Data Security Measures using Hybrid Encryption Technique

Ankit Vishnoi, Durgansh Sharma, Manish Prateek

Abstract*: *Data security is a process of enhancing the data privacy measures to filebase, database, websites while preventing unauthorized access to the datasets and data-streams. Encryption is the key data security technique that prevents the access of digital data from unauthorized person or hackers. This research work proposes a novel approach using data transformation and encapsulation techniques namely Hadamard Transform along with DNA Cryptography and Amino Acid for enhancing data security.

Index Terms: Hadamard Transform, Amino acids, DNA Cryptography, Encryption.

I. INTRODUCTION

In the current environment of digital complexities and data challenges, there are various techniques available towards data security. Data is generated by the user, stored or forwarded to a specific computing terminal. The process of encoding is implemented by the program or algorithm; encrypt the data into cipher text, which makes it unreadable and useless. This cipher can only be decrypted into plaintext with the use of right key. Cryptography is the method of transforming plaintext into cipher text using cryptographic techniques and key. These algorithms are complex mathematical calculations and methods. Later, cipher text transforms into plain text with the use of reverse cryptographic techniques. This process is also defined as encryption and decryption. We are proposing a novel approach to secure data using transformation and encapsulation of data. This cipher technique will transform existing malicious system into optimally secure computing environment. In this paper, the proposed method has been presented in two parts: first, the Hadamard Transform applied to the data and in second half, the data is encapsulated using DNA and Amino Acid sequence.

II. EXISTING WORK

Encryption estimation anticipates basic part in correspondence security. Our examination work inspected the execution of existing encryption strategies like AES, DES and RSA estimations. In light of the substance records used and the preliminary outcome, it was assumed that AES computation eats up smallest encryption and RSA consumes longest encryption time. We also watched that Decryption of AES count is better than various figurings. From the re-enactment result, we surveyed that AES computation extraordinarily improved than DES and RSA figuring. The work will focus on idea about analyzing existing cryptographic computations like AES, DES and RSA. It will join preliminaries on picture and sound data and focus will be to improve encryption time and unscrambling time [1]. Extortion has been found in present business structure: money falsified, checks changed, Visa numbers hacked, which concludes, whatever implemented in the area of security, examined because of usability and accuracy. Thus, researcher must concentrate to develop secure method for the data correspondence [2]. In RSA, encryption and decryption utilizes measured exponentiation. Quick particular exponentiation calculations have pragmatic hugeness in RSA. In place of calculating the entire sequence of numbers in one go, better to calculate sub sequence of numbers in parallel, which in result, would enhance the proficiency of algorithm. In addition, it decreases the computational overhead and saves time to enhance the quality of system [3]. Mandal composed a calculation by blending RSA calculation and one other algorithm to give a more elevated amount of information security [4]. Hadamard Transform is the transform which changes 2^m genuine numbers s_n into 2^m genuine numbers S_k. The Hadamard Transform can characterized by utilizing twofold portrayal of files n and k [5]. Encoding of the data sequence using amino acid structure can performed by applying DNA cryptography. DNA Cryptography is a process of encapsulating data sequence by using Amino Acid sequence. It can be done by using genetic codes to replace by the characters [6-10].

III. PROPOSED WORK

Transformation using Fast Walsh Hadamard Transform

Fast Hadamard Transform converts 2^i numbers into 2^j numbers [5], by dividing them into two equal halves.

Revised Manuscript Received on July 08, 2019.
Ankit Vishnoi, School of Computer Science, UPES, Dehradun, India.
Dr. Durgansh Sharma, School of Computer Science, UPES, Dehradun, India.
Dr. Manish Prateek, School of Computer Science, UPES, Dehradun, India.

The method of converting 2^i numbers into 2^j numbers by following steps:

Forward Hadamard code for 8 bit data:
Step1:

```
for(z=0;z<8;z++)
  printf("a[%d] = %d\n", z,a[z]);
  printf("\n");
```

```
  b[0]=a[0]+a[4];
  b[1]=a[1]+a[5];
  b[2]=a[2]+a[6];
  b[3]=a[3]+a[7];
  b[4]=a[0]-a[4];
  b[5]=a[1]-a[5];
  b[6]=a[2]-a[6];
  b[7]=a[3]-a[7];
```

