Volume 2, Issue 4, April 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Secret Key Encryption Algorithm Using Genetic Algorithm

Ankita Agarwal
IMSEC, Ghaziabad (India)
ankita.890@gmail.com

Abstract: ***In today's information age, information sharing and transfer has increased exponentially. Security, integrity, non-repudiation, confidentiality, and authentication services are the most important factors in information security. In now days the security of digital images attracts much attention, especially when these digital images are stored in memory or send through the communication networks. Many different image encryption methods have been proposed to keep the security of these images. Image encryption technique tries to convert an image to another image that is hard to understand. Genetic algorithms (GAs) are a class of optimization algorithms. Many problems can be solved using genetic algorithms through modelling a simplified version of genetic processes. In this paper, I proposed a method based on Genetic Algorithm (GA) which is used to produce a new encryption method by exploitation the powerful features of the Crossover and Mutation operations of (GA).***

Keywords: ***Genetic Algorithm, Mutation, Encryption, Decryption, Secret key, Cryptography***

1. Introduction

Basically Gas are a heuristic search, optimization and machine learning [1] techniques based on the principles of the Darwinian idea of Survival of the fittest and natural genetics.

Cryptography is the science of making communication unintelligible to everyone except the intended receiver(s). It is the study of methods of sending messagesin disguised form so that only intended recipients can remove the disguise and read the message. Cryptography offers efficient solution to protect sensitive information in a large number of applications including personal data security, internet security, diplomatic and military communications security, etc. through the processes of encryption/decryption. A cryptosystem is a set of algorithm, indexed by some keys(s), for encoding messages into cipher text and decoding them back into plaintext [3] and [4]. The model for a secret key system, first proposed by Shannon [2] is shown in Fig. 1

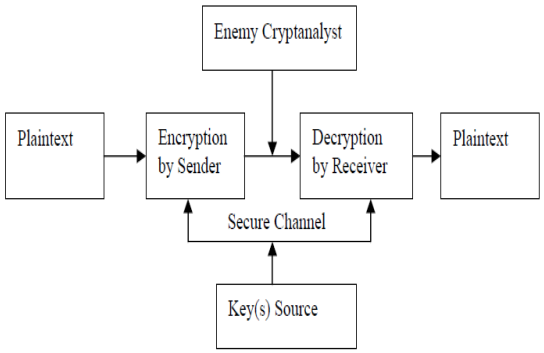

Fig. 1: Shannons model of secret communication

Generally, genetic algorithms contain three basic operators: reproduction, crossover, and mutation, where all three are analogous to their namesakes in genetics. Reproduction and crossover together give genetic algorithms most of their searching power. A simple GA is mainly composed of three operations: selection, genetic, and replacement operation.

Many genetic algorithm based encryption have been proposed. A. Tragha et al.[5, 6], describe 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 length are variable and can be fixed by the user at the beginning of the ciphering. ICIGA is an enhancement of the system (GIC) "Genetic algorithms Inspired Cryptography" [7].

In this paper, a new approach of Genetic Algorithm is proposed in which, the operations of GA (Crossover and Mutation) are exploited to produce this encryption method. This new method was applid to the candidate type of data i.e. images.

This paper organized in Sections. Firstly we describe the introduction of Genetic Algorithm and Cryptography under the heads of Introduction in Section-I. Subsequently we have gone through the literature review and found problems and solutions in several papers. All this we have mentioned under heads of Backgrounds in Section-II. In Section-III, the proposed method is described in detail. Finally, this paper concluded and mentions its further enhancements under future scope in Section – IV and Section-V respectively. All used references used during writing of this paper are mention in Section –VI under head of references.

2. Backgrounds

Several solutions have been proposed in this area. In 1993, for the first time, the paper by Spillman [8] presented a genetic algorithm based approach for the cryptanalysis of substitution cipher. The paper has explored the possibility of random type search to discover the key (or key space) for a simple substitution cipher.

In the same year Mathew used an order based genetic algorithm for cryptanalysis of a transposition cipher. In 1993, Spillman [9] successfully applied a genetic algorithm approach for the cryptanalysts of a knapsack cipher also. In 2006, Garg studied that the efficiency of genetic algorithm attack on knapsack cipher can be improved with variation of initial entry parameters.
In 2006, Garg [10] study gives the base that genetic algorithm can be used to break S-DES. In 2008 Garg [11] explored the use of memetic algorithm to break a simplified data encryption standard algorithm.
In 2006, Nalini [12] compared the attack of SDES using Optimization Heuristics technique and GA based techniques. The results show that GA based approach minimizes the time complexity.

