Faiyaz Ahamad, Saba Khalid,Mohd.Shahid Hussain/ International Journal of Engineering Research and Applications
(IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue 3, May-Jun 2012, pp.3049-3051

Encrypting Data Using The Features of Memetic Algorithm and Cryptography

Faiyaz Ahmad*, Saba Khalid, Mohd. Shahid Hussain*
Department of Information Technology, Integral University
Department of Computer Science and Engineering, Integral University
Lucknow,226026, India

Abstract—The proposed system highlights an approach for encrypting data using the concept of memetic algorithm and cryptography. This approach yields high data security ,integrity and feasibility for practical implementation.

Keywords-*Geneticalgorithm(GA);Memetic algorithm;Crossover; Encryption ; Decryption*

I. INTRODUCTION

In the advent of greater demand of computer for business transactions illegal data access is a major threat to combat data security. To prevent this threat various cryptographic methods are employed to maintain confidentiality, authenticity and integrity of the data.
In this paper we have used a variation of genetic algorithm that is memetic algorithm in cryptographic techniques to secure data. Cryptography is the science of making communication unintelligible to everyone except the intended receiver[1][2]. A cryptosystem is a set of algorithms indexed by some keys of encoding message into cipher text and then deciphering into plaintext. There are two types of cryptographic techniques[3][4]:- symmetric key and asymmetric key cryptography .In symmetric key cryptography same key is used for encryption and decryption where as in asymmetric key cryptography two keys are used namely public key and private key for encryption and decryption.

Genetic algorithm is a randomized search and optimization technique guided by the principle of natural genetic systems. Genetic algorithms contain three basic operators: reproduction, crossover and mutation [5].The GA goes through the following cycle: Evaluate, select, mate, and mutate until some stopping criteria are reached. The memetic algorithms [6] can be viewed as a marriage between a population-based global technique and a local search made by each *of* the individuals. They are a special kind of genetic algorithms with a local hill climbing. Like genetic algorithms, memetic Algorithms are a population-based approach. They have shown that they are orders of magnitude faster than traditional *genetic Algorithms* for some problem domains. In a memetic algorithm the population is initialized at random or using a heuristic. Then, each individual makes local search to improve its fitness. To form a new population for the next generation, higher quality individuals are selected. The selection phase is identical inform *to* that used in the classical genetic algorithm selection phase. Once two parents have been selected, their chromosomes are combined and the classical
Operators of crossover are applied to generate new individuals. The latter are enhanced using a local search technique. The role of local search in memetic algorithms is to locate the local optimum more efficiently then the genetic algorithm. In this paper we have proposed the system for encrypting and decrypting data using the concept of variation of genetic algorithm and cryptography in a different manner.

Rest of the paper is as follows: Section II, covers the various cryptography techniques based on genetic algorithm as available in the literature in chronological order is given. In Section III a new approach of genetic algorithms (GA) with pseudorandom sequence to encrypt data stream is proposed. Section IV represents the analysis of the security. Finally, section V concludes the paper with special emphasis of highlighting the areas of further research.

II. RELATED WORK

Only few genetic algorithms based encryption have been proposed. A. Kumar et al [7] describe encryption using the concept of the crossover operator and pseudorandom sequence generator by NLFFSR (Non-Linear Feed Forward Shift Register). The crossover point is decided by the pseudorandom sequence and the fully encrypted data they are able to achieve. A. Kumar et al [8] further extended this work and used the concept of mutation after encryption. Encrypted data is further hidden inside the steno-image. A. Tragha et al.[9, 10], described a new symmetrical block ciphering system named ICIGA (Improved Cryptography Inspired by Genetic Algorithms) which generates a session key in a random process. The block sizes and the key lengths are variable and can be fixed by the user at the beginning of ciphering. ICIGA is an enhancement of the system (GIC) ―Genetic algorithms Inspired Cryptography‖ [10].

ICIGA is a block cipher system whose secret key is generated during each session using a random process. The user can fix the size of the blocks as well as the length of the key. The operation of ICIGA depends on the length of the secret key selected by the user. ICIGA uses this length to divide the plaintext into parts of equal size. During the ciphering, the first part is broken up into blocks of the same size which are used to generate the secret key. This key will then be used to cipher the other parts of the message. If the user did not set the length of the secret key the plaintext is composed of only one part and ICIGA generates a key maximum length. M. Husainy [11] proposed Image Encryption using Genetic Algorithm based Image Encryption using mutation and crossover concept. A. Tragha [12] at al proposed a new encryption algorithm using genetic algorithm approach. The only related work is the attack of the asymmetric ciphering ―Knapsack Cipher. This is inspired by the resolution of back bag problem. Thus efficiency genetic algorithms have been proven in cryptanalysis. The problem of ciphering a message M is modeled as a combinatorial optimization problem. Then a genetic solution based on the method used to solve the traveling salesman problem (TSP) is also proposed. In the second system SEC-EX , for scrambling plaintext, they introduce a new technique, which consists to encode plaintext in binary, chooses randomly an integer k and cuts plaintext into blocks of size k.

