ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 1, Issue 10, December 2012

Using Genetic Algorithm for Symmetric key Generation in Image Encryption

Aarti Soni, Suyash Agrawal

***Abstract*- Cryptography is essential for protecting information as the importance of security is increasing day by day with the advent of online transaction processing and e commerce. In now a day the security of digital images attracts much attention, especially when these digital images are stored in memory or send through the communication networks. Genetic algorithms 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 which is used to generate key by the help of pseudo random number generator. Random number will be generated on the basis of current time of the system. Using Genetic Algorithm we can keep the strength of the key to be good, still make the whole algorithm good enough. Symmetric key algorithm AES has been proposed for encrypting the image as it is very secure method for symmetric key encryption.**

***Index Terms*-Cryptography, Genetic Algorithm, Pseudo random Number Generators, Symmetric Key Cryptography.**

I. INTRODUCTION

Recently with big losses from illegal data access and, with the greater demand in digital signal transmission, data security has become a critical issue in multimedia data transmission applications. To protect valuable information from unauthorized access or against illegal reproduction and modifications, various types of cryptographic schemes are needed.

There are two types of cryptographic schemes based on the key used:

A. Symmetric Cryptography

Here same key is used for encryption and decryption. Symmetric key cryptography is one of the most important types of cryptography where key is shared between both the communicating parties. Symmetric key cryptography is used for private encryption of data to achieve high performance. For e.g. AES, IDEA, DES, etc.

B. Asymmetric Key Cryptography

Two different keys are used in Asymmetric cryptography where key for encryption is known as the public key, and the other for decryption, known as the private key. For e.g. RSA, Diffie - Hellman.

II. SECURITY OF THE KEY

In the literature review, it was observed that the characteristics feature that determine the strength of the key are not quantifiable but matrices might be used for evaluating and comparing cryptographic algorithm .

The characteristics that are considered are Type: Symmetric or Asymmetric; Functions: Integrity and authentication of message; Key size and rounds; and the complexity of the algorithm. The attacks that can be carried out to test the strength of the algorithm are brute force attack and differential cryptanalysis. The matrices that have been used to judge the effect of these attacks are based on the key length and complexity of the algorithm from which key is generated.

A. Pseudo Random Number Generator (PRNG)

Pseudo random number generators are used to generate a sequence of number that approximates the properties of random numbers. Pseudorandom numbers are practiced for their speed in number generation and their reproducibility.

III. GENETIC ALGORITHM

Genetic algorithm [5] is a randomized search and optimization technique guided by the principle of natural selection systems. Three basic operators used in Genetic algorithms contain: selection, crossover and mutation. The GA goes through the following cycle: Evaluate, select, mate, and mutate until some stopping criteria are reached. Reproduction and crossover together give genetic algorithms most of their searching power.

A. Selection

It is quantitative criterion based on fitness value to choose the chromosomes from population which are going to reproduce.

B. Crossover

In crossover operation two chromosomes are taken and a new is generated by taking some attributes of first chromosome and the rest from second chromosome.

For example, the strings 11001011 to 01101010 could be crossed over after the third locus in each to produce the two offspring 11001010 to 01101011. There are three

type of crossover operation Single Point Crossover, Two Point Crossover, Uniform Crossover.
Figure 2 showed the working of crossover operator.
Fig (a) illustrates the bits contained in two strings.
Fig (b) both the strings are detached from their third locus.
Fig (c) new population after crossover operation.

