Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 6, June 2013, pg.376 – 383

RESEARCH ARTICLE

Key Generation Using Genetic Algorithm for Image Encryption

Aarti Soni[1], Suyash Agrawal[2]
[1]Computer Science& Engineering, CSVTU, India
[2]Computer Science& Engineering, RCET, India

[1] *aarti.oct@gmail.com;* [2] *suyash.agrawal1983@gmail.com*

***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. Now a day the security of digital images are major area of concern, especially when we deal with digital images where it may be stored or send through the communication channel. Genetic algorithms are a class of optimization algorithms. Genetic algorithms can be used to solve different problems through modeling a simplified version of genetic processes. This paper proposed a method based on Genetic Algorithm which is used to generate key by the help of random number generator to make the key complex. Key generation will go through a number of process and main criteria for key selection will be the fitness value of the population. AES which is a symmetric key encryption algorithm is used to encrypt the image.**

Key Terms: - Cryptography; Random Number Generator; Genetic Algorithm; AES

I. INTRODUCTION

Now a day unauthorized access of data and, with the greater demand in digital signal transmission, data secrecy has become a vital 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. Cryptography is used to change the original data in to unreadable format with the help of key. Greater complexity involved in the key generation process make it difficult for the cryptanalyst to attack the key. 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 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 parameters used to judge the effect of these attacks are based on the key length and complexity of the algorithm from which key is generated. Key can be made complex by increasing the complexity involved in generation process. It will become very difficult for a cryptanalyst to attack the key. In this paper random number generator is used to generate key and genetic algorithm is used to make the key more complex. Which key should be selected will entirely depends on the fitness value of the different strings generated by random number.

A Random Number Generator (RNG)

A random number is a number generated such that it cannot be predicted, and which is difficult to reproduce sequentially and reliably. 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. Random numbers are numbers that occur in a sequence such that two conditions are met:

(1) The distribution of values are uniform across a defined set interval or, and

(2) Prediction of future values on the basis of past or present ones is impossible.

III. GENETIC ALGORITHM

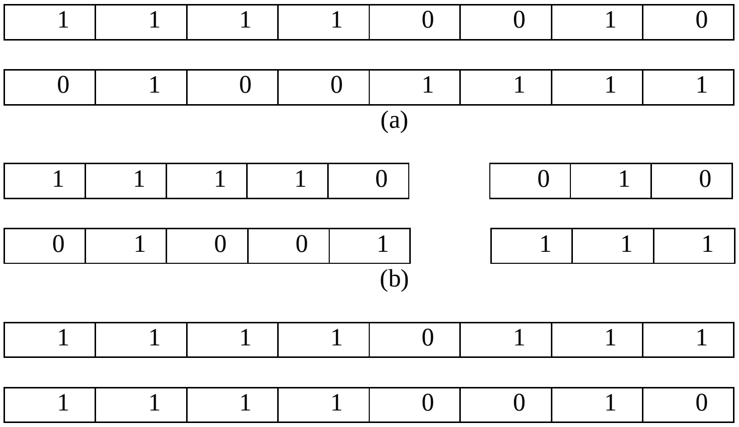
Genetic algorithm [5] is a randomized search and optimization technique guided by the principle of natural selection systems. Three basic operators used in Genetic algorithms contain: selection, crossover and mutation. The GA goes through the following cycle: Selection, crossover, and mutate until some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

A. *Selection*

It is quantitative approach where the chromosomes from populations are chosen to reproduce based on fitness value of chromosomes.

B. *Crossover*

In crossover operation two chromosomes are taken and a new is generated by taking some features of first Chromosome and the rest over from the another or second chromosome. For example, the strings 11110010 and 01001111 could be crossed over after the third locus in each to produce the two offspring 11110111 and 01001010. 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.



1	1	1	1	0	0	1	0
0	1	0	0	1	1	1	1

(a)

1	1	1	1	0		0	1	0
0	1	0	0	1		1	1	1

(b)

1	1	1	1	0	1	1	1
1	1	1	1	0	0	1	0

(c)

Fig 1. Working of Crossover Operator

C. *Mutation*

Mutation is used to maintain genetic diversity from one generation to the next generation of population. It is similar to biological mutation. GAs involves string-based modifications to the elements of a candidate solution.

