Southeast Europe Journal of Soft Computing ISSN 2233 – 1859
Available online: http://scjournal.ius.edu.ba

Vol 12, No. 2, September 2023, pp. 30-33

A Cryptographic Algorithm using Fuzzy Logic and Deck of Cards

[1*]Kala Raja Mohan, [1]R. Narmada Devi, [1]Nagadevi Bala Nagaram, [1]Regan Murugresan and [1]T. Bharathi

[1]Department of Mathematics,
Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology,
Avadi, Chennai – 600 062,
Tamil Nadu, India.
[1]Loyala College, Nungambakkam, Chennai-600 034,
Tamil Nadu, India.
**Corresponding Author*: kalamohan24@yahoo.co.in

Article Info

Article history:

Article received on 09 10 2023

Received in revised form 30 10 2023

Keywords:

Cryptography; Mathematics; Fuzzy logic; Deck of Cards

ABSTRACT: Sharing of information in a secured manner is extremely essential in this world of internet technology. In recent times, many people come across situations wherein their personal data are being hacked by trespassers. These stolen data are used for many malpractices including theft of money. Many researchers involve themselves in finding a better path to overcome this difficulty. Cryptography plays a major role in bringing out a solution to rectify this issue. Mathematics provides a helping hand in most of the cryptographic techniques. It helps to secure data from hackers involved in the robbery of data. Fuzzy logic find its application in many field of research. This paper proposes a cryptographic technique which make use of fuzzy logic together with the help of deck of cards and its membership functional value.

1. INTRODUCTION

Nowadays, an unevitable part of our life is mobile communications, computer networks which uses internet for its base. Still, the internet provides option for many hackers to steel the data stored in the system such as mobile or computer. It is very much essential to provide safety measure while sharing the information. Cryptography plays a major role in providing such information security. Cryptography ensure communication between any two individuals in a secured way.

Fuzzy logic is a form of approach in which values are assumed as truth values from zero to one. It provides an oppoutunity in which values can be assigned flexibly with valid reasons. Mathematical models in decision making with uncertainty make use of fuzzy logic. It finds its application in many areas such as predictive analysis, neutral network, pattern recognition and many more.

Deck of cards is a term used to denote a pack of 52 playing cards. It includes four type of cards namely suits. Each of the suits consists of 13 cards. These playing cards have got attraction of all age group of people. Many type of games are being played by them using these type of cards. Many probability problems also make use of deck of cards and its selection process. Apart from this, these cards are also made available online and offline for software usage through various games applications.

P. Hiwarekar in 2014 proposed two cryptographic technique applying Laplace Transform and Hyperbolic functions [1,3]. M. Tuncay Gencoglu in 2017 introduced a crytographic process involving Laplace

Transform with Hyperbolic functions [2]. Dr. K. Hemant K. Undegaonkar introduced a secured communication method involving Laplace Transform [4]. S. Sujatha in 2013 made use of the application of Laplace Transform in the field of cryptography [5]. C. H. Jayanthi and V. Srinivas in 2019 framed a new mathematical modelling involving Laplace Transform [6]. G. Nagalakshmi et al in 2020 involved Laplace Transform Laplace Transform using Asymmetric key for secured communication [7]. S. Dhingra et al proposed a network security method involving Laplace Transform [8]. M. Saha in 2017 utilized Laplace Mellin Transform in forming a cryptographic method for secured information sharing [9]. A. K. H. Sedeeg et al in 2016 formulated a new cryptographic algorithm applying Aboodh Transform [10].

Kala Raja Mohan et al in 2022 applied Bilinear Transform with Probability in identifying a secured information sharing algorithm [11]. A. Meenakshi et al applied graph network in designing a crypographic algorithm [12]. Kala Raja Mohan et al in 2022 made use of Laplace transform and hyperbolic tangent function in cryptography [13]. This paper aims at developing a cryptographic algorithm using fuzzy logic.

In section 2, the standard definitions made use of in this crypto analysis are described. Section 3 represents the algorithm which is applied for encryption. The encryption algorithm which is explained in section 3 is demonstrated with an example in section 4. Section 5 depicts the algorithm applied for decryption. With the help of the cipher text obtained in Section 4, decryption process is explained in section 6. Section 7 is about the conclusion followed by references.

2. STANDARD DEFINITIONS

The cryptographic analysis proposed in this paper make use of the following standard definitions in this paper.

The information which is to be shared to the other person secretly is the plain text.

The encrypted message making use of the key specified for the process is the cipher text.

The process by which the plain text gets transformed into the cipher text is the cipher.

