not possible without social media because we are connected everywhere and share anything through online but the problem is security. In this application part we have introduced a strong security system to share the message. A new fuzzy soft encryption and decryption is introduced.

***Keywords*- Fuzzy soft set, Fuzzy soft matrix, Hadamard Fuzzy soft matrix product, Fuzzy Soft encryption, Fuzzy Soft decryption.**

I. Introduction

Fuzzy soft Matrix is the generalization of soft Matrix. In economics, engineering, environmental science, medical science, and many other fields researcher's deals with the complexities of modelling uncertain data. Typical methods are not always successful, because the alternatives and attributes appearing in these cases may be of distinct types. The concept of fuzzy sets was first developed by Zadeh [22] in 1965, is the most optimistic framework for dealing with uncertainties. Most of the real-life situation problems encountered in the complexity involved uncertain or unknown data. In 1999, Molodtsov [9] has defined the soft set which is efficient to solve uncertain data. Çagman and Enginoglu [2] in 2010 had worked on the soft matrix which is a matrix representation of the soft set. In 2001, Maji et.al;[8] has initiated the idea of a fuzzy soft set by implant the concept of a fuzzy set into the soft set. In 2016 Alcantud [1] was instigate some properties of fuzzy soft sets. In 2010 Majumdar et.al; and in 2009 Xiao [7,19] also bring in some properties of fuzzy soft set. Gong et al. [5] in 2013 introduced the concept of bijective fuzzy soft set. Cagman and Enginoglu [2] in 2012 again analyse the fuzzy soft matrix and the related operations was reproduced which make theoretical perspective of the fuzzy soft sets more efficient. They presented the operation of products of fuzzy soft matrices and then proposed a fuzzy soft max–min decision making method using these products. Xiao et al. [20] and Pei and Miao [14] discussed the similarity between the soft sets and information systems.

Secret way of transmission is clearly one of the most significant intentions of cryptography, therefore many keys such as secret-key, public-key of cryptosystems have been proposed to resolve it. It is furthermore widely confessed that the main security concept to be achieved is the semantic security by Rivest [15]. Stinson [18] has developed the theory and practice concept of cryptosystem. For secret communications a semantically secure public-key of cryptosystem is not only the most important, but for many complex aggregation protocols it is also fundamental primitive, such as electronic voting, electronic biometric and functions of secret evaluation to cite them. Nevertheless, in general having a secure cryptosystem is not sufficient to build efficient, elucidation for the above-mentioned problems. In general, more specified properties, such as kind of malleability, or even homomorphic relations, are beneficial to obtain practical constructions.

A public-key encryption scheme allows one person to secure a message for a unique beneficiary, the one who has the corresponding private key (decryption key). But in reality, there is often a natural hierarchy, whether for security or for safety cause: the captain of the crew may want to be able to read some message sent to the members of the crew, people may want to be able to retrieve the plain texts even if they forgotten their private key. For that reason, it is highly appreciable to give schemes that enable to deal with intermediate layout, in which users are permitted to process their own data. Moreover, in reality, there are many scenarios on which we require more than a plain an encryption key.

Specifically, it is recursively useful that allows to carry out some computation on the plaintexts without revealing them explicitly. The Hadamard product defined on fuzzy soft matrices was used in fuzzy soft encryption and fuzzy soft decryption.

II. PRELIMINARIES

Definition 2.1:[9]

Let V be the universal set and M be the family of parameters is a mapping from M to I(U) where I(U) is the power set and M is the set of parameters. The pair (F, M) is called the soft set is the mapping from the parameter set M to V.

Definition 2.2:[9]

Let V be the universal set and M be the family of parameters. F is a mapping from E to $J^{(V)}$ where $J^{(V)}$ is the collection of all fuzzy subsets of V and M is the set of parameters. The pair (F, A) is called the fuzzy soft set. F is the mapping from the parameter set M to V.

Definition 2.3[11]

Let (F, A) be a Fuzzy soft set over V. Then a subset of V × M is uniquely defined by,
R_A = {(v, m) : m ∈ A, v ∈ F_A(e)} ,which is called a relation form of (F, M).

