© 2015 IJSRSET | Volume 1 | Issue 6 | Print ISSN: 2395-1990 | Online ISSN: 2394-4099
Themed Section: Engineering and Technology

Novel Architecture for Data – Shuffling Using Fisher Yates Shuffle Algorithm

C. Aishwarya, J. R. Beny
Department of Electrical and Electronics Engineering, SNS College of Technology, Tamilnadu, India

ABSTRACT

Securing information from obtrudes is the miscellaneous process in communication, cryptography is an effective manner of securing the information. New architecture is designed in this paper based on Fisher Yates Shuffle algorithm to maintain secrecy of data. A newly modified magic rectangle (NMMR) is constructed based few constrains, like sum of row and column values are equal. The numerical value of data is taken and it is added with NMMR values in random position. To enhance data security iterative fisher Yates shuffle algorithm (IFYS) is designed in which, third order shuffling is carried out. IFYS-algorithm shuffles the elements in NMMR randomly, which potentially increase data security. These cipher texts are transmitter in channels through modulation techniques. This process ensures that data transfer with confidentially and integrity of the data can be improved effectively.

Keywords: Confidentiality, NMMR, Data Security, IFYS-Algorithm, Modulation Techniques

I. INTRODUCTION

Security is a major concern in wired communication. Various techniques are used for providing the security for the transmitting data. Most commonly used cryptographic algorithms are advanced encryption standard (AES), data encryption standards (DES), triple data encryption standards T-DES for symmetric cryptography and Diffie Hellman key exchange[1] and Rivest Shamir and Adleman (RSA) algorithm for the Asymmetric cryptography, in which RSA is the most commonly used algorithm[2][3]. To improve this algorithm, various methods are created to overcome the repetitive of the cipher text, due to repeatation of same character in the data, magic square is implemented, in which both column sum and the row sum will be equal [11]. The data for encryption is taken from the magic square similarly, magic rectangle is implemented [14] for providing more security, since the value of the column sum and row sum will be different and the two value are difficult to obtain without the magic pattern. The construction of magic square and magic rectangle will consume more time than encryption and decryption process. If the pattern of the magic structure is found then security is no longer valid. To ensure higher order security among data prefixing to be done.

In prefixing, Shuffling process is done for improving the complexity of data that is needed to be transmitted. Images can be encrypted by shuffling the pixels and adding public key to the colored image [12]. Fisher-Yates shuffle algorithm is most commonly used algorithm for shuffling .since it provides unique randomness for every shuffle. It is quite efficient; indeed, its asymptotic time and space complexity are optimal. Combined with a high-quality unbiased random number source, it is also guaranteed to produce unbiased results. The advantage of Fisher Yates shuffle algorithm is higher speed and precision in estimating the randomness of the data.

II. METHODS AND MATERIAL

To strengthen the security of the data newly modified magic rectangle is created such that each value of sum of column is equal and the each row values are equal. The filling order is based on the table 1.1

Table 1.1 Order of magic formation

$\text{Max}_{\text{START}}$	+2	+4	-6	-16	+16
+8	-10	-12	+14	+24	-24
-14	+12	+10	-8	-30	+30
+6	-4	-2	$\text{Min}_{\text{START}}$ 4	+22	-22

Based on the Maxstart value and the Minstart value the magic table is formed. The Max value is decremented and the Min value is incremented according to the value present in the filling order table.

The max value is determined by the column sum value. The column sum value is calculated by diving the initial value by four (1)

$$\text{Column}_{\text{sum}} = \frac{\text{Initial value}}{4} \quad \text{----------} \; [1]$$

Similarly Row sum is calculated using the formula (2)

$$\text{Row}_{\text{sum}} = \left(\text{Column Sum}/2\right) + \left(\text{Column Sum}\right) \quad [2]$$

The Min $_{\text{start}}$ value is consider as the 4 since the basic filling order is taken in 4x6 size thus the number of row is taken as the Min $_{\text{start}}$ value.
Based on the column $_{\text{sum}}$ value the Max$_{\text{start}}$ value is calculated using the formula (3)

$$\text{Max}_{\text{start}} = \left(\text{Column}_{\text{sum}} / 2\right) - \text{Min}_{\text{start}} \quad [3]$$

On using the formula (1) (2) (3) the newly modified magic rectangle is created for the given initial value. The order of the matrix is taken in smaller size to reduce the computational time of the process.