The process involved in converting plain text into secret message is encryption.

The reverse process of encryption is decryption, which converts secret message to plain text.

To imitate human reasoning and cognition fuzzy logic is used.

The degree of truthfulness in the fuzzy logic is membership function.

The process by which input values are converted into degree of membership is fuzzification.

The reverse process of obtaining output values from conclusion is defuzzification.

A pack consisting of 52 cards is deck of cards.

The four divisions of cards such as clubs, diamonds, hearts and spades are called as suits.

Each suits comprising of 13 ranks starting from Ace, 2 to 9, Jack, Queen and King.

3. ALGOFRTHIM FOR ENCRYPTION

The procedure to be followed in the process of encryption is as given below.

Step 1: Coding table for this proposed analysis is formed as a two way table. With one side mentioning the ranks and to the other side the suits. To each of the box both capital and small alphabets are assigned.

Step 2: Using the coding table, the plain text is assigned the corresponding codes. Step 3: For the coding table, membership function table is framed.

Step 3: For the coding table, membership function table is framed.

Step 4: The codes in the step 2 are assigned the corresponding membership value after multiplying with 1000. These codes are represented in a graph and shared as cipher text between the sender and the receiver.

4. ENCRYPTION ILLUSTRATION

The coding table is given in table 1.

Table 1 Coding Table

	♠	♣	♥	♦
1	A	N	a	n
2	B	O	b	o
3	C	P	c	p
4	D	Q	d	q
5	E	R	e	r
6	F	S	f	s
7	G	T	g	t
8	H	U	h	u

9	I	V	i	v
10	J	W	j	w
11	K	X	k	x
12	L	Y	l	y
13	M	Z	m	z

For numerical illustration, the word ‘Mathematics’ is chosen. The word in coded format is given below in Table 2.

Table 2 Coded form of Plain text

M	a	t	h	e	m	a	t	i	c	s
♠ 13	♥1	♦7	♥8	♥5	♥ 13	♥1	♦7	♥9	♥3	♦6

Table 3 Membership Function

	1	**2**	**3**	**4**
1	0.082	0.089	0.097	0.102
2	0.156	0.164	0.171	0.179
3	0.231	0.238	0.246	0.253
4	0.305	0.313	0.320	0.328
5	0.380	0.388	0.395	0.402
6	0.455	0.462	0.470	0.477
7	0.529	0.537	0.544	0.552
8	0.604	0.611	0.619	0.626
9	0.679	0.686	0.694	0.701
10	0.753	0.761	0.768	0.776
11	0.828	0.835	0.843	0.850
12	0.902	0.910	0.917	0.925
13	0.977	0.985	0.992	1

The membership function used for this process is given in Table 3. Formation of each membership function is as defined below: For calculation purpose Ace is assigned to number 1, Jack, Queen, King are assigned to 11, 12 and 13. These numbers are made as row headings. The suits spade, club, heart and diamond are assigned as numbers 1, 2, 3 and 4, which are made as column heading. There are 13 rows and 4 columns in the table. For finding each membership function, its corresponding row heading is multiplied with 10 and added to its corresponding column heading count. Then the total is divided by 134.

Using the codes obtained in Table 2, their corresponding membership function is expressed by multiplying each of them by 1000.

Table 4: Cipher Text Table

♠ 13	♥1	♦7	♥8	♥5	♥ 13	♥1	♦7	♥9	♥3	♦6
977	097	552	619	395	992	097	552	694	246	477

The table values obtained in Table 4 are graphically represented as shown in Figure 1 and shared as an encrypted image.

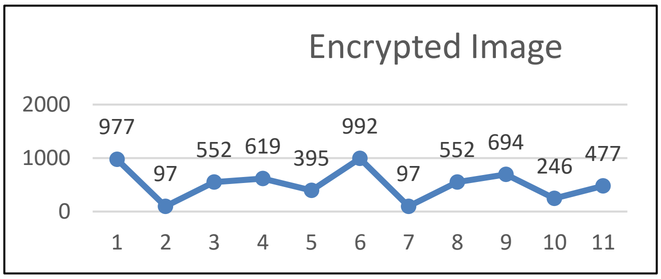

Figure 1:

5. ALGOFRTHIM FOR DECRYPTION

The procedure to be followed in the process of decryption is as given below.

Step 1: The numbers present in the encrypted image are multiplied by 1000.

Step 2: The values obtained are multiplied by 134.

Step 3: The resulting numbers are next divided by 10.

Step 4: The quotient value together with the decimal rounded off are considered to be the heading of column and row. Using these, the membership value to each of the combination is found.