III. THE PROPOSED MODEL

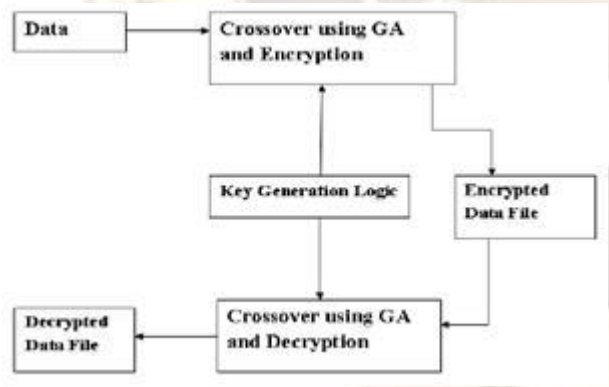

Figure1. The proposed method for data seurity

The block diagram of the proposed method is shown in figure 1. It consists of pseudorandom sequence generator, crossover operator, and encryption and decryption modules.

A. *The Key Generation Logic*

In key generation procedure nine parameters are used which provide strength to the algorithm rendering it difficult for cryptanalysis by intruder. The nine parameters of the key are:-

Key={Xn, a, c, m, Popbuffer, first no, last no, mod, remainder}

Where

a) Xn,a,c,m are the parameters of Linear Congruential method whose values are known only to the intended sender and recipient.

b) Population buffer is the buffer in which random numbers are generated.

c) First no is the number to start in population buffer.

d) Last no is the number to end within the pop buffer.

e) Mod is the number used to extract only those number to be used for substitution which give the remainder.

f) Remainder is obtained when the no between starting and ending no are divided by modulus.

1) *PRNG using GA and Linear Congrential Method*

The most widely used technique for PRNG is an algorithm proposed by Lehmer, Which is known as Linear Congrential Method. The algorithm is parameterized by four numbers as follows:

m the modulus m>0
a the multiplier 0<=a<m
c the increment 0<=c<m

the sequence of random number is obtained via the following iterative formula:

Xn+1=(aXn + c) mod m

Where Xn is the seed value which is kept secret.

B. *The Encryption Process*

The encrypting process of proposed model makes use of GA in a deterministic way to generate Pseudo random numbers. The encryption process emulates the working of the crossover operator and mutation operator deterministically. The encryption process emulates the operation of key generator and crossover operator. The encryption process comprises of following steps:

1. Generate the Pseudo random sequence using the Linear Congrential method.
2. Take mode 8 of the Pseudo random sequence generated to get decimal values ranging from 0 to7
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.
8. Again perform byte substitution over encrypted data to further create confusion.

C. *The Decryption Process*

The steps for decryption are just reversal of the encryption. First generate the pseudorandom sequence using LGM and then use the pseudorandom sequence and cross over operator to decrypt the data.

IV. 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.

Time analysis of the proposed method: The speed of the algorithm is the important factor for a good encryption algorithm. We have measured the encryption/decryption rate for several gray scale images of different size. The average time taken by the algorithm for different size of images is shown in table 1.

Table 1: Average ciphering speed of some grey scale images

Image size in Pixels	Bit depth	Average encryption/decryption time
128X128	8	0.0009-0.0013
256X256	8	0.037-0.046
512X512	8	0.068-0.0110

V. CONCLUSION

This paper proposes a new approach for data security. It uses the concept of memetic algorithms and pseudorandom binary sequence. This methodology of securing the confidential data is highly safe and reliable. In future work we are planning to design a sophisticated hardware based on this technique which will be targeted to use in highly secure multimedia data transmission applications.

REFERENCES

[1] David E.Goldberg,"Genetic algorithm in search,optimization and machine learning"Addision-Wesley Pub.Co. 1989
[2] A.J.Bagnall,"The application of Genetic algorithm in cryptanalysis",School of Information Systems,University of East Anglia,1996.
[3] Douglas, R. Stinson, "Cryptography - Theory and Practice", CRC Press, 1995. [6] Goldberg D.E., "Genetic algorithms in search optimization & Machine learning", Addison- Wesley, 1989.
[4] Menzes A. J., Paul, C., Van Dorschot, V., anstone, S. A., "Handbook of Applied Cryptography", CRS pess 5th Printing; 2001.
[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.
[6] P, Moscato, "on evolution, scorch, optimization. genetic algorithm and martial arts: toward memetic algorithms", Technical report, California, 1989.
[7] A Kumar, N Rajpal, ―Application of Genetic Algorithm in the Field of Steganography‖, in Journal of Information Technology, Vol. 2, No.1, Jul-Dec.2004, pp-12-15.
[8] A Kumar, N Rajpal, A. Tayal, ―New Signal Security System for Multimedia Data Transmission Using Genetic Algorithms‖ NCC'05 Held in the IIT Kharagpur, pp-579-583, 28-20 Jan 2005.
[9] A. Tragha, F. Omary, 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, November 2005.
[10] A. Tragha, F. Omary, A. Mouloudi,‖ ICIGA: Improved Cryptography Inspired by Genetic Algorithms‖, 2006 International Conference on Hybrid Information Technology (ICHIT'06).
[11] M. Husainy, ― Image Encryption using Genetic Algorithm‖ , Information Technology Journal 5 (3):pp 516-519, 2006.