Fisher Yates shuffle algorithm is used for random shuffling which is the basic method for generating the random number 1 through N. To shuffle the n elements of arrays the end value is consisdered as (n-1).

Comparing with other shuffling algorithm timing and complexity is optimized and it produce the high quality unbiased result when it combines with the unbiased code. In this fisher Yates shuffle algorithm third order iteration is implementing to achieve high level of complexity for data.

In the proposed work this newly modified magic rectangle and the iterative fisher Yates shuffle algorithm is implemented in the data before transmitting the data to the channel. Block diagram is shown in the fig 1.1

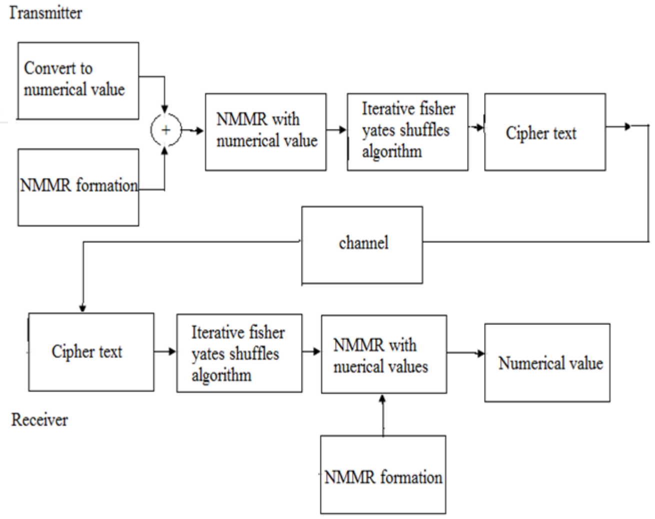

Transmitter
Convert to numerical value
+
NMMR formation
NMMR with numerical value
Iterative fisher yates shuffles algorithm
Cipher text
channel
Cipher text
Iterative fisher yates shuffles algorithm
NMMR with nuerical values
Numerical value
Receiver
NMMR formation

Figure 1.1: System Block Diagram

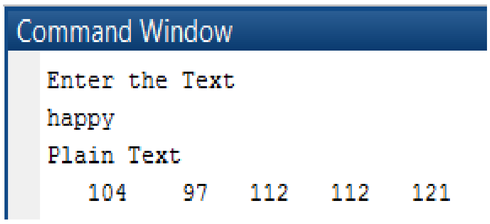
In the transmitter section numerical value of the data to be transmitted is taken , newly modified magic rectangle is formed based the the given initial value system calculate the col $_{\text{sum}}$ value which used for obtaining row$_{\text{sum}}$ value and max min value . Depending on the position of the filling order the max$_{\text{start}}$ value is decremented by 2 and min $_{\text{start}}$ value is incremented.

This NMMR value and the numerical value of the text is combined together by the addition operation, and it is followed by the iterative fisher Yates shuffle algorithm. This shuffle the position of the element in the matrix randomly based on the algorithm. Third order shuffling is given to the matrix to increase the complexity. Obtained cipher text is transfer in the public channel.

In receiver section, the transmitted data, which is in form of cipher text, is received from the public channel. This cipher text is processed with the iterative fisher Yates shuffle algorithm is used to recover the original position of the matrix. From the recovered matrix, the numerical value of the plain text and value of NMMR value is separated.

