A Study on Cryptography using Genetic Algorithm

Rajat Jhingran
M.Tech Pursuing. (CSE)
Amity University Haryana

Vikas Thada
Asst. Prof, Dept. (CSE)
Amity University Haryana

Shivali Dhaka
Asst. Prof, Dept. (CSE)
Amity University Haryana

ABSTRACT

Cryptography is a basic tool for protection and securing data. Security provides safety, reliability and accuracy. Genetic Algorithm (GA) is typically used to obtain solution for optimization and search problems. This paper presents application of GA in the field of cryptography. The selection of key in the field ofpublic key cryptography is a selection process in which keys can be categorized on the basis of their fitness function, making GA a better candidate for the key generation. We propose a new approach for e-security applications using the concept of genetic algorithms with pseudorandom sequence to encrypt and decrypt data stream. Many different image encryption methods have been proposed to keep the security of these images. Image encryption algorithms try to convert an image to another image that is hard to understand.

General Terms

Genetic algorithm,Crossover,Mutation, Selection, Encryption, Decryption.

Keywords

Secret key cryptography, Pseudo random binarysequence generator.

1. INTRODUCTION

In this section we are going to describe the basics of genetic algorithm, cryptography with the help of some algorithms based on crossover, mutation, and selection etc. A very vast technique related to the generation of secret key cryptography and random number is applied under this concept.

1.1 Genetic Algorithm

The Genetic algorithm is a search based on the mechanics of natural selection and natural genetics. The main idea is that in order for a population of individual to adapt to some kind of environment, it must behave like a natural system. This generally means that survival and Re-production of an individual is promoted by the elimination of useless or harmful traits and by rewarding with some useful behavior. Basically, a GA starts with a randomly generated set of individuals. Once the starting population has been created, the genetic algorithm directly enters in a loop. At the last of each iteration, a newly population has been produced by applying a certain number of stochastic operators to the previous population. That type of iteration is known as a generation. The genetic algorithm uses two reproduction operators - crossover and mutation.

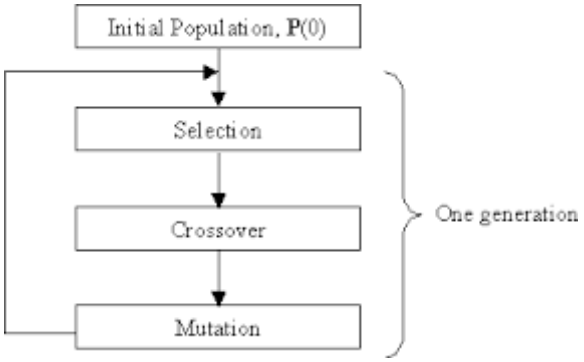

Figure 1). Flow chart of genetic algorithm

To apply a crossover operator, parents are paired together. There are several different types of crossover operator functions, but the types available depend on what representation is used for the individuals. For the binary string individuals, one-point, two-point, and uniform crossover function, mutation is applied.

The purpose of the mutation operator is to simulate the effect of transcription errors that can happen with a very low probability when an individual is mutated. A standard mutation operator for binary strings is a bit inversion means '0' would mutate into '1' and vice versa.