Step2:

```
for(z=0;z<8;z++)
  printf("b[%d] = %d\n", z,b[z]);
  printf("\n");
  c[0]=b[0]+b[2];
  c[1]=b[1]+b[3];
  c[2]=b[0]-b[2];
  c[3]=b[1]-b[3];
  c[4]=b[4]+b[6];
  c[5]=b[5]+b[7];
  c[6]=b[4]-b[6];
  c[7]=b[5]-b[7];
```

Step3:

```
for(z=0;z<8;z++)
  printf("c[%d] = %d\n", z,c[z]);
  printf("\n");
  d[0]=c[0]+c[1];
  d[1]=c[0]-c[1];
  d[2]=c[2]+c[3];
  d[3]=c[2]-c[3];
  d[4]=c[4]+c[5];
  d[5]=c[4]-c[5];
  d[6]=c[6]+c[7];
  d[7]=c[6]-c[7];
  for(z=0;z<8;z++)
  printf("d[%d] = %d\n", z,d[z]);
  printf("\n");
```

Similarly for Backward Hadamard:
For each step, we need to run this code each time

```
for(z=0;z<8;z++)
   {
        b[z]=(((a[z][0])  *  (c[0]))+((a[z][1])  *
(c[1]))+((a[z][2])  *  (c[2]))+((a[z][3])  *
(c[3]))+((a[z][4])  *  (c[4]))+((a[z][5])  *
(c[5]))+((a[z][6]) * (c[6]))+((a[z][7]) * (c[7])))/8;
   }
```

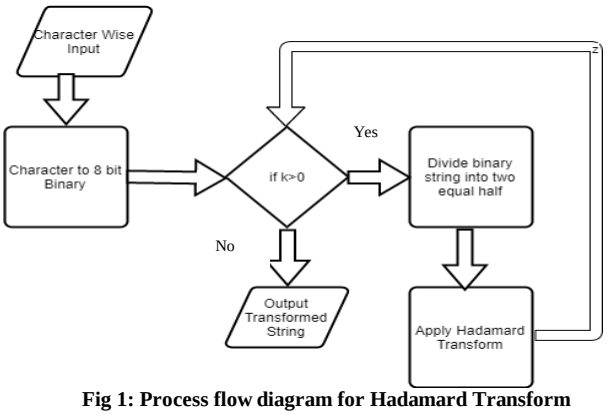

Fig 1: Process flow diagram for Hadamard Transform

Above method can summarized as depicted in Fig 2.

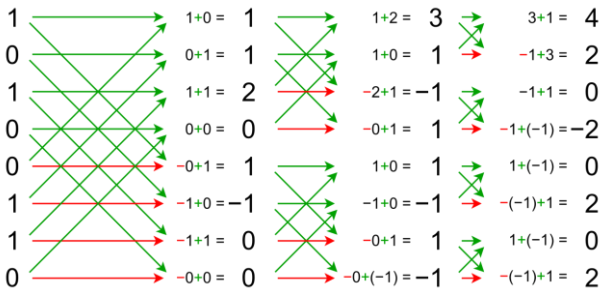

Fig 2: Fast WHT Representation

The input binary sequence 10100110 is transformed into 420-20202. The complexity calculated for above method is O (N $\log_2$ N). This transformed sequence further encapsulated with the DNA Cryptography is described below.

Encapsulation Using DNA and Amino Acid

The encapsulation is done by representing the data sequence into amino acid sequence. The sequence received from the Fast Hadamard Transform can easily be converted into binary form. These binary forms are encapsulated to the DNA form, to convert all the letters into Amino Acid process required to generate codons for the English letters. This can be achieved as shown in Fig 3.

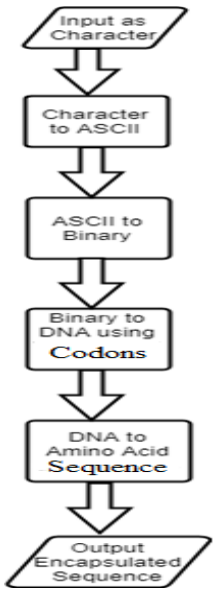

Fig 3: Process flowchart for encapsulation

Table 1: Paper Pen encapsulation of character string to amino acid sequence

Input	4	0	0	0
ASCII	52	48	48	48
Binary	110100	110000	110000	110000
DNA	AT CA	AT AA	ATAA	ATAA
Amino	M Q	M N	M N	M N

The following can represented by taking transformed string and applying encapsulation on it. Let us consider '4000' as input as shown in Table 1. Therefore, the final encapsulated string will be 'MQMNMNMN'. O (Log2 N) defines the complexity of the encapsulation process.

