Cryptanalysis on Chaotic Mapping using Genetic Algorithm

Nithya Jayaraj
Department of Computer Science and Engineering
Mahendra Engineering College
Namakkal, India

K. R. Sathish Kumar, Asst Professor.,
Department of Computer Science and Engineering
Mahendra Engineering College
Namakkal, India

Abstract— **The exchange of sensitive information such military, medical, industrial or electronic commerce is, widely used. The multimedia and particular, image data have reached its highest importance level nowadays; especially on people and things identification. So, the security of such information through the network becomes essential. Various image encryption methods and algorithms have been proposed to ensure the security but still many attacks have been introduced to break the encrypted messages. Image encryption involves complex algorithms and methods to allow a high security and complexity. Nowadays, Crypt-analytic attacks have been commonly used to retrieve the plain text from the ciphertext without using the key. In the existing system plain image is encrypted using chaotic mapping which in turn is also an input to the crypt-analytic attacks. The Chaos theory is a mathematical study which aims the behavior of non-linear dynamical systems. Here, image is encrypted using chaotic mapping which involves two steps: Chaotic confusion and Pixel diffusion. Now the image encrypted using chaotic mapping act as a ciphertext and brute force attack is used to decrypt the encrypted image. Many problems can be solved using genetic algorithms through modeling a simplified version of genetic processes. In the proposed method, same image encrypted with chaotic mapping is used as a ciphertext and genetic algorithm is used to decrypt the image. In genetic algorithm we use selection, fitness function, cross over and mutation to obtain the plain image. The feature of such an approach includes high feasibility to obtain the solution.**

Keywords – Encryption, Chaos theory, Pixel Confusion and diffusion, Genetic Algorithm, Fitness function.

I. INTRODUCTION

Encryption

The encryption scheme generated pseudo-random encryption key with help of algorithm. It is in principle possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, large computational resources and skill are required. The decrypt accessed by authorized recipient with the key provided by the originator to recipients, but not to unauthorized interceptors. The purpose of encryption is to make sure that only somebody who is authorized to access data that person only can access the data with help of using the decryption key. Somebody who is not authorized can be excluded, because he or she does not have the required key, without which it is impossible to read the encrypted information. At the same time of development of encryption models, various crypt-analytic attacks have been also emerged where a part of encryption schemes have been found vulnerable [6].

Image encryption is a technique that converts original image to another format with the encryption techniques. The same way in the decryption no one can access the information without knowing a decryption key. Image security is an utmost concern in the web attacks has become more serious. Protecting the confidential images is the legal requirement. So as to make a strong encryption for an image so that it can't be hacked easily. And the perfection in the original image can obtain after decrypting it[4],[5]. Another use of internet could transfer the secure data which may be very essential for a group of companies, that the data should not be view by others. Therefore sensitive data hiding becomes the most important area in securing network information. The method is used for secure the data is known as encryption. After encrypting the data, with the help of network it is transferred to the destination. At its destination, encrypted data is decoded with the help of provided algorithm which is known as decryption.

II. CHAOS PRINCIPLE

A.CHAOS THEORY

Chaos is a pseudo-random process produced in nonlinear dynamical systems. It is non-periodic in nature, non-convergent and extremely sensitive to the initial condition. The chaos theory has been developed, since early 60‘s from many research disciplines (such as Mathematics, Physics, Biology, Chemistry, and Engineering). As a result of the above relationships, a good number of chaos-based cryptosystems has been proposed; some of them lack robustness and security.

B.CHAOTIC MAPS

It is a dynamic system that can be easily denoted by mathematical equations. Generally for the chaotic map the initial value act as its input, the control parameter determines its actions, and the output is the sequence produced by the iterated map[2]. It has some typical property suitable for data encryption. Given the initial value, the chaotic map generated the sequence with random properties. The sequence is sensitive to the initial value, that is, two initial values with a slight difference will cause a great difference after multiple iterations. Additionally, the sequence is very sensitive to the control parameters, that is, different parameters produces different sequences and a chaotic map is similar to a cipher. The initial value of the chaotic map is regarded as the plain image, the control parameter as the key and the output sequence as the cipher image.