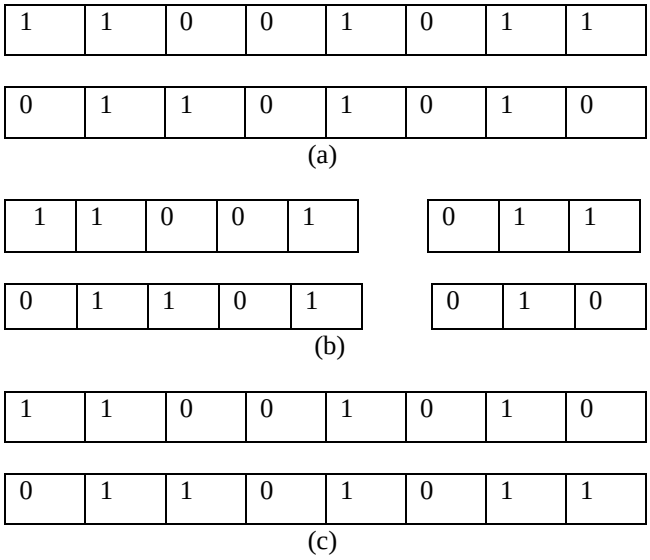

Fig 1. Working of Crossover Operator

C. Mutation

Mutation is used to maintain genetic diversity from one generation of population to the next. It is similar to biological mutation. GAs involves string-based modifications to the elements of a candidate solution. These include bit-reversal in bit-string GAs. This operator randomly flips some of the bits in a chromosome.

For example, the string 00000100 might be mutated in its second position to yield 01000100.
The basic GA Cycle has been showed in fig1.

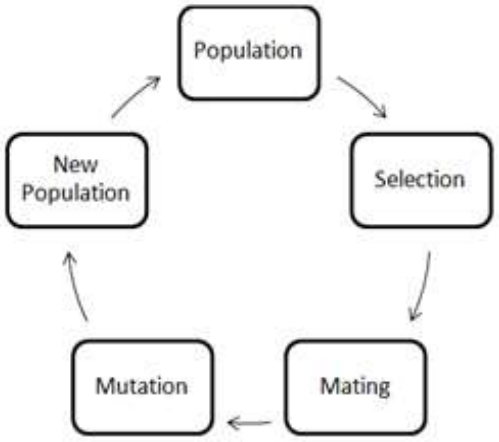

Fig 2. Basic Model of Genetic Algorithm

IV. RELATED WORK

Only few genetic algorithms based cryptographic scheme have been proposed. A. Kumar [6] describes encryption by the use of crossover operator and pseudorandom sequence generator by NLFFSR (Non-Linear Feed Forward Shift Register). Pseudorandom sequence decides the crossover point and the fully encrypted data are achieved. A. Kumar et al [7] further extended the work and used mutation after encryption. Encrypted data is further hidden inside the steno-image. A. Tragha [8, 9], described a new symmetrical block ciphering approach named ICIGA (Improved Cryptography Inspired by Genetic Algorithms) where session key is generated in a random process. ICIGA is an enhancement of the system (GIC) ―Genetic algorithms Inspired Cryptography [9]. Ankita [4] applied GA in the encryption algorithm using secret key for encryption process.

Soniya Goyat [1] stated that if the quality of the random numbers produced by the method is good then the key generated will always be strong. The author used a threshold value for selection. The coefficient of correlation is used to check the randomness of the sample. Faiyaz Ahamad [3] proposed a model which makes use of GA to generate Pseudo random numbers. The encryption process follows the working of the crossover operator and mutation operator. It uses the concept of memetic algorithms and pseudorandom binary sequence. In key generation procedure nine parameters of linear congruential generators are used. Nitin [2] 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.

V. PROPOSED METHODOLOGY

In the proposed method GA will be used in key generation process. The crossover and mutation operation is used along with Pseudo random number generators to make the key very complex. For encryption we have proposed AES. Symmetric key algorithm is proposed due to its computation speed and less overhead in key management.

The process of generating the key from the Genetic Population has the following steps:

STEP 1: A pseudo random binary sequence is generated on the basis of current date using millisecond function.
STEP 2: The generated string or population is divided in to two halves.
STEP 3: On the selected string crossover operation is performed to achieve good randomness among the key.
STEP 4: After crossover operation the bits of the string are swapped again to permute the bit values.
STEP 5: The same process is iterated two times.
Figure 3 illustrate the above step.