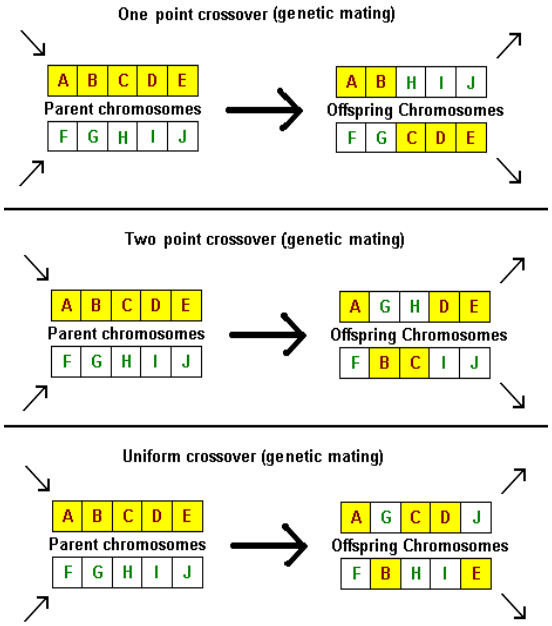

Figure 2). Types of Crossover

Cycle can be summarized as follows- generation = 0Seedpopulation

While not (termination condition) do

Generation = generation + 1
Calculate fitness
Selection
Crossover
Mutation
End
Toughest application areas for genetic algorithms include:
• Image Encryption
• Graph Applications such as
– Coloring
– Paths
– Circuit Layout
• Scheduling
• Satisfiability
• Game Strategies
• Chess Problems.

1.2 Cryptography

Cryptography technique is used when secret message are transferred from one party to another over a communication series. Cryptography technique needs some algorithm and techniques to play its role as better as it can.

Key generation in cryptography has been given with in many papers but the use of GA in the process has not as yet been explored. It is the most important part of encoding the data .A non-repeating key guarantees better results and generates a code that is theoretically impossible to break .Some of the classical techniques used for generating unique keys are Pseudo random number generators and OTP. Original message is known as the plain text and coded message is known as cipher text. Encryption or Enciphering: the process from converting plain text to cipher text is known as (Encrypting the code of text).Decryption or Deciphering: Restoring plain text from cipher text is known as decryption.

Cryptography: There are so many schemes used for enciphering constitute the area of study known as cryptography. Types of Cryptography: There exist two main types of cryptography: First is Secret key cryptography and second is Public key cryptography.

Secret key cryptography is also known as symmetric key cryptography. With the help of this type of cryptography, both the receiver and 89the sender know the same secret code, known to be the key. Files are encrypted by the sender using the key and decrypted by the receiver using the same key. Public key cryptography, also known as asymmetric key cryptography, uses a pair of keys for encrypting and decrypting. But with public key cryptography, if public and private keys matched then it make a best pair of key.

2. LITERATURESURVEY

Lot of work is already defined by different researcherson the area of image encryption and decryption with the help of genetic algorithm. Some of the works are defined in this section-

RozaAfarinet al[1] describes a method which depends on two phases. Substitution phase- here location of pixels and their values are changed from the adjacent pixels to reduce the correlation among the pixels. Modification phase- here pixels values are changed and input image get encrypted. Both phases work on binary patterns. In substitution phase, patterns are developed by local binary pattern (LBP) and in modification phase (BPS) bit plane slicing technique is used. For the selection of population, a predefined key and a random number generator is used. By applying fitness function, histogram analysis and entropy gives a fast and effective image encryption. Merit- here fitness function is used at each generation, this work gives fast and high entropy. Demerit- increases computational error and burden.

R. Afarinet al.[2] states a method in which rows and columns of image are randomly dislocated. Then image is divided into four equally sub images. Now two pixels are randomly chosen from the population. After that crossover and mutation is applied and image get reconstructed again. Now entropy is checked of the image, if it increases then image is used for the next step and lastly randomness is measured by entropy, histogram analysis and coefficient correlation.

S.Geethaet al.[3] gives a new technique related to (GA) based approach for an audio stegnlysis. In this method so many audio quality matrices are calculated over the stego audio and cover audio and support confidence framework is used as a fitness function. Merit- this technique gives flexibility to implement a new technique of steganography. Author implements digital steganography in which a file has an encrypted concealed file within itself. Concealed file is known as stego file. Images, movies, audios are cover file. Author work on rule based approach which is based on if-then technique that is generated by soft computing which consists of fuzzy logic, probabilistic reasoning and artificial neural network. It has some conditions and some outputs. Merit- cost effective and adaptive. Demerit- low extrapolation power.