These include bit-reversal in a string of bits Gas. These operators randomly interchange two bits or simply flip the bit in a chromosome. For example, the string 00000111 might be mutated in its fifth position to yield 00001111. The basic GA Cycle has been showed in fig1.

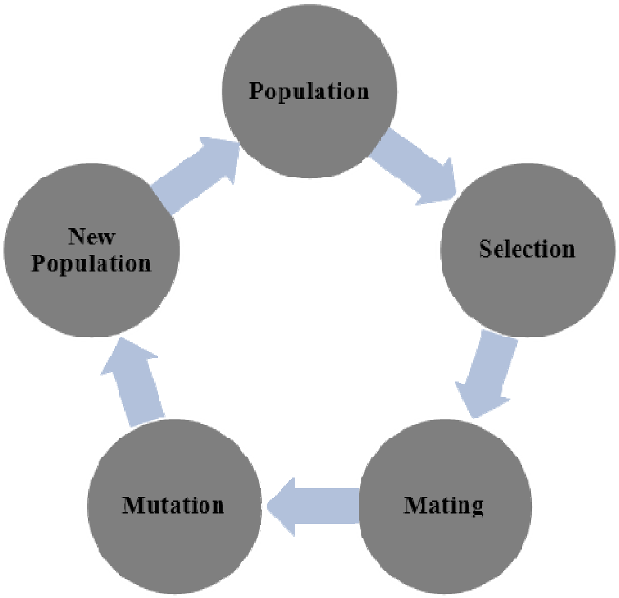


Fig 2. Basic Model of Genetic Algorithm

In the above figure the process starts with initial population. From the initial population the individuals which in having maximum fitness value are selected for the further process. Fitness value is calculated from the fitness function. The selected population is the mated using cross over operation and mutated to generate new best individuals.

IV. Advance Encryption Standard

AES is a symmetric block cipher. It means that it uses the same key or a single key for both encryption and decryption. The algorithm is based on Rijndael principle which allows a variety of block and key sizes. The block and key can be chosen independently from 128, 160, 192, 224, 256 bits and need not be the same. The AES standard states that the algorithm can only accept a block size of 128 bits and a choice of three keys - 128, 192, 256 bits. A number of AES parameters depend on the key length. For example, if the key size used is 128 then the number of rounds is 10 whereas it is 12 and 14 for 192 and 256 bits respectively. At present the most common key size likely to be used is the 128 bit key.

The algorithm begins with an Add round key stage followed by 9 rounds of four stages and a tenth round of three stages. This applies for both encryption and decryption with the exception that each stage of a round the decryption algorithm is the inverse of its counterpart in the encryption algorithm. The four stages are as follows:

1. Substitute bytes
2. Shift rows
3. Mix Columns
4. Add Round Key

The tenth round simply eliminates the Mix Columns step.

V. 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 than hidden by masking with 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 randomness quality of the numbers produced by the method is good then the generated key will always be strong. The author used a threshold value for selection. The randomness of the sample was checked by the coefficient of correlation. 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 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.

VI. METHODOLOGY

The generation of initial population of chromosomes is in hexadecimal number using random function. This initial population is 128 bit long. Here 'n' number of population is generated. All this individuals are sent to a fitness function. This fitness function is a maxima function which means that the individual which is having maximum fitness value is selected for the further process. After this process we select two best individuals. On the selected individuals one point crossover is performed and the point of crossover is decided on the basis of a random number. After performing crossover we get the offspring of the selected individuals. Now again fitness function is applied on the children and if their fitness value is better than the parent, then parents are replaced by the children otherwise not. Now the output of previous step will work as input of mutation operation. After mutation we will get the final key which will be used for encryption process. The key generation process from the Genetic Population has the following steps:

A. *Initial Population Generation:*

128 bit long initial populations of chromosomes are generated using a random number generator in decimal number.

B. *Conversion:*

The decimal number is converted in to hexadecimal number.

C. *Fitness Calculation:*

The fitness value of each individual is calculated. The fitness value is calculated on the basis of symbol which is repeated maximum. The fitness function can be expressed as:

$$\boxed{\mathbf{F = n + (€ /m)}}$$

Where F = Fitness Function.
n = Total number of symbols used in key formation.
m = Percentage of maximum appeared symbol.
€ = Ideal Percentage of each symbol.

D. *Crossover:*

On the randomly selected two chromosomes one point cross over is performed on the basis of a random value. After crossover operation we get two new offspring's generated from their parent chromosome.