3. Proposed Method

The overall procedure is summarized as follows:

Algorithm for Encryption

Step 1: Consider an image I (W*H)
Where W and H are width and height of L
Split the image I to a set of N vectors of length L where L=8 bytes.

Step 2: (crossover operation)
For 1 = 0... N-l, each vector Vi from the set of N vectors:
Do crossover
We use secret key for crossover. In our research secret key have two attributes termed a, b
belonging to 1 to 8. We do crossover by swapping a to b in each vector
V1 [b0, b1, b2, b3, b4, b5, b6, b7]
For example
let the secret keys are 3 and 5 and we do crossover on vector V1 then
V1 becomes [b1, b2, **b5**, b4, **b3**, b6, b7, b8]

Step 3: (mutation operation)
For each vector Vi
Do mutation by an another secret key of single variable of k.
By the Vi [bk] = 255- V i[bk]
For example let the secret key is 4 and we do mutation on vector V1 then
V1 becomes [b1, b2, b5, (**255-b4**), b3, b6, b7, b8]

Step 4: Construct an encrypted image from the set of N vector that are produced from the
Mutation.

Algorithm for Decryption

Step 1: In the encrypted image
Split the image in N vectors of L=8

Step 2:
For each vector Vi
Do the reverse mutation by secret key k
i.e. Vi[bk]= 255 – Vi[bk]
For example let the secret key is 4 and we do reverse mutation on vector V1 then
V1 becomes [b1, b2, b5, **(255-(255-b4))**, b3, b6, b7, b8]
Now V1 becomes [b1, b2, b5, **(b4)**, b3, b6, b7, b8]

Step 3:
For 1 = 0... N-l, each vector Vi from the set of N vectors:
Do reverse crossover by using secret key b to a
We do crossover at this time by swapping b to a in each vector Vi
Vi [b0, b1, b2, b3, b4, b5, b6, b7]
For example
let the secret keys are 3 and 5 and we do crossover on vector V1 then
V1 becomes [b1, b2, **b3,** b4, **b5**, b6, b7, b8]

Step 4: Construct an image from the set of N vectors that are produced from the step 3.

4. Conclusion

In this paper, I propose a genetic algorithm based secret key image encryption method. After the examinations of the proposed method, it is clear that this encryption method is satisfied the goals that are required in any encryption method for encrypt images.

5. Future Work

In this paper, Genetic algorithm based secret key image encryption method is presented. In the future work, there is a planning to design a sophisticated software based on this technique which will targeted to use in highly secure multimedia data transmission applications.

REFERENCES

[1] David E Goldberg, 'Genetic algorithms in search, optimization and machine learning',Addision- Wesley Pub.Co.1989.

[2] C.E.Shannon, "Communication Theory of Security System",Bell,System Technical Journal, 28, 1949

[3] A.J.Bagnall, "The Applications of Genetic Algorithms in Cryptanalysis", School of Information Systems, University Of East Anglia, 1996.

[4] N.Koblitz , 'A Course in Number Theory and Cryptography', Springer-Verlag, New York, Inc., 1994.

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

[6] National Bureau Standards, "Data Encryption Standard (DES)," FIPS Publication 46; 1977

[7] 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.

[8] Spillman R,Janssen M, Nelson B and Kepner N, "Use of Genetic Algorithm in Cryptanalysis of Simple Substituion Cipher" Cryptologia, Vol.17, No.4, pp. 367-377, 1993.

[9] Spillman R,"Cryptanalysis of Knapsack Ciphers using Genetic Algorithms", Cryptologia, Vol.17, No.4, pp. 367-377, 1993.

[10] Garg Poonam, Genetic algorithm Attack on Simplified Data Encryption Standard lgorithm, International journal Research in Computing Science, ISSN1870-4069, 2006.

[11] Garg Poonam, Memetic Algorithm Attack on Simplified Data Encryption Standard Algorithm, proceeding of International Conference on Data Management, February 2008, pg 1097-1108 .

[12] Nalini, Cryptanalysis of Simplified data encryption standard via Optimization heuristics, International Journal of Computer Sciences and network security, vol 6, No 1B, Jan 2006.