M Prashantet al.[4] use the concept of molecular genetics and image pattering. At first it deals with the concept of molecular genetic that is meiosis, fertilization, translation and mutation. At second step data is encrypted in the form of image. Main purpose of this paper is just to get high level of data security; both the concepts are work together. Here a key is generated, and then with the help of that key so many sub keys are generated. Then several patterns are developed for a particular key. Rather than image, it works on knowledge of image pattern, which directly gives the information on the basis of key pattern of image. Demerits- it takes larger percentage of total time for coding.

Sheetal U. Bhandari et al.[5] , uses genetic algorithm, image encryption and video encryption with the help of physical model which can work on cryptography. Proposed method works on signal and image processing. For many devices, partial reconfiguration is supported by Xilinx. Here real time video signal is transmitted on virtex-4 with the help of partial reconfiguration. In the future work author is going to load bit files through ICAP driven by soft core machines which are based on image analysis.

A. Traghaat el.[6]., developed an algorithm which gives an approach to a new symmetrical blocks ciphering system, that is [ICIAG]. In this method user can choose the size of blocks and length of key. Later author gives a brief comparison among the most used symmetrical techniques like IDEA, AES and DES. This method works in information processing technology. Merits- size of blocks and key can be selected by user, secret key is generated at each session process. After that mutation, crossover, left shift and right shift are used. Complexity of ICFAG is o(n) by pushdown automata.

Abdel-karim et al.[7]., generates a concept of encrypt and decrypt the data with the help of (GA) and RSA. Here integration of two methods are done first is- symmetrical system using the GA and asymmetrical system using RSA cryptography. With the help of this method a strong key can be generated and can be made non-repeating too, because of this it is not easy to break at all. This method provides high security of data and information. Author takes GA as a base for developing key and generates a new block ciphering system. This algorithm is better than DES, AES, ELLIPTIC CURVE, RSA, NTRU etc. Merit- no one can break the code of key yet.

PrempratapSingh et al. [8]., provides a new method of security that is e- security with the help of GA and pseudorandom sequence, just to encrypt and decrypt the data. Images on internet or any other transmission medium can be secured by this technique. Here author generates a pseudorandom sequence with the help of nonlinear feedback shift register{NLFSR}, then apply crossover operator to encrypt data over pseudorandom sequence, then mutation is applied on the binary patterns. Merit- speed of algorithm is good at the time of encryption process, safe and reliable because of lack of knowledge about pseudorandom sequence and mutation string.

Sindhuja K et al.[9]., gives a symmetric key cryptosystem with the help of GA, firstly plain text is converted in the form of matrix that is key matrix and text matrix, secondly additive matrix is produced by adding both the text and key matrix. Now substitution function is applied to produce intermediate cipher on additive matrix and then crossover and mutation is applied. Merit- easy and simple to operate this method, high security because of key generation and additive cipher technique.

Mohammad A.F.Al-Husainy.et al.[10]., uses simply a GA to produce a new method of encryption which also covers strong points of crossover and mutation, here implementation is done on an image with some width and height . Author uses visual C++ 6.0 programming for the implementation and recorded noise is 0%. Merit- no data loss in encryption and decryption.

Dr. DilbaghSingh et al.[11]., proof that when a high level of security is needed, symmetric and asymmetric methods doesn't work. To obtain a perfect result within least time, author proposed an algorithm in which GA is incorporated with cryptography and output of that combination is an optimal solution. Here author gives limitations of hash functions and digital signature. MATLAB 7.8.0 platform is used. With the help of random number generator, pseudo random numbers are generated. Transmission of data in the form of image over the internet, Analysisof encryption and decryption process in respect with time and an algorithm is proposed on graphs too. Values of colors are based on bit level gray scale. 0 is for black and 255 are for white. Merit- this algorithm gives better throughput and solution with in given time.

AartiSoni, et al.[12].,proposed a new method in which a key is generated by pseudorandom number generator and these random numbers will be developed with the help of current time of the computer system. Now GA is applies on it and image encryption is done with the help of [AES] symmetric key algorithm. Merit- his algorithm will increase the efficiency and decrease the computational time, irregularity of key increases the complexity of key generation and additive cipher technique.