E. *Fitness Check:*

Now again the fitness checking is done on the new child chromosome and if they are found better than the previous one are replaced by their child otherwise not.

F. *Mutation:*

Now mutation is performed on a randomly selected chromosome and its new fitness value is calculated.

G. *Fitness Check*

Again Fitness value of whole population of that particular run is checked and maximum one is taken in to account.

The whole process is performed hundreds of time. In each iteration population having maximum fitness value is recorded. After the stopping condition is met the population with maximum fitness value is selected as a key for encryption. Figure 3 illustrate the key Generation Process.

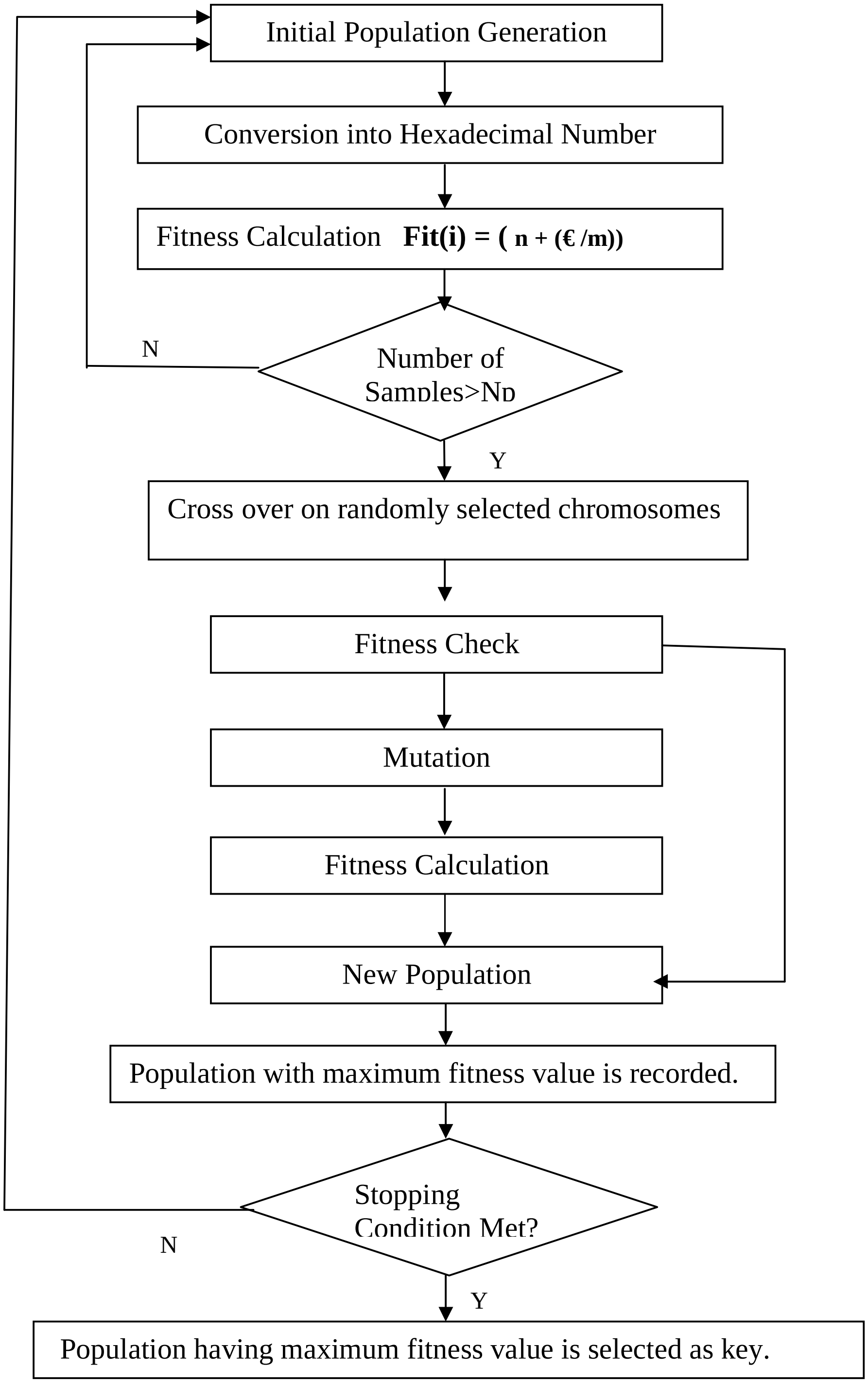

Initial Population Generation
Conversion into Hexadecimal Number
Fitness Calculation Fit(i) = (n + (€ /m))
Number of Samples>Np
N
Y
Cross over on randomly selected chromosomes
Fitness Check
Mutation
Fitness Calculation
New Population
Population with maximum fitness value is recorded.
Stopping Condition Met?
N
Y
Population having maximum fitness value is selected as key.