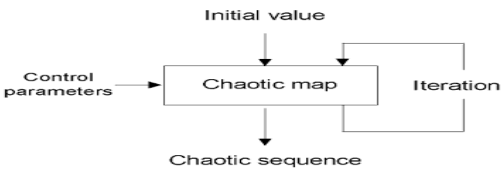


FIGURE 2.1: General architecture of chaotic map

III. EXISTING SYSTEM

Image encryption attack is viewed as a decryption-key search through a finite discrete space. Its complexity is measured by the average number of candidate keys required to locate the right one that allowed revealing the plain-image. In literature, such strategy is based in a way that reducing the search space; so, an encrypted image with wide key spaces is viewed as secure. To surpass such difficulty, we need much attention to the problem formulation and use appropriate attack algorithms. This fact avoids modest results as those performed by classical crypt-analysis algorithms. Chaotic based encryption methods have been extensively applied in existing system. Chaos discrete models are suggested as a suitable alternative in design of secure image encryption techniques[12]. This is due to their high security, performance aspects, sensitivity to control parameters and initial conditions. Therefore, image encryption schemes based on chaotic maps constitute an area widely exploited and referenced afterwards; they allowed to convert a plain-image to an encrypt form through various pixel mixing and transformations such substitution, permutation or combination of both schemes. Such operations alter statistical characteristics of image by changing grey-values of pixels which provide robustness and security of encrypted data.

Brute Force Attack (BFA) was used to check the efficiency of chaotic technique for real-time image encryption and their resistance against such attacks. It is inefficient and hence useless when dealing with homogeneous problems of higher complexity. In existing model it is not suitable for solving problems that have an hierarchical structure and involve logical operations. Because of this using, the model have does not require any derivative information (which may not be available for many real-world problems).It can be optimize both continuous and discrete functions and also multi-objective problems. The propose system provides a list of “good” solutions and not just a single solution.

Existing system used cryptographic attack using Brute force algorithm. It does not that much advantage. The basic intention of an attacker is to break a cryptosystems and to find the plain-text from the cipher text. If attacker obtains the plain-text, that people find out the secret decryption key. Those keys are maintained in algorithm is already in public domain. Once the attacker is able to determine the key, the attacked system is considered as broken or compromised. For this we proposed attacking based on Genetic Algorithms.

IV. PROPOSED MODEL

The proposed system uses chaotic mapped image as input. It converts the image to cipher image. The diagram shows image encryption using chaotic mapping. An image is encrypted using chaotic mapping through various pixel mixing and transformations using substitutions. Such operation changes the pixel value which in turn provides the security for the image to be transmitted. The robustness for such an image can be obtained through two methods: Pixel confusion and Diffusion.

- **Pixel Confusion –** Permutes each pixel of a plain image with another using chaotic mapping.
- **Pixel Diffusion –** Changes each pixel values based on initial parameters.

The plain image is first converted to Byte array which is then converted into Binary Data. Confusion of an image is carried out by dividing the Binary data into number of blocks (Here maximum 50 Blocks has been taken). Each block is made to undergo different operations based on the decimal value of first 3 digits of the binary data in a block. If the decimal value of the first 3 digits of a Block is 0 then, the even positions of the Block are changed from 0 to 1, and odd position from 1 to 0. Likewise, we follow different operations on different cases as follows:

Decimal 0 : Even position bits changed from 0 10 1 and odd position is changed from 1 to 0.
Decimal 1 : Reversal operation of the binary data for a Block.
Decimal 2 : Perform NOT operation on a Block.
Decimal 3 : REVERSE (NOT) operation.
Decimal 4 : No changes to the block (Similar to input data).
Decimal 5 : Apply powers of 2 operation. Change the bits in the positions like (2,4,8,etc,…).
Decimal 6: Take module 3(MOD 3) bits position and perform conversion from 0 to 1 and 1 to 0.
Decimal 7 : NOT operation of Decimal 6 condition.

After performing the confusion of Binary data then follow the next process of shuffling inorder to change the position of the bits in the blocks which leads to change in pixel positions which will make the Image to get more chaotic. This chaotic image is now very difficult to decrypt which makes difficulties to derive the Plain Image.

A.OVERVIEW OF GENETIC ALGORITHM:

Genetic Algorithm (GA) is a search-based optimization technique based on the principles of Genetics and Natural Selection. It is frequently used to find optimal or near optimal solutions to difficult problems which otherwise would take a lifetime to solve. It is frequently used to solve optimization problems, in research, and in machine learning. In GAs, we have a pool or a population of possible solutions to the given problem. These solutions then undergo recombination and mutation (like in natural genetics), producing new children, and the process is repeated over various generations. Each individual (or candidate solution) is assigned a fitness value (based on its objective function value) and the fitter individuals are given a higher chance to mate and yield more “fitter” individuals.