NitinKumarRajendra et al.[13]., incorporates GA and BRAIN- MU – WAVES for the encryption of data which finally provides better security, confidentiality and integrity of the data stored in information. Pseudorandom binary sequence is integrated with the brain mu waves for the encryption and decryption of data. Key is generated by user thinking or thought of user brain, now pseudorandom binary sequence is generated and crossover if applied on it. Merit- because of these processes key that is generated very difficult to guess at all, speed of algorithm is good. Demerit- decreases the throughput.

SoniaJawed et al.[14]., proposed algorithm and increases time. A natural selection method for the key generation, proposed method will give the best fit key for encryption which is generated by pseudorandom number generator and it is non-repeatable too. Now crossover ,mutation and fitness function is applied to get the solution, gap test and frequency test is done in the calculation of fitness function; then hams distance is generated by doing XOR of two binary keys and lastly final key is selected. Java technology cxvis being used for observations. 100 chromosomes, 2.5 crossover rate, 0.5 mutation rate are set for the algorithm. Merit- result is good enough and key is unique, protection is good against eavesdroppers and cryptanalysts. Demerits- difficult to implement for image or audio cryptography.

SwatiMishra et al.[15].Generates a best fit key so that it can make code so difficult to crack. The key have best fitness function value will be used; fitness of keys can be calculated by Pearson coefficient of autocorrelation. Author also takes good sample of frequency and gap test, after generating random number and pure key; crossover and mutation is applied. Here public key is differing from the private key, according to fitness value, a population is transferred into a new population,and ring crossover is used. Data structure is used to implement the algorithm and flowchart is done in C++ programming, frequency test id done by chi-square test.

AbdelsalamAlmarimiet al.[16].,deals with the confidentiality of e-data that is transmitted over a network. Author proposed a concept in which GA and pseudorandom sequence are integrated to encrypt and decrypt the data. Firstly pseudorandom sequence is generated with the help of nonlinear feedback shift register [NFFSR]. Secondly crossover operator is used for already generated sequence of pseudorandom for the encryption of data. In pseudorandom clock pulse is a medium which generate binary sequence. Method is an image is selected and its pixel value gets changed with the help of crossover and new image is created, that is to be encrypted. Here exchange of bit is done with the help of pseudorandom number generator the same procedure is used for decryption method. Further speed and time is alsoanalyzed by the author.

Sonia Goyat et al.[17]., studied so many research papers and these are finally reach at a conclusion that natural selection based technique are better than the mathematical generated technique like AES and DES. An author use a key which is generated by the vernamciphers a sample rather than pseudorandom number generator and conclude that vernam ciphers is better than the PRNG. Method- plain text is converted into cipher text by applying XOR function between the plain text and binary key. This make a key better than PRNG, the min work of this paper is to find out the randomness of the sample.

Dr. Poornima G. Naik et al.[18].Attempted to exploit randomness by generating asymmetric key pair by encrypting and decrypting message that involves a crossover and mutation technique. Here author proposed four crossover points and three mutation points, permutation factor and a single random byte, key length is 36 and isdefined or mutually shared permutation factor is used. Implementation is done in java and key is written in word document.

A.Traghaet al.[20], gives a new symmetrical ciphering block system whichnamed {Improved Cryptography Inspired with Genetic Algorithms} ICIGA, that produces a session key in a random process, and apply algorithm for the further encryption and decryption.

A.Kumar et al [20,21] describes an encryption method with the use of crossover operator and pseudorandom sequence generator by NLFFSR (Non-Linear Feed Forward Shift Register). Pseudorandom sequence is going to give the crossover point and hence a fully encrypted data achieved. A. Kumar et al [20] further extended the work and used mutation after the encryption. Theinformation that is encrypted can be further hided inside the steno-image.

SoniaGoyat et al.[22] stated that if the quality of the random numbers produced by the current algorithm is superior, then the key that is produced will always be excellent. Author uses a threshold value for the selection. Basically just to check the randomness of the samplecoefficient of correlation is used.