The characteristic function of R_A is written by μ_{R_A}: V × M → {0, 1}

$$\mu_{R_A}(v, m) = \begin{cases} \mu_j(c_j) & e_j \in A \\ 0 & e_j \notin A \end{cases}$$

If V = $\{v_1, v_2, \ldots\ldots, v_m\}$, M = $\{m_1, m_2, \ldots\ldots, m_n$ and A ⊆ E,

Then the R_A can be presented by a table as in the following form

R_A	m_1	m_2	.	. .	m_n
v_1	$\mu_{R_A}(v_1,m_1)$	$\mu_{R_A}(v_1,m_2)$			$\mu_{R_A}(v_1,m_n)$
v_2	$\mu_{R_A}(v_2,m_1)$	$\mu_{R_A}(v_2,m_2)$			$\mu_{R_A}(v_2,m_n)$
.	.	.			.
.	.	.			.
.	.	.			.
.	.	.			.
v_m	$\mu_{R_A}(v_m,m_1)$				$\mu_{R_A}(v,m_n)$

Table 2.1(Representation of fuzzy soft matrix)

If a_{ij}=$\mu_{R_A}(u_i,e_j)$, we can define a matrix

$$[a_{ij}]_{m\times n} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nm} \end{bmatrix}$$

which is called an m × n fuzzy soft matrix of the soft set (F, M) over V.

Example 2.4:

Consider two pens from a shop, we denote them as s_1 and s_2 .Let the parameters be e_1 , e_2 colors of green and red, which is denoted by g and r respectively.

$U = \{s_1, s_2\}$, $E = \{g, r\}$,$A = \{e_1, e_2\}$

The set, $(F_A, E) \Rightarrow F(e_1) = \{(s_1, 0.8), (s_2, 0.5)\}$, $F(e_2) = \{(s_1, 0.4),(s_2, 0.3)\}$

The Fuzzy soft matrix been as follows: $\begin{bmatrix} 0.8 & 0.5 \\ 0.4 & 0.3 \end{bmatrix}$.

Definition 2.5: [4]

Let A and B be m × n matrices with entries in C. The Hadamard product of A and B is defined by $[A \circ B]_{ij} = [A]_{ij}\,[B]_{ij}$ for all 1 ≤ i ≤ m, 1 ≤ j ≤ n.

III. PROPOSED METHOD

In this section we define a new Hadamard Fuzzy Soft Matrix Product.

Fuzzy soft matrix product:

Let $[a_{ij}], [b_{ij}] \in$ FSM. The entrywise product $.e$ is defined as $[a_{ij}].e\,[b_{ij}] = [c_{ij}]$, where

$$[c_{ij}] = \begin{cases} max(a_{ij}, b_{ij}) & a_{ij} > b_{ij} \\ min(a_{ij}, b_{ij}) & a_{ij} < b_{ij} \\ b_{ij} & a_{ij} = b_{ij} \end{cases}$$

Example:

Consider two pens and two pencils from a shop, we denote them as s_1 and s_2 .Let the parameters be e_1, e_2 colors of green and red, which is denoted by g and r respectively.

$U = \{s_1, s_2\}$, $E = \{g,r\}$,$A = \{e_1, e_2\}$

consider two fuzzy soft matrices

$$[a_{ij}] = \begin{bmatrix} 0.1 & 0.5 \\ 0.3 & 0.4 \end{bmatrix} \qquad [b_{ij}] = \begin{bmatrix} 0.6 & 0.5 \\ 0.9 & 0.3 \end{bmatrix}$$

Product of two matrix according to the above Hadamard fuzzy soft product matrix was,

$$\begin{bmatrix} 0.1 & 0.5 \\ 0.3 & 0.4 \end{bmatrix} .e \begin{bmatrix} 0.6 & 0.5 \\ 0.9 & 0.3 \end{bmatrix} = \begin{bmatrix} 0.1 & 0.5 \\ 0.3 & 0.4 \end{bmatrix}.$$

IV. PROPERTIES

Associative property 4.1:

Let $[a_{ij}], [b_{ij}], [c_{ij}]$ are Fuzzy soft matrix. The associative property of fuzzy soft matrix is defined as $([a_{ij}].e\,[b_{ij}]).e\,[c_{ij}] = [a_{ij}].e\,([b_{ij}].e\,[c_{ij}])$. The representation of $.e$isentrywise product.