Normally GAs comprised of set of population(s) which might represent one or more groups. These populations are composed of feasible solutions for any given problem to solve. The evolution of such population is based on biological metaphors when are subjected to probabilistic operators. GAs show least processing time compared to other methods. Recently Rosa afrain [3] proposed GA can also be used directly for image encryption. Crossover and mutation operations change binary format of the pixels values from the middle point to reduce correlation coefficients between adjacent pixels by using predefined functions. In, pixels located at even positions are considered as first parents. For mutation, the function which finds out the second parent is altered.Wafa' Slaibi Alsharafat [4]planned in this paper about Genetic Algorithm (GA) is an adaptive exploratory search algorithm premised on the evolutionary ideas of natural selection and genetic.

Recently Tahar Mekhaznia [1] analyses the robustness of a recent image encryption scheme and propose an attack methodology based on genetic algorithm. The goal of the approach is to demonstrate the effectiveness of the approach in handling such problem[11][13]. In this paper author demonstrated chaos based image encryption and attacks the same using genetic algorithm. For this problem new approach based on block cipher encryption technique which is used to encrypt the image. In the process of encryption a key will be generated. Key length and bit stream is chosen at random.

A Composite algorithm for improved image security is proposed by taking the advantages of DNA based image encryption and evolutionary algorithms (EA). A number of deoxyribonucleic acid (DNA) masks are created using logistic map function and DNA conversion rules. Then encryption is performed on the plain image to generate a number of cipher images. Finally, genetic algorithm (GA) is applied to find the best DNA mask. From the simulation results it is observed that the proposed scheme improves the level of security[8][9].

B. ATTACK ON CHAOTIC IMAGE USING GENETIC ALGORITHM:

Initial population which may be generated at random or seeded by other heuristics. The Parents select from this population for mating. Apply crossover and mutation operators on the parents to generate new off-springs. And finally these off-springs replace the existing individuals in the population and the process repeats. In this way genetic algorithms actually try to mimic the human evolution to some extent.

The blocks of the above encrypted chaotic image is divided into sub-blocks and given as input to the cryptanalytic attack. Genetic algorithm involves the sub modules as below:

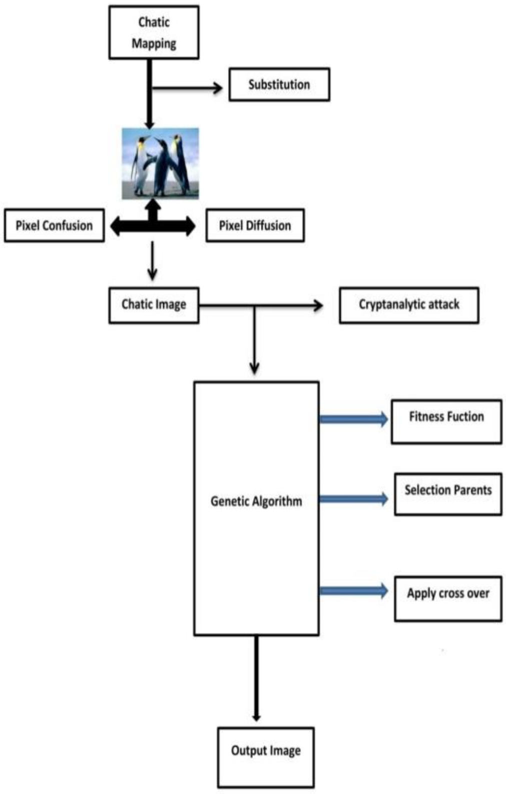


FIGURE 4.1: Block Diagram of Genetic Algorithm

Designing the fitness function

A fitness function can be designed based on the binary format of cipher images in order to produce set of individuals that are filtered from initial population based on the fitness values. Fitness Proportionate Selection is one of the most popular ways of parent selection. In this every individual can become a parent with a probability which is proportional to its fitness.

Here, the fitness function is taken by considering the average count of 1's and 0's in blocks and selecting the individuals for further processing.

$$\sum_{1}^{i} f(n) \quad \textit{where}, i \textit{ is the length of the block}$$

Here, f(n) is the function which is used to calculate the average number of 1's and 0's.The comparison percentage for all the individuals are calculated by checking the average number of 1's and 0's of both plain and chaotic blocks.

Selection of parents for generating off springs

Different Selection operators are applied over the filtered individuals which selects the parents for the crossover operation. Here Parent Selection obtaining the process of selecting parents which mate and recombine to create off-springs for the next generation. It is very crucial to the convergence rate of the GA as good parents drive individuals to better and fitter solutions. Maintaining good diversity in the population is extremely crucial for the success of a GA. The entire population by one extremely fit solution is known as premature convergence and is an undesirable condition in a GA. Parent Selection here is done based on the comparison percentage of the fittest individuals with the individuals generated after fitness function. A Sub-Block can be divided into equal no.of.Blocks based on the fitness function and are taken as separate parent.