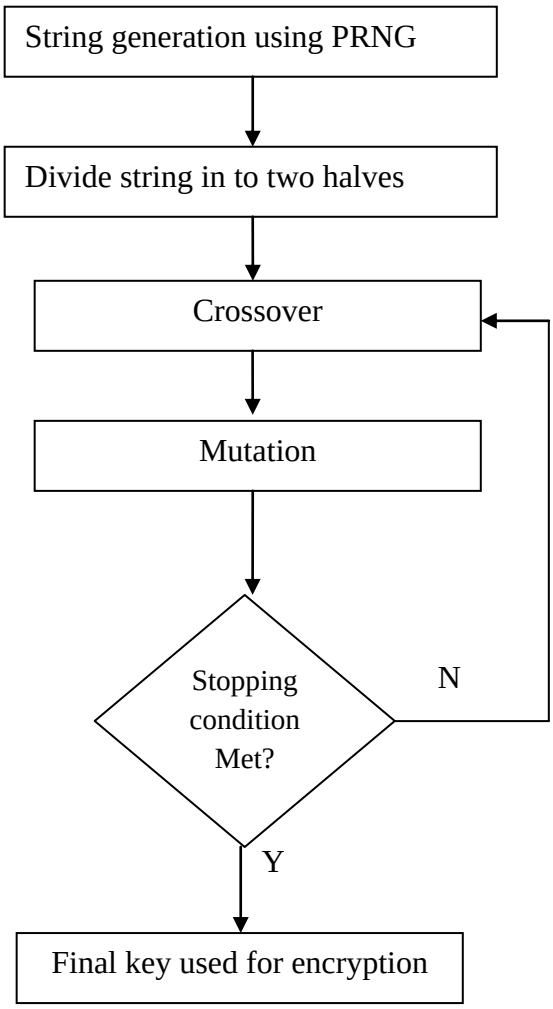

Fig 3. Key Generation Process

Here the crossover and mutation is done two times to create more complexity and randomness in the key. This key will be then used for encryption process. Here AES will be used for encryption as it is one of the most efficient symmetric key algorithms and its whole security lies in the key used.

VI . EXPECTED OUTCOME

This paper proposes a new approach for data security.The proposed algorithm will increase the efficiency of the algorithm in terms of computation time required and complexity to attack the message. It uses the concept of pseudorandom number generator and genetic algorithms to increase the complexity of key by increasing the irregularity of the key.

Implementation of Genetic Algorithm with PRNG a very complex key which is very difficult for cryptanalyst to attack and encrypting using AES symmetric key encryption algorithm will provide an efficient method for encrypting image and increasing the overall efficiency of the system . The result can be viewed with the help of graphs.

REFERENCES

[1] Sonia Goyat, "Genetic Key Generation For Public Key Cryptography", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-3, July 2012 231.

[2] Nitin Kumar, Rajendra Bedi, Rajneesh Kaur, "A New Approach for Data Encryption Using Genetic Algorithms and Brain Mu Waves", International Journal of Scientific and Engineering Research Volume 2, Issue 5, May-2011 ISSN 2229-5518.

[3] Faiyaz Ahamad, Saba Khalid, Mohd. Shahid Hussain published a paper entitled, "Encrypting Data Using The Features of Memetic Algorithm and Cryptography" at International Journal of Engineering Research and Applications, Vol. 2, Issue 3, May-Jun 2012, pp.3049-3051.

[4] Ankita Agarwal, "Secret Key Encryption Algorithm Using Genetic Algorithm" at IJARCSSE, 2012.

[5] Anil Kumar and M. K. Ghose,"Overview of Information Security Using Genetic Algorithm and Chaos", Information Security Journal: A Global Perspective, 18:306–315, 2009.

[6] 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.

[7] 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.

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

[9] A. Tragha, F. Omary, A. Mouloudi, "Improved Cryptography Inspired by Genetic Algorithms", ICIGA, 2006 International Conference on Hybrid Information Technology (ICHIT'06).

Aarti Soni. She was born in Chhattisgarh on 28th October 1986. She has got her bachelor's degree BE –Computer Science &Engineering from Chhattisgarh Swami Vivekananda Technical University, Bhilai. Chhattisgarh, India. At present she is pursuing M.Tech from RCET Bhilai in 3rd semester and working as a lecturer in CSE Department in GDRCET, Bhilai. Her area of interest in field of research includes Cryptography.

Suyash Agrawal. He was born on 12th August 1983. He has got his post graduate degree M.Tech- CSE from CSVT University, Bhilai and bachelors degree BE- CSE from RCET Bhilai. He has published a number of papers in leading international journals. At present he is working as Reader in Computer Science Dept. RCET Bhilai. His area of interest in the field of research includes Image Processing.