Commutative property 4.2:

Let $[a_{ij}], [b_{ij}]$ are Fuzzy soft matrix.The commutative property of fuzzy soft matrixes defined as $([a_{ij}] .e\,[b_{ij}]) = ([b_{ij}] .e\,[a_{ij}])$.The representation of $.e$ is entrywise product.

Distributive property 4.3:

Let $[a_{ij}], [b_{ij}], [c_{ij}]$ are Fuzzy soft matrix.The distributive property of fuzzy soft matrix is defined as $[a_{ij}].e\,([b_{ij}] + [c_{ij}]) = ([b_{ij}].e\,[a_{ij}]) + ([c_{ij}].e\,[a_{ij}])$.The representation of $.e$ is entrywise product.

Multiplicative identity property 4.4:

Let $[a_{ij}]$ is Fuzzy soft matrix and [0] be the zero fuzzy soft matrix. The multiplicative property of fuzzy soft matrixis defined as $([a_{ij}].e\,[I]) = [a_{ij}] = ([I].e\,[a_{ij}])$.The representation of $.e$ is entrywise product.

Multiplicative of zero property 4.5:

Let $[a_{ij}]$ is Fuzzy soft matrix and [0] be the zero fuzzy soft matrix. The multiplicative of zero property of fuzzy soft matrix is is defined as $([a_{ij}].e\,[0]) = [0] = ([0].e\,[a_{ij}])$.The representation of $.e$ is entrywise product.

Dimension property 4.6:

The dimension property of fuzzy soft matrix is defined as the product of an O×P fuzzy soft matrix and an P×R Fuzzy soft matrix is an O×R Fuzzy soft matrix.

V. FUZZY SOFT CRYPTOSYSTEM

Generally, **Cryptography** enables to store sensitive information or transmit it across secure networks so that it cannot be read by anyone except recipient. Here it is shown that new encryption and decryption methodology. In this paper, we rectify it by the following algorithm.

Fuzzy Soft encryption algorithm:

1. Jemi takes a fuzzy soft set.
2. Jemi finds corresponding soft matrix.
3. Jemi parts message blocks and transfer it according to some secret key.
4. Jemi makes product message with fuzzy soft matrix.
5. Jemi turns from matrix to letter and sends to Jefi.

Fuzzy Soft decryption algorithm:

1. Jefi takes fuzzy soft matrix.
2. Jefi parts cipher text blocks and transfers from secret key.
3. Jefi makes product cipher text with fuzzy soft matrix.
4. Jefi turns from matrix to letter.
5. Jefi obtains message.

VI. ANALYSIS OF ALGORITHM

ENCRYPTION:

1.) Jemi takes the fuzzy soft set,

$(f_A,\mathrm{E}) = \{(e_1;u_1,u_2), (e_2;u_1,u_3,u_4), (e_3;u_4), (e_4,u_1,u_3)\}$

Consider the Fuzzy soft matrix,

$$\begin{bmatrix} 0.1 & 0.3 & 0 & 0 \\ 0.2 & 0 & 0.1 & 0.4 \\ 0 & 0 & 0 & 0.3 \\ 0.5 & 0 & 0.1 & 0 \end{bmatrix}.$$ ---------- eqn 1

KEY:

A	B	C	.	.	J	K	..	.	.	Z
0.1	0.2	0.3			1.0	0.1				0.6

2.) Jemiwants to send the message '**ABSTRACT**' to Jefi.For that shebreaks the word into blocks as **ABST – RACT.**

3.) Shemakes the block as fuzzy soft matrix using the key.

- Fuzzy soft matrix of Block I (ABST) is $\begin{bmatrix} 0.1 & 0.2 & 0.9 & 0.1 \\ 0.2 & 0.2 & 1.0 & 0.2 \\ 0.9 & 1.0 & 0.9 & 0.9 \\ 0.1 & 0.2 & 0.9 & 1.0 \end{bmatrix}$
- Fuzzy soft matrix of Block II (RACT) is $\begin{bmatrix} 0.8 & 0.8 & 1.0 & 0.8 \\ 0.8 & 0.1 & 0.3 & 0.1 \\ 1.0 & 0.3 & 0.3 & 0.3 \\ 0.8 & 0.1 & 0.3 & 1.0 \end{bmatrix}$.

4) Product block I with fuzzy soft matrix 1 using the Hadamard soft fuzzy product and we obtain ABST as KLSU. Consequently, product block II with fuzzy soft matrix 1 and convert RACT as SRJH.