This data is secure because even if the pattern of the magic rectangle is obtain the data cannot be retrieved since the intruder has to know the shuffling order of the matrix. Since the algorithm used here is iterative Fisher Yates shuffle algorithm the randomness of the shuffle is hard to discover.

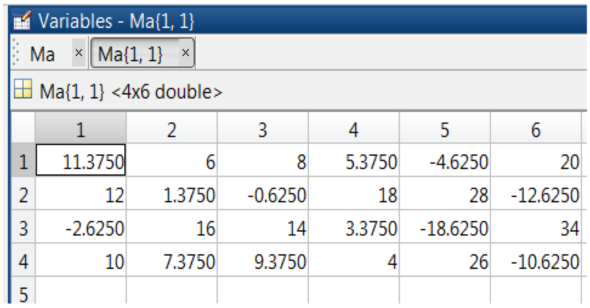
Simulation result is discussed using the Matlab tool. The plaintext is simulated to get numerical value in fig 1.2 ASCII value representing the corresponding data is taken as the numerical value of the plain text .



```
Enter the Text
happy
Plain Text
    104    97    112    112    121
```

Figure 1.2: numerical value of plain text

Newly modified magic rectangle is formed based on the initial value given col sum , row sum values are based on the initial value. The formation of NNMR is shown in fig 1.3.



	1	2	3	4	5	6
1	11.3750	6	8	5.3750	-4.6250	20
2	12	1.3750	-0.6250	18	28	-12.6250
3	-2.6250	16	14	3.3750	-18.6250	34
4	10	7.3750	9.3750	4	26	-10.6250
5						

Figure 1.3 : NNMR formation

The value of the colsum and the rowsum will be equal it is described through the table 1.1

11.375	6	8	5.375	-4.625	20	46.125
12	1.375	-0.625	18	28	-12.625	46.125
-2.625	16	14	3.375	-18.625	34	46.125
10	7.375	9.375	4	26	-10.625	46.125
30.75	30.75	30.75	30.75	30.75	30.75	

Table 1.2

Numerical value and the plain text values are combined together and form the single value this new value is placed the same position of the magic rectangle this is shown in table 1.3.

115.375	**127**	8	5.375	-4.625	20
109	1.375	-0.625	18	28	-12.625
109.357	16	14	3.375	-18.625	34
122	7.35	9.375	4	26	-10.625

Table 1.3 NMMR with text value

In the above table 1.3 the text value is added in column wise of the magic rectangle. The position of the value is unchanged. The iterative fisher Yates shuffling is done to the table 1.3 to obtain the cipher text. The steps of the iterative fisher algorithm is shown in the following tables.

8	20	-4.625	115.375	127	5.375
- 0.625	-12.625	28	109	1.375	18
14	34	-18.625	109.375	16	3.375
9.375	-10.625	26	122	7.375	4

Table 1.4 First iteration

127	5.375	115.375	8	20	-4625
1.375	18	109	-0.625	-12.625	28
16	3.375	109.375	14	34	-18.625
7.375	4	122	9.375	-10.625	26

Table 1.5 second iteration

8	115.375	20	-4.625	127	5.375
-625	109	-12.625	28	1.375	18
14	109.375	34	-18.625	16	3.375
9.375	122	-10.625	26	7.375	4

Table 1.6 Third iteration

The basic shuffle done in the iteration is described in detail using the tables. For illustration first iteration is taken.