Step 5: Corresponding to the membership value, the coding is obtained.

Step 6: From the coding obtained, plain text is identified.

6. DECRYPTION ILLUSTRATION

The cipher text obtained from the encrypted image written in three digits format is 977-097-552-619-395-992-097-552-694-246-477.

Each number is divided by 1000 and represented in Table 5.

Table 5 Cipher Text Value divided by 1000

.977	.097	.552	.619	.395	.992	.097	.552	.694	.246	.477

Values obtained in Table 5 are multiplied with 134 and represented in Table 6.

Table 6: Values multiplied with 134

130.9	12.99	73.97	82.95	52.93	132.9	12.99	73.97	92.99	32.96	63.92

The values obtained are again divided by 10. Then the quotient and the decimal values are rounded off to obtain the row and column heading of each membership value. Those values are presented in Table 7.

Table 7 Heading values in Decryption process

13-1	1- 3	7- 4	8- 3	5- 3	13- 3	1- 3	7- 4	9-3	3- 3	6- 4

From the values obtain in Table 7, plain text is obtained by referring to the coding table as given in Table 8.

Table 8 Decryption process plain text

♠ 13	♥1	♦7	♥8	♥5	♥ 13	♥1	♦7	♥9	♥3	♦6
M	a	t	h	e	m	a	t	i	c	s

7. CONCLUSION

In the process of secured data communication, cyptography plays a predominant role. Mathematics also lays a major background in the development of cryptographic algorithm. This paper proposes a new cryptographic algorithm involving fuzzy logic and deck of cards. It is hard to identify the fuzzy membership function proposed in the algorithm. Thus it is beneficial in the field of cryptography. The proposed algorithm has been illustrated with the word ‘Mathematics’ as an example.

REFERENCES

[1] A. P. Hiwarekar, “New mathematical modeling for cryptography,” Journal of Information Assurance and Security, 9, 027-033 (2014).

[2] M. Tuncay Gencoglu, “Cryptanalaysis of a New Method of Cryptography using Laplace Transform Hyperbolic Functions.” Communications in Mathematics and Applications, 8, 183-189 (2017).

[3] A. P. Hiwarekar, “A new method of Cryptography ussing Laplace transform of Hyperbolic functions,” International Journal of Mathematical Archive, 4, 208-213 (2013).

[4] Dr. K. Hemant K. Undegaonkar, “Security in Communication By Using Laplace Transform and Cryptography,” International Journal of Scientific & Technology Research, 8, 3207-3209 (2019).

[5] S. Sujatha, “Application of Laplace Transforms in Cryptography,” International Journal of Mathematical Archive, 4, 67-71 (2013).

[6] C. H. Jayanthi and V. Srinivas, “Mathematical Modelling for Cryptography using Laplace Transform,” International Journal of Mathematics Trends and Technology, 65, 10-15 (2019).

[7] G. Nagalakshmi, A. Chandra Sekhar and D. Ravi Sankar, “Asymmetric key Cryptography using Laplace Transform,” International Journal of Innovative Technology and Exploring Engineering, 9, 3083-3087 (2020).

[8] S. Dhingra, A. A. Savalgi and S. Jain, “Laplace Transformation based Cryptographic Technique in Network Security,” International Journal of Computer Applications, 136, 6-10 (2016).

[9] M. Saha, “Application of Laplace – Mellin Transform for Cryptography,” Raj Journal of Technology Research & Innovation, 5, 12-17 (2017).

[10] A. K. H. Sedeeg, M. M. Abdelrahim Mahgoub, and M. A. Saif Saeed, “An Application of the New Integral “Aboodh Transform” in Cryptography,” Pure and Applied Mathematics Journal, 5, 151-154 (2016).

[11] Kala Raja Mohan, Suresh Rasappan, Regan Murugesan, Sathish Kumar Kumaravel and Ahamed A. Elngar, “Secret Information Sharing Using Probability and Bilinear Transformation”, Proceedings of 2nd International Conference on Mathematical Modeling and Computational Science, 115-122 (2022).

[12] A. Meenakshi, J. Senbagamalar, and A. Neel Armstrong, “Encryption on Graph Networks”, Proceedings of 2nd International Conference on Mathematical Modeling and Computational Science, 123-130 (2022).

[13] Kala Raja Mohan, Suresh Rasappan and Sathish Kumar Kumaravel, “Secret Information sharing Using Laplace Transform and Hyperbolic Tangent Function”, AIP Conference Proceedings 2516, 12003, 1-6, (2022).