IV. CONCLUSION

The proposed mathematical model is suitable for any type of data and provides the optimal security with the complexity of [O (N Log_2 N)]. The advantage of this proposed method is that, it only does the mathematical calculations, which reduces the computational overhead. The implementation of this proposed mathematical model is under progress, which will further entail towards comparison with the existing cipher techniques to reassure the optimal outcome of our work done.

ACKNOWLEDGMENT

We are grateful to Dr Durgansh Sharma, Associate Professor, SCS, UPES Dehradun and Dr. Manish Prateek, Professor, SCS UPES Dehradun for their guidance in writing this paper.

REFERENCES

[1] P. Mahajan and A. Sachdeva, "A Study of Encryption Algorithms AES, DES and RSA for Security," Global Journal of Computer Science and Technology Network, Web & Security, Volume 13 Issue 15 Version 1.0, 2013.
[2] K. Acharya, M. Sajwan and S. Bhargava, "Analysis of Cryptographic Algorithms for Network Security," International Journal of Computer Applications Technology and Research, Volume 3– Issue 2, pp. 130-135, 2014.
[3] C. Wu and C. Hu, "Computational Complexity Theoretical Analyses on Cryptographic Algorithms for Computer Security Application", 2012 Third International Conference on Innovations in Bio-Inspired Computing and Applications, 2012.
[4] B. K. Mandal, D. Bhattacharyya and S. Kumar Bandyopadhyay, "Designing and Performance Analysis of a Proposed Symmetric Cryptography Algorithm," in International Conference on Communication Systems and Network Technologies, Gwalior, India, 2013.
[5] D. Sharmila and R. Neelaveni, "A Proposed SAFER plus security algorithm using Fast Walash Hadamard transform for Bluetooth Technology," International Journal of Wireless & Mobile Networks (IJWMN), pp. 80-87, 2009.
[6] Y. M and E.A, "Amino Acids in Data Encryption," Journal of Analytical & Pharmaceutical Research, 2016.
[7] N. V and U. Nanaji, "A Simple Message-Encryption Scheme based on Amino-acid Protein Sequence," International Journal on Computer Science and Engineering (IJCSE), pp. 3547-3551, 2011.
[8] M. Sabry and M. Hashem, "Three reversible Data Encoding Algorithms based on DNA and Amino Acids' Structure," International Journal of Computer Applications, pp. 24-30, 2012.
[9] S. Namdev and V. Gupta, "A DNA and Amino Acid Based Implimentation of Four Square Cipher," International Journal of Engineering Research and Applications, pp. 90-96, 2016.
[10] A. Atito, A. Khalifa and S. Rida, "DNA-Based Data Encryption and Hiding Using Playfair and Insertion Techniques", Journal of Communications and Computer Engineering, vol. 2, no. 3, p. 44, 2011.

AUTHORS PROFILE

Ankit Vishnoi, Assistant Professor (Senior Scale) at University of Petroleum and Energy Studies. He has done his B. Tech (Computer Science), from U.P. Technical University, M. Tech (Computer Science), from Gautam Buddh Technical University, Lucknow and is currently pursuing PhD from University of Petroleum and Energy Studies. His area of interests include Mobile Computing, Computer Networks, Cyber Security, and Cloud Computing.

Dr. Durgansh Sharma, Associate Professor at University of Petroleum and Energy Studies. He completed his B.Sc. (Electronics), from Delhi University, M.Sc. (Computer Science), from Maharishi Dayanand University, Masters (Computer Science), from Maharishi Dayanand University, M. Tech. (Comp. Sc.) from IETE, PGDBA (IMM) and Ph.D (Computer Science), University of Petroleum and Energy Studies, Dehradun. His area of research includes AI based decision support systems; Enhancing human vision using Machine Vision, Deep neural networks assisted target detection, Melancholy detection through Video analytics, Sports analytics, Healthcare and alternative medicines, Business Analytics, Image Processing, Data Security, and has published more than 25 papers in these areas.

Dr. Manish Prateek, Professor & Dean, School of Computer Science at University of Petroleum and Energy Studies. He has done his Ph. D. in the area of Manufacturing & Robotics in the year 2005. He started his career in 1996 as a customer support engineer with franchises of HCL Info systems Ltd. and gradually grew up to the level of Manager Information Technology by 2004. He has more than 50 publications in the area of Robotics, Image Processing and Data Security.