Fig 3. Key Generation Process Using Genetic Algorithm

For encryption, Advanced Encryption Standard (AES) has been used. Symmetric key algorithm is proposed due to its computation speed and less overhead in key management.

VII. RESULT

The work has been implemented and analyzed .The implementation has been done in Mat lab. The Mean of the maximum fitness value collected at different runs has been calculated. Standard deviation is also calculated. Graph has been plot against mean and standard deviation. The work has been tested for 500 iteration with 10 population and 15 runs each. The various graphs obtained are as follows.

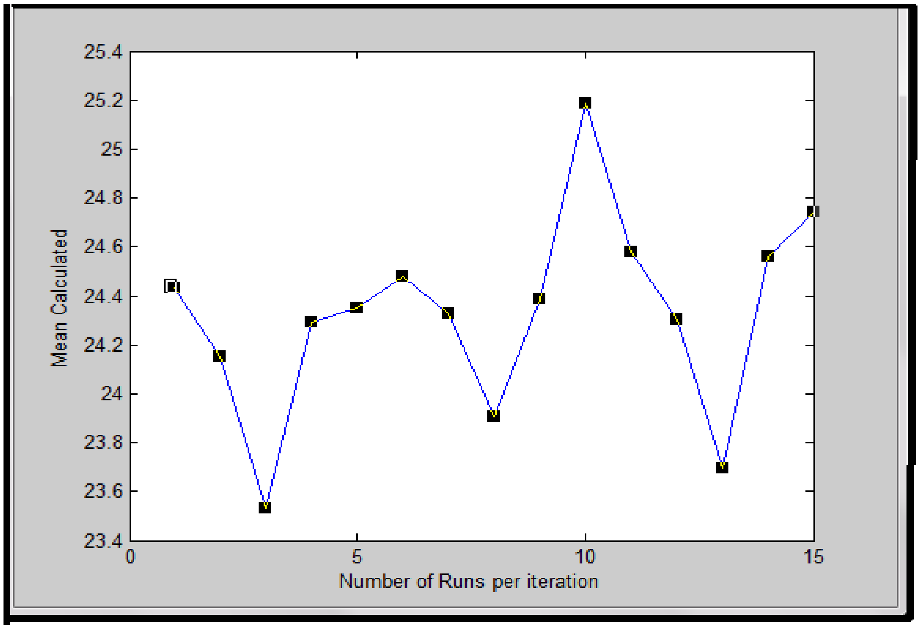


Fig 4. Mean

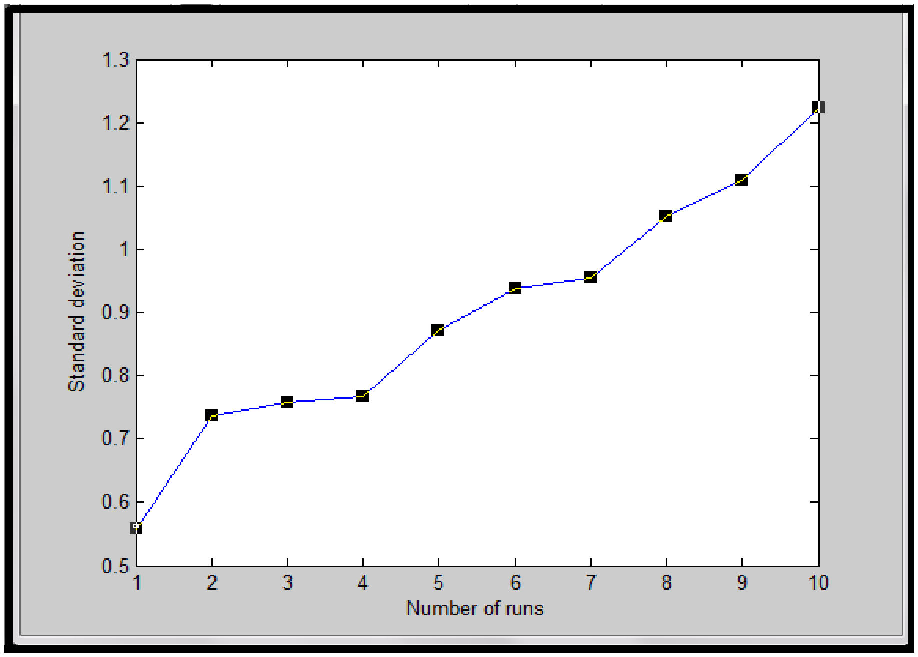


Fig 5. Standard Deviation

Encryption and decryption has also been carried out using AES algorithm. Encryption was carried out on more than 10 images but here only 2 images are shown here. One is colored and another is gray scale image.

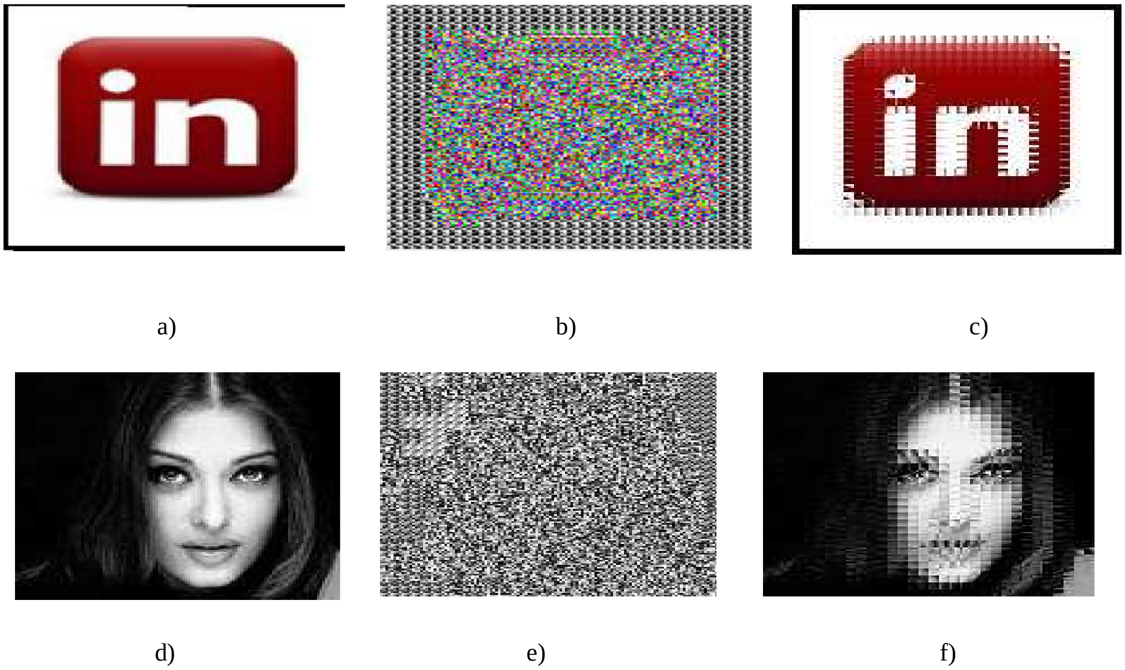


Fig 6. a) In image b) Encrypted Image c) Decrypted Image d) Aish Image e) Encrypted Image c) Decrypted Image

In Fig 6. a) 'in" is the original coloured image b) is the encrypted "in" image and fig 6.c) is the decrypted image. Fif 6. d) Aishwarya gray scale image, e) is encrypted image and f) is the decrypted image.

It can be seen in the encrypted figure that the original image is not at all predictable.

VIII. Conclusion

The work has been carried out for hundreds of sample. Each population varies greatly from another. Key length for which test is carried out is 128 bit long. Longer key sequence will also work but time constraint does not permit to check. The time taken to generate key for 300 iteration with 10 new population each time and 10 crossover and mutation operations each iteration is 75.382 seconds. Encryption and decryption is also performed but in decryption some data are lost. In future it can be implemented using different algorithm with no data loss.

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, 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 Modeling & 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).