A New Approach for Data Encryption Using Genetic Algorithms and Brain Mu Waves

Gove Nitinkumar Rajendra, Bedi Rajneesh kaur

Abstract: In today's computer world security, integrity, confidentiality of the organization's data is the most important issue. This paper deals with the confidentiality of the data that organization manages and works with. This paper proposes a new approach to data security using the concept of genetic algorithm and brain mu waves with pseudorandom binary sequence to encrypt and decrypt the data. The feature of such an approach includes high data security and high feasibility for practical implementation.

Index Terms—Mu waves, Genetic algorithms, Pseudorandom binary sequence, Encryption, Crossover operator, Data security, Confidentiality.

INTRODUCTION

Recently, due to the big data losses from illegal data access, data security has become an important issue for public, private and defense organizations. In order to protect this valuable data or information from unauthorized readers and illegal modifications and reproductions various types of cryptographic techniques are used.

There are two basic types of cryptographic techniques [1],[2]: symmetric and asymmetric cryptography. In symmetric cryptography, same key is used for encryption and decryption. While in asymmetric cryptography, two different keys are used, one for encryption called public key and another for decryption called private key.

Symmetric key algorithms are typically fast and are suitable for processing large stream of data. Some of the popular and efficient symmetric algorithms include Twofish, Serpent, AES, Blowfish and IDEA etc. There are other encryption algorithms which are proposed. Genetic algorithms [4] are among such techniques.

Generally, genetic algorithms contain three basic operators: reproduction, crossover and mutation [5].

Reproductions and crossover together gives the genetic algorithms most of their power.

This paper proposes a new approach for encrypting large volume of organization data and highly secret personal data or information. First, an 8 character long string is interpreted from the mu waves generated by the brain. Second, a pseudo random binary sequence is generated from the string obtained after processing above string. Third, the first character string and the pseudorandom sequence is applied to crossover operator which will output two keys which then are concatenated to get a final 512 bit key.

This key is then used to encrypt and decrypt data.

The rest of the paper is organized as follows. In section 2, the proposed method is introduced. Section 3 gives the analysis of proposed method. Section 4 concludes the paper.

1. THE PROPOSED METHOD

The proposed method block diagram is shown in fig 1. It consists of key generation logic, encryption and decryption modules, which are explained in following subsections.

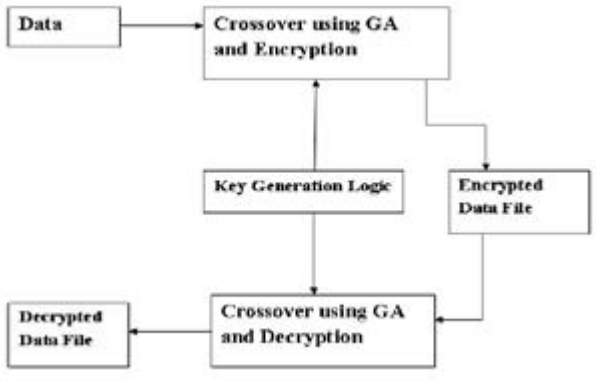

Fig 1.The Block Diagram of Proposed Method

- *Gove Nitinkumar Rajendra is currently pursuing bachelors degree program in computer engineering in Pune University, India, E-mail: gove.nitinkumar@gmail.com*
- *Rajneesh Kaur Bedi is Head of the Department of computer engineering in MITCOE, Pune University, India. E-mail: meenubedi@hotmail.com*