115.375	127	5.375	8	20	-4.625
109	1.375	18	-0.625	-12.625	28
109.375	16	3.375	14	34	-18.625
122	7.375	4	9.375	-10.625	26

5.375	127	115.375	8	20	-4.625
18	1.375	109	-0.625	-12.625	28
3.375	16	109.375	14	34	-18.625
4	7.375	122	9.375	-10.625	26

127	5.375	115.375	8	20	-4.625
1.375	18	109	-0.625	-12.625	28
16	3.375	109.375	14	34	-18.625
7.375	4	122	9.375	-10.625	26

8	20	-4.625	115.375	127	5.375
-0.625	-12.625	28	109	1.375	18
14	34	-18.625	109.375	16	3.375
9.375	-10.625	26	122	7.375	4

8	20	5.375	115.375	127	-4.625
-0.625	-12.625	18	109	1.375	28
14	34	3.375	109.375	16	-18.625
9.375	-10.625	4	122	7.375	26

8	127	5.375	115.375	20	-4.625
-0.625	1.375	18	109	-12.625	28
14	16	3.375	109.375	34	-18.625
9.375	7.375	4	122	-10.625	26

The final matrix is obtained by shuffling all the rows in the matrix using fisher Yates shuffle algorithm.

III. RESULT AND CONCLUSION

In this work, strong algorithm has been proposed for data security by combining new modified magic rectangle and iterative fisher Yates shuffle algorithm. The repeatation of character in data is overcome through NMMR and complexity of the data is increased by introducing IFYS the shuffle algorithm along with NMMR. The data is hard to retrieve without the knowledge of magic pattern and shuffling order.

IV. REFERENCES

[1]. A.J. Menezes ,P.C Van Oorschot, and S.Vanstone , “Handbook of Applied cryptography”, CRC Press , boca Ration, Florida, USA.

[2]. W.Diffle and M.E hellman, “New directions in cryptography”, IEEE Transactions on information theory vol IT-22 nov 1976.

[3]. Ueli M. Maurer and Yacov Yacobi “Non-interactive public-key cryptography” Advances in cryptology-EUROCRYPT’91, Springer.

[4]. B.Alomair and P.poovendran, “E-MACs:toward more secure and more efficient construction of secure channels” IEEE transaction on computers, vol 63, No.1, January 2014.

[5]. Dr.Mamta sood, Manohar Wagh, and Monika Cheema “A review on various data security techniques in wireless communication system” journal of engineering research and applications (IJERA) vol.3, issue 2, April 2013.

[6]. D.I George Amalerethinam, J.Sai Geetha and K.Mani “Add-on security level for public key cryptosystem using magic rectangle with column/row shifiting” international journal of computer applications vol 96-No-14 june 2014.

[7]. Sapna Saxena and Bhanu Kapoor “An efficient parallel algorithm for secured data communication using RSA public key cryptography method”IEEE International Advance Computing Conference(IACC) 2014.

[8]. Charanjit S Jutla “ Encryption modes with almost free message intergrity” IBM T.J >Watson Research center,Yorktown Heights,USA.

[9]. Zeenat MahmoodJ. L Rana ,Ashishkhare “Symmetric Key Cryptography using Dynamic Key and Linear Congruential Generator (LCG)” International Journal of Computer Applications, July 2012

[10]. Hongjun WANG, Zhiwen SONG, Xiaoyu NIU and qun DING “Key Generation Research Of RSA Public Cryptosystem And Matlab Implement” International Conference On Sensor Network Security Technology And Privacy Communication System, May2013.

[11]. GopinanathGanapathy and K.Mani “Add-On Security Model For Public-Key Cryptosystem Based On Magic Square Implementation” Proceeding Of The World Congress On Engineering And Computer Science Vol1, October 2009.

[12]. Ganeshkumar. K Arivazhagan. D and Sundaram. S “Advance cryptography algorithm for symmetric image encryption and decryption scheme for improving data security” Journal Of Academia And Industrial Research(JAIR) VOL 2, MARCH 2014.

[13]. Ade-lbjola and AbejideOlu “A Simulated Enhancement of Fisher-Yates Algorithm for Shuffling in Virtual Card Games Using Domain-Specific Data Structures” International Journal Of Computer Application Vol 54, September 2012.

[14]. D. I. George Amalarethinam and J.SaiGeetha“An enhancement security level of public key cryptosystem using MRGA” IEEE, DOI 10.1109/ WCCT 2014.32.