FayezAhamad et al.[23] proposed a model in which GA is used to generate Pseudo random numbers. The encryption technique follows the procedure of the crossover and mutation operator. Author uses an advance technique of mimetic algorithms and pseudorandom binary sequence.

Nitin et al.[24] uses the concept of, pseudorandom binary sequence,brain thoughts, GA, and Mu waves. This technique of securing the confidential data is highly safe and reliable.

Ankita et al.[25] applied Genetic Algorithm as the encryption algorithm by using a secret key for encryption and decryption process.

Chaos theory and entropy et al.[26,27], have large application and technique in securing the data communication and the desired disorder will be provided by inherent nature of genetic algorithm [26,27].

Mohammad SazzadulHoque et.al.[28] has presented an intrusion detection system by applying GA so that it can efficiently detect various types of the network intrusions.

3. FUTURE SCOPE

In present study a cryptographic algorithm has been designed using the concept of genetic algorithms. This algorithm improves the quality, efficiency and effectiveness of the technique being used for the cryptography. With the experimental results, it proves that the present algorithm has achieved the objective set in the present study. Statistical analysis gives dimensions of original data and the encrypted are totally different. Also the histogram of the encrypted image is nearly uniform and is quite different from the original image; hence, it does not suggests any clue to employ any type of attack on the proposed image encryption technique. This total way of transferring secret information is highly safe and reliable. So, without the data of the pseudorandom sequence no one will be able to extract the message.

In the future work, we plan to design a sophisticated software based on this technique which will targeted to use in highly secure multimedia data transmission applications.

5. CONCLUSION

We introduced an encryption method based on GA which is used to generate key by pseudorandom number generator. Using Genetic Algorithm we can keep the strength of the key to be long, we are still on working to make the complete algorithm better enough. We proposed a modified approach to data security using the concept of Genetic algorithms Inspired Cryptography and RSA cryptography to encrypt and decrypt the information. The feature of such amethod, gives high data security and feasibilityfor thepractical implementation. We introduce a modified cryptographic ciphering concept that lead to new ciphering system that can be used in encrypting data.So, without the secret thought or information stored in the brain of the person i.e., the keys will never be able to extract the data. Because the pass thought is unpredictable so it is very difficult to decrypt correctly without knowing the initial pass thought of the brain. Time analysis results show that the throughput rate of the proposed method is awesome and it is found that this algorithm gives a much better and acceptable throughput rate.

6. ACKNOWLEDGEMENT

I sincerely wish to express my appreciation for the valuable help, which I received duringthe completion of the paper by the following:

Mr. VikasThada, for supervising my project, guiding me throughout my research and for his very informative skills on Cryptography and Genetic Algorithm.

Mrs. Shivali Dhaka, for his interesting skills on Mutation and Crossover and help me to generating the key.

7. REFERENCES

[1] R. Afarin., S.Mozaffari2013.”Image encryption using genetic algorithm and binary patterns” at MVIP and IEEE.

[2] R. Afarin., S.Mozaffari2013.,”Image encryption using genetic algorithm” at MVIP and IEEE .

[3] S.Geetha, Siva S.Sindhu 2006, A. Kennan., “An active rule based approach to audio steganalysis with a genetic algorithm” at IEEE.

[4] M Prashant, R Siddhartha and Rajeev Kumar2011.”Formulation of an encryption algorithm on the basis of molecular genetics and image patterns” at IEEE.

[5] Sheetal U. Bhandari , S.Subbaraman , Shashank S. Pujari2009 , RashmiMahajan.,”Real time video processing on FPGA using on the fly partial configuration” at IEEE.

[6] A. Tragha, F. Omary, A. Mouloudi2006.”ICIGA: improved cryptography inspired by genetic algorithms” at IEEE.

[7] Abdel-karim S.O. Hassan, Ahmed F. Shalash and Naglaa F. Saudy MAY 2014.,”Modifications on RSA cryptosystem using genetic optimization” at IJRRAS 19 (2).