1.1 The Key Generation Logic

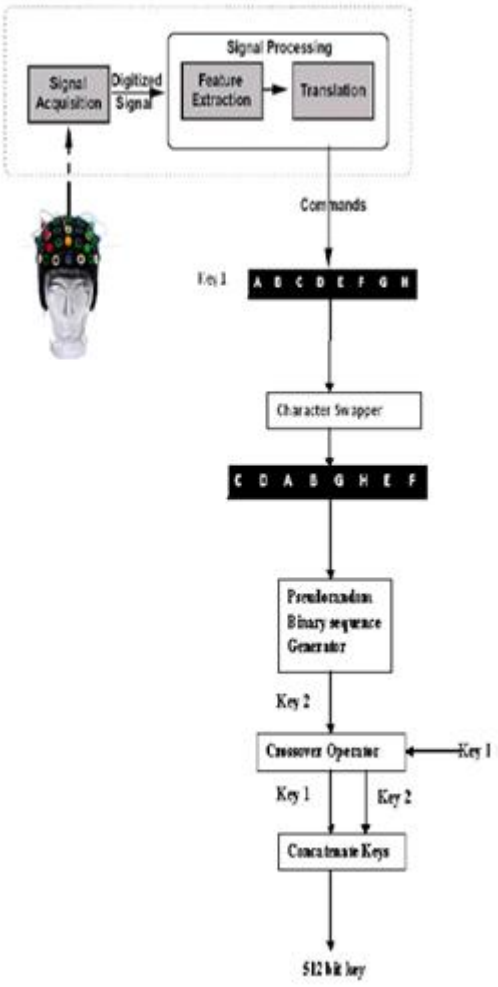

Fig 2.Block Diagram for Key Generation Process

Fig 2 shows the model of key generation logic. It consists of sensory input detection unit which is responsible for detecting the mu waves of the pass though of user (pass thought is the thinking which is used as a key in latter processing.) and interpreting appropriate characters that the user is thinking about to press. This involves signal acquisition, feature extraction, and finally translation.

The other modules involved in this are character swapper, pseudorandom binary sequence generator and crossover operator. The pseudorandom binary sequence generator is explained in following subsections.

2.1.1 Character Swapper

There are mainly two function performed by this unit. First is, separating the characters according their position i.e., odd or even. Then each two consecutive odd/even positioned characters are swapped with their next character.

2.1.2 Pseudorandom Binary Sequence Generator

Fig 3 shows a general model of PRBSG [3]. It is a non linear forward feedback shift register with a feedback function f and non linear function g.

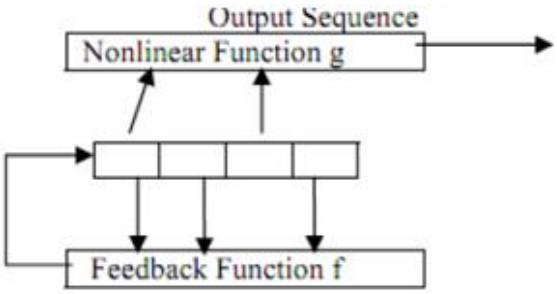

Fig 3.A General Model Of 4 bit NLFFSR

When register is loaded with a non-zero value, a pseudo random sequence with very good randomness and statistical properties is generated.

The only signal required for the operation of this module clock pulse. The balance, run and correlation properties of the sequence generated make it more useful for generating the private key.

2.1.3 Crossover Operator

Crossover in simple words is a process in which two strings are mixed such that they match their desirable qualities in a random fashion.

Crossover operator proceeds in three steps as given below:

1. Two new strings are selected.

2. A random location from strings is selected.

3. The portions of strings on right side are swapped together.

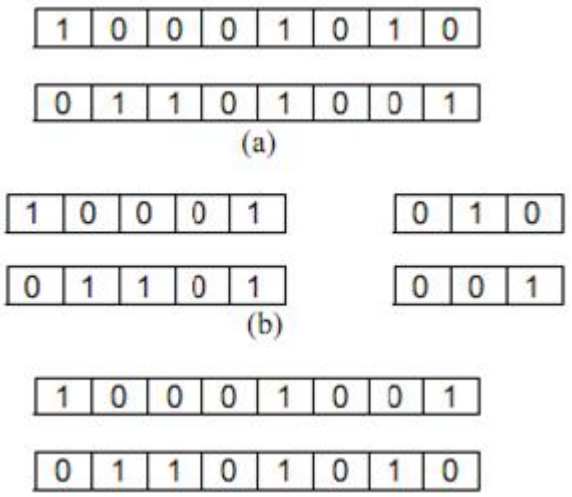

Fig 4. Illustration of crossover operator

2.1.4 Key Generation Process

The key generation algorithm used here produces a very strong key which is very difficult to guess even with exhaustive search. The process of key generation is as given below:

1. Scan the pass thought. Take the string generated after sensing, filtering and processing Mu waves. This is key1.

2. Pass this string to the character swapper.

3. Pass the non zero output of character swapper to the pseudo random binary sequence generator.

4. The output of PRBSG is key2.

5. Both key1 and key2 are 256 bit long.

6. Apply both these keys to crossover operator.

7. Finally, concatenate the two strings generated at

after crossover operation.

This whole process is depicted in fig 2.

2.2 The Encryption Process

The encryption process emulates the operation of key generator and crossover operator. The encryption process comprises of following steps:

1. Generate the key using the key generator logic as Kn.

2. Take mode 8 of the key generated to get decimal value ranging from 0 to 7.

3. Kn =mod (Kn, 8)

4. Initialize i=0

5. Take two consecutive bytes of the data file as A1 and A2

6. Crossover the two consecutive bytes of the data file as B1 and B 2 Using the number Ki.

7. Encrypt data as C1 and C2 .This is done as follows:

Xi=Ki XOR Ki << 4

Xi+1=ki+1 XOR ki+1 <<4

C1=Bi XOR X1

C2=B2 XOR Xi+1

And i=i+2

Repeat steps 4 to 6 until end of the file.

2.3 The Decryption Process

The steps for encryption are just reversal of the encryption. First extract the key1 from sensory output, then obtain key2 through character swapper, generate PRBS and then the key, apply the process using crossover operator decrypt the data.

3. PERFORMANCE ANALYSIS

It should be checked that, if a data is encrypted by the proposed technique whether it can be easily decrypted or not. Since there are M combinations to encrypt 2 consecutive data bytes, thus the number of possible encryption results is M (N/2), where N is the total number of bytes in data to be encrypted and M is the length of one data byte.

The speed of the algorithm is good.

But, the initial key generation process takes some time which may decrease the throughput of the algorithm and may increase the execution time by some seconds.

4. CONCLUSION

This paper proposes a new approach for data security. It uses the concept of brain Mu waves, genetic algorithms and pseudorandom binary sequence. This methodology of scurrying the confidential data is highly safe and reliable. So, without the secret thought of the person i.e., the key no one will be able to extract the data. Since, the

pass thought is unpredictable is unpredictable it is very difficult to decrypt correctly without knowing the initial pass thought. The proposed method is very sensitive to the changes in pass thought. In the future work, we plan to implement a system implementing this methodology and provide security to highly confidential and secret data in defense and other institutions.

ACKNOWLEDGMENT

We wish to thank the Dept. of Computer Engineering, MIT COE for their important support.

REFERENCES

[1] Douglas, R. Stinson, "Cryptography - Theory and Practice", CRC Press, 1995. [6] Goldberg D.E., "Genetic algorithms in search optimization & Machine learning", Addison- Wesley, 1989.

[2] Menzes A. J., Paul, C., Van Dorschot, V., anstone, S. A., "Handbook of Applied Cryptography", CRS pess 5th Printing; 2001.

[3] Ahmad A., Al-Musharafi M. J., Al-Busaidi S., Al-Naamany A., and Jervase J. A., "An NLFSR Based Sequence Generation for Stream Ciphers", Proceedings of International Conference on Sequences and their Applications, pp. 11-12, 2001.

[4] Tragha A., Omary F., and A. Kriouile, "Genetic Algorithms Inspired Cryptography" A.M.S.E Association for the Advancement of Modeling & Simulation Techniques in Enterprises, Series D: Computer Science and Statistics, 2005.

[5] Tragha A., Omary F., Mouloudi A.,"ICIGA: Improved Cryptography Inspired by Genetic Algorithms", Proceedings of the International Conference on Hybrid Information Technology (ICHIT'06), pp. 335-341, 2006.