Here, parent selection is done based on the comparison percentage of the fittest individuals with the individuals generated after fitness function. The individual with the highest comparison values are selected for further processing.

Applying Crossover and Mutation to obtain plain image

Crossover operators are applied on the parents provided by the Selection process to produce group of off springs that converges to the solution. One Point Cross over operation have been applied to the Individuals obtained after selection operation. In this one-point crossover, a random crossover point is selected and the tails of its two parents are swapped to get new off-springs as follows:

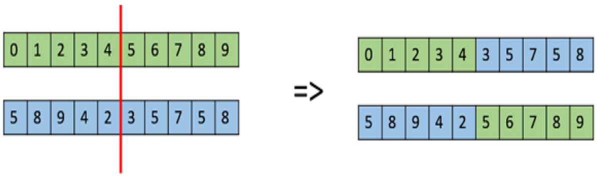


FIGURE 4.2 : Representation of One Point Crossover

Mutation is applied rarely in order to converge to the solution. Reproduction and biological crossover produced by crossover operator.. In this parent selected more than one and one or multiple off-springs are produced using the genetic material of the parents. It can be usually applied in a GA with a high probability – p_c . Bit Flip Mutation have been after the comparison of Cross over results with Plain image Bits for the same Blocks/Sub-blocks.

In this bit flip mutation, we select one or more random bits and flip them. This is used for binary encoded GAs.

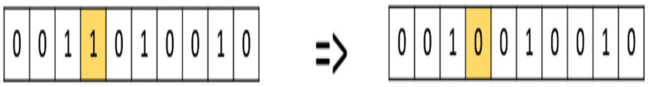


FIGURE 4.3 : Representation of Bit Flip Mutation

V. ANALYSIS AND RESULTS

When the number of iteration increases there might be a possibility of attaining a saturation point in the fitness value of the individual. To avoid this Mutation operation is applied say for every 20 generations. And also it could be seen that there is an increase in the fitness value of the chromosomes. The below table shows the random population generation and its corresponding highest fitness value obtained (Say for every 20 generations).

TABLE I: FITNESS VALUES OBTAINED FOR 100 POPULATIONS GENERATED FOR A BLOCK

ITERATION	INITIAL POPULATION	HIGHEST FITNESS VALUE
20	100	71
40	100	68
60	100	68
80	100	73
100	100	68

TABLE II: FITNESS VALUES OBTAINED FOR 500 POPULATIONS GENERATED FOR A BLOCK

ITERATION	INITIAL POPULATION	HIGHEST FITNESS VALUE
20	500	78
40	500	69
60	500	71
80	500	72
100	500	70

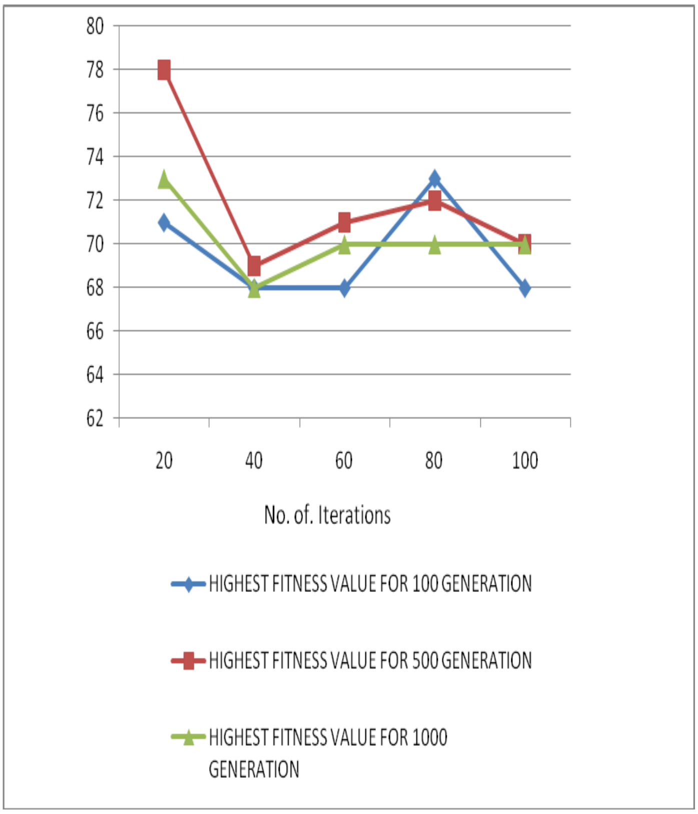
TABLE III: FITNESS VALUES OBTAINED FOR 1000 POPULATIONS GENERATED FOR A BLOCK

ITERATION	INITIAL POPULATION	HIGHEST FITNESS VALUE
20	1000	73
40	1000	68
60	1000	70
80	1000	70
100	1000	70

The below graph shows the variations of fitness values over all the generations considered in the above 3 tables.