[8] P.Singh, G. Gosawi, S. Dubey 4 (2014). "GA: A technique for cryptography real time data transmission" at binary journal of data miming and networking 37-40.

[9] Sindhuja K, P. Devi2014,414-416.,"A symmetric key encryption technique using GA" at IJCSIT, volume 5(1).

[10] Mohammad A.F.Al-Husainy2006, 516-519..,"Image encryption using GA" at ITJ 5 (3).

[11] Dr. D. Singh,P.Rani, Dr. R. Kumar2013.," To design a GA for cryptography to enhance the security" at issue 2April 2013.

[12] A.Soni, S.Aggarawal2012.,"Using GA for symmetric key generation in image encryption" at IJARCET 2012.

[13] N. Rajendra, B. Rajneesh Kaur2011.,"A new approach for data encryption using GA and brain mu waves" at IJSER 2011.

[14] S.Jawaid, Adeeba Jamal2014.,"Generating the best fit key in cryptography using GA" at IJCA (0975-8887) volume 98-no.20, July 2014.

[15] S. Mishra, S. Bali2013.," Public key cryptography using GA" at IJRTE. 2277-3878, VOLUME 2, ISSUE 2 MAY 2013.

[16] A.Almarimi, A. Kumar, I. Almerhag, N. Elzoghbi 2013.,"A new approach for data encryption using GA" atLIBYA.2013.

[17] S. Goyat2012.,"Cryptography using GA" at IOSRJCE, 2278-0661, volume 1, issue 5(may-June 2012).

[18] Dr. Poornima G. Naik , Girish R. Naik 2014.,"Asymmetric key encryption using GA" at IJLTET, volume 3,issue 3 Jan 2014.

[19] Tragha A., Omary F., Kriouile A2007.," The (GA) Inspired by Cryptography", Association for the Advancement of Modeling & Simulation Techniques in Enterprises (A.M.S.E), Series D: Computer Science and Statistics, 15- November 2007.

[20] A Kumar, N Raj pal 2004, ―Application of Genetic Algorithm in the Field of Steganography, in Journal of Information Technology (IJIT), Vol. 2nd, No.1, Jul-Dec.2004, pp-12-15.

[21] A Kumar, N Raj pal, A. Tayal 2005, ―Security System for Multimedia Data Transmission Using Genetic Algorithms" NCC, 05 Presented in the Kharagpur (IIT), page-579-583, 28-20 Jan 2005.

[22] S. Goyat 2012, "Genetic Key Generation for Public Key Encryption Cryptography", (IJSCE) ISSN: 2231-2307, Volume-2nd, Issue-3rd, July 2012 231.

[23] F. Ahamad, Mohd. Shahid ,S. Khalid 2012, published a paper titled, "Encrypting The Information Using The Features of Mimetic Algorithm With Encryption and Decryption Technique" at (IJERA) International Journal of the Engineering Research and the Applications, Vol. 2nd, Issue 3rd, May-Jun 2012, page.3049-3051.

[24] N. Kumar, R.Bedi, Rajneesh Kaur 2011, "A Special Technique for the Information Cryptography by Using Genetic Algorithms and Brain Mu Waves", International Journal of Scientific and Engineering Research Volume 2nd, Issue 5th, June 2011 ISSN 2229-5518.

[25] A. Aggarwal 2012, "The Secret Key Data Encryption Algorithm Using Genetic Algorithm" at IJARCSSE, 2012.

[26] H. S. Kwok, W. K. S. Tang 2007, Chaos Solutions and Fractals, page 1518–1529.

[27] Y. Mao and G. Chen 2003. Handbook of computational geometry for, computervision, patternrecognition, robotics, and neural computing.Springer.

[28] M. SazzadulHoque, Md. Abu NaserBikas and Md. Abdul Mukit 2012 ,"The Implementation of Intrusion Detection System Using(GA)", International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012