5)Jemi send the message (cipher text) as **KLSUSRJH** to Jefi.

DECRYPTION:

1) Mike receives the message KLSUSRJH and key.

2) She converts the cipher text to fuzzy soft matrix.

3) With that matrix using the proposed product she got the fuzzy soft matrix of Block I and Block II.

4) She converts the fuzzy soft matrix into words.

5) She obtains the message ABSTRACT.

VII. CONCLUSION

This system depends on Fuzzy soft sets and Fuzzy soft matrices. Thus, in this application we have taken fuzzy soft matrices where our gadgets read messages as binary numbers but there may be some uncertainty so we consider that as fuzzy soft matrices, this system makes fast encryption and decryption. To avoid hacking attacks, we should be careful in the choice of fuzzy soft sets. If we choose elements of the Fuzzy soft sets thus encryption security is increased. Also, similarly operations of column can make which make operations with line to which our scheme can be applied. We can secure the important information by using this method. By taking the best fuzzy soft matrix we can improve the security. We can easily store this in our computer memory.

VIII. REFERENCES

[1] Alcantud JCR, A novel algorithm for fuzzy soft set-based decision making from multi observer input parameter data set. Inf Fusion 29:142–148, 2016.

[2] Cagman N, Enginoglu S, Fuzzy soft matrix theory and its application in decision making. Iran J Fuzzy Syst 9(1):109–119, 2012.

[3] Dubois.D, H. Prade, Fuzzy Set and Systems: Theory and Applications, Academic Press, New York, 1980.

[4] ElizabethMillion, The Hadamard Product, volume 1, April 12, 2007.

[5] Gong K, Wang P, Xiao Z, Bijective soft set decision system-based parameters reduction under fuzzy environments. Appl Math Model 37(6):4474–4485, 2013.

[6] Lin, R.R. Yager, B. Zhang (Eds.), Proceedings of Granular Computing, vol. 2, IEEE, pp, 617–621, 2005.

[7] Majumdar P, Samanta SK, Generalized fuzzy soft sets. Comput Math Appl 59(4):1425–1432, 2010.

[8] Maji PK, Biswas R, Roy AR, Fuzzy soft sets. J Fuzzy Math 9(3):589–602, 2001.

[9] Molodtsov D, Soft set theory—first results. Comput Math Appl 27(4–5):19–31, 1999.

[10] D. Molodtsov, The description of a dependence with the help of soft sets, Journal of Computer and Systems Sciences International 40 (6) 977–984, 2001.

[11]Molotov, The Theory of Soft Sets, URSS Publishers. , Moscow,(in Russian), 2004.

[12] M.M. Mushrif, S. Sengupta, A. K. Ray, Texture classification using a novel, soft-set theory-based classification, algorithm, Lecture Notes in Computer Science 3851, 246–254, 2006.

[13] Z. Pawlok, A. Skowron, Rudiments of soft sets, Information Sciences 177, 3–27, 2007.

[14] Pei.D, D. Miao, From soft sets to information systems, in: X. Hu, Q.Liu, A. Skowron, T.Y.

[15] Rivest.R, L. Adleman, M. Dertouzos, On data banks and privacy homomorphisms, In Foundations of Secure Computation, 169–180, 1978.

[16] Roger Horn. Topics in Matrix Analysis, Cambridge University Press, 1994.

[17] A. Rosenfeld, Fuzzy groups, J. Math. Anal. Appl. 35, 512–517, 1971.

[18] Stinson D, Cyrptography: Theory and Practice, CRC Press, New Jersey, 573pp, 1995.

[19] Xiao.Z, L. Chen, B. Zhong, S. Ye, Recognition for soft information based on the theory of soft sets, in: J.Chen (Ed.), Proceedings of ICSSSM-05, vol. 2, IEEE, pp., 1104–1106, 2005.

[20] Xiao Z, Gong K, Zou Y, A combined forecasting approach based on fuzzy soft sets. J Computational Application Math 228(1):326–333, 2009.

[21] Yang. Y and Chenli Ji, "Fuzzys soft matrices and their applications", Lecture notes in Computer Science 7002, pp: 618 – 627, 2011.

[22] Zadeh L.A, Fuzzy sets. Inf Control 8:338–353, 1965.