Here, the x axis represents the number of iterations and y axis represents fitness values obtained for that iteration.

As a result we could see the increase in the fitness value has occurred for 500 generations of the image which is taken as input. Hence, the number of generations required to retrieve/attack an image may be higher or lower based on the size of the image obtained after chaotic mapping.



GRAPH I : COMPARISON OF FITNESS VALUES OBTAINED ON DIFFERENT GENERATIONS

VI. CONCLUSION

Genetic algorithm is a computational intelligence methodology for exploitation of wide search space with moderate resources consumption. It has been successfully applied in resolution of various real-life problems included the cryptanalysis.In this paper, we propose the use of such algorithm for attack of image encryption based chaos map. The experiments conducted on typical grey image indicate the effectiveness of the approach in handling the considered problem. According to the results obtained, it turns that a large part of decryption keys of 64 bits can be achieved in most cases. Also, the AG has been proved its efficiency against Brute Force attack with better results in similar environment.

VII. REFERENCES

[1] Tahar Mekhaznia , Abdelmadjid Zidani, "Genetic algorithm for attack of image encryption scheme based on chaotic map", University of Tebessa, Algeria, 978-1-4673-7689-1/16/$31.00 ©2016 IEEE.

[2] ALI.S.AL-KHALID , ALAA.O.AL-KHFAGI, "Cryptanalysis of a Hill Cipher using Genetic algorithm", Middle Technical University, 978-1-4799-9907-1/15/$31.00 ©2015 IEEE.

[3] Roza Afarin, Saeed Mozaffari, "Image Encryption Using Genetic Algorithm", 2013 8th Iranian Conference on Machine Vision and Image Processing (MVIP), 978-1-4673-6184-2/13/$31.00 ©2013 IEEE.

[4] Wafa' Slaibi Alsharafat, "Evolutionary Genetic Algorithm for Encryption", 2014 IEEE International Conference on Computational Intelligence and Computing Research", 978-1-4799-3975-6/14/$31.00 ©2014 IEEE.

[5] G. Aparna, G. Venkata Raghava Rao, G. Vasavi, "Computationally efficient ciphering scheme for image encryption using common division and genetic algorithm", 2016 IEEE 6th International Conference on Advanced Computing, 978-1-4673-8286-1/16 $31.00 © 2016 IEEE, DOI 10.1109/IACC.2016.64.

[6] Saranya M R, Arun K Mohan, K Anusudha, "A composite image cipher using dna sequence and genetic algorithm", 2014 International Conference on Contemporary Computing and Informatics (IC3I), 978-1-4799-6629-5/14/$31.00c 2014 IEEE.

[7] a. S. Arumugam and D. K. Jothi, "Image encryption algorithm based on improved 3d chaotic cat map," *2010 IEEE Int. Conf. Comput. Intell. Comput. Res.*, no. 2, pp. 1–4, 2010.

[8] M. K. Mandal, G. D. Banik, D. Chattopadhyay, and D. Nandi, "An image encryption process based on Chaotic logistic map," *IETE Tech. Rev.*, vol. 29, no. 5, p. 395, 2012.

[9] D. E. Goldberg, *Genetic Algorithms in Search, Optimization, and Machine Learning*. Addison-Wesley, 1989.

[10] X. Li, C. Tang, X. Zhu, B. Li, L. Wang, and X. Yan, "Image/videoencryption using single shot digital holography," Opt. Commun., vol.342, pp. 218–223, 2015.

[11] .-J. Tong, "Design of an image encryption scheme based on a multiple chaotic map," Commun. Nonlinear Sci. Numer. Simul., vol. 18, no. 7, pp. 1725–1733, 2013.

[12] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," Int. Jrc. Chaos, vol. 8, no. 6, pp. 1259–1284, 1998.

[13] S. Lian, J. Sun, and Z. Wang, "Security analysis of a chaos-based image encryption algorithm," Phys. A Stat. Mech. its Appl., vol. 351, no. 2–4, pp. 645–661, 2005.