INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

Enhancement in Genetic Algorithm to prevent Brute Force Attack

Saniya Puri[1], Harwant Singh Arri[2]

Lovely Professional University
Jalandhar, Punjab
[1]Saniya.Saniya.Puri@gmail.com, [2]hsarri@gmail.com

ABSTRACT: *The network is much vulnerable to different type of security attacks. The attacker can sniff information from the network and trigger the attack. Among all the different type of attacks brute force attacks is most common type of attack. Genetic algorithm is much vulnerable against brute force attack. In this paper, we proposed new technique to prevent brute force attack in genetic algorithm. In the proposed approach enhancement is made in traditional genetic algorithm to prevent brute force attack.*

KEYWORDS: *Genetic Algorithm, Brute force attack, Image processing, Vulnerable, Sniff*

1. INTRODUCTION

Cryptography is used to send the information between the various participants in such a manner, so that it could not be seen by the others. The technique is used to prevent the information from third party; third party means that from attacker. Cryptography provides the various services like integrity checking, authentication etc. In the integrity checking the user assures the recipient of a message that the message has not been altered by any other source. In case of authentication the user verifying the identity of the person, who wants to use the data. The message in the original form is known as plaintext. The message encrypted by the user is known as cipher text. When the cipher text is produces from plaintext, this process is known as encryption. The reverse process of encryption is called decryption. In the cryptographic systems an algorithm and a secret value is used. The secret value is known as the key. Cryptography systems can be broadly classified into symmetric key systems. In the cryptography, single key system is used, in this same key is used by the sender and recipient. The other is *public key* system; in this case two keys are required. One is the public key that is known to everyone and other is the private key that only the recipient of messages uses. The multimedia technology plays an important role in our society. It has promoted digital images to plays a more significant role. To fulfil the security and privacy in various applications, encryption of images is very important to frustrate malicious attacks from unauthorized group. In this regard, a solution is to use an encryption algorithm to mask the image data. For a long period, cryptography has been turned into a battleground of some of the world's most illustrious mathematicians and computer scientists, starting from Shannon's ideas dates back from 1949 , which has led to the celebrated number theory based encryption algorithms such as Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), and RSA . However, these encryption schemes appear not to be ideal for image applications, due to some intrinsic features of image, such as: Redundancy and bulk capacity of data, strong correlation among adjacent pixels, being less sensitive as compared to the text data etc. This work focuses on a totally new development towards the key generation algorithm for image encryption. If we can design a key to be applied on an image that will largely decrease the correlation among the image elements, then the generated cipher image will be more protected. In this work, we have tried to introduce a block based transformation algorithm using chaos mapping, where the mapping is derived by applying one important artificial intelligence procedure Genetic Algorithm and the algorithm hides the original image through simple permutation of the pixel location. We have also compared the work with a popular encryption method Blowfish Algorithm. Blowfish algorithm was designed as a fast, free alternative for existing encryption algorithms. Blowfish algorithm acts as a general purpose

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

algorithm. It intended as a replacement for the old DES and free of the problems and constraints associated with other algorithms. Digital imaging has become an important way of communication. Research in this area is still a dynamic process. The effectiveness of encryption depends on the algorithm applied as well as on the key applied. If bad key is selected protection will fail to provide the security in right manner and improper access can be gained on secured information the first algorithm in cryptography system design is the algorithm to generate key.

2. LITERATURE REVIEW

Algorithm for Image Processing Using Improved Median Filter and Comparison of Mean, Median and Improved Median Filter" has discussed about an improved median filter algorithm is implemented for the de-noising of highly corrupted images and edge preservation. Mean, Median and improved mean filter is used for the noise detection. Fundamental of image processing, image degradation and restoration processes are illustrated. In addition, the studied method uses simple fixed length window, and hence, it requires significantly lower processing time compared with other methods. The simulation results show that the studied method can be applied to different types of image and provide very satisfying results. It has significant improvement over the existing methods. In the future, various techniques can be considered to incorporate in this scheme to further improve the performance and preserve more edges in both highly and lowly corrupted images [1]. Intelligent Parking Space Detection System Based on Image Processing" has presented an intelligent system for parking space detection based on image processing technique that capture and process the brown rounded image drawn at parking lot and produce the information of the empty car parking spaces. It will be display at the display unit that consists of seven segments in real time. The seven segments display shows the number of current available parking lots in the parking area. This proposed system, has been developed in software and hardware platform [2]. Application of Improved Median Filter on Image Processing described about median filter is the most common method of clearing image noise. This paper proposes improved algorithm of median filter to remove sale and pepper noise of image. According to the characteristics of salt and pepper noise, the algorithm detects image noise, and establishes noise marked matrix, without processing the pixels marked as signal. The signal of the pixel is marked as not treated, labeled according to their pixel noise pollution in the neighborhood to take a different pixel weighted mean filter window size, weight pixel region by the noise points to determine the local histogram. Matlab experiments show that improved median filter can greatly reduce the time of clears image noise and it performs better than median filters on noise [3]. Comparative Study of Edge Detection Algorithms on the Remote Sensing Images using matlab has explained about classified and comparative study of edge detection algorithms is presented. Experimental results prove that canny operator is better than Prewitt and Sobel for the selected image. Subjective and objective methods are used to evaluate the different edge operators. This paper evaluates the performance of Canny, Sobel and Prewitt Edge Detector for detection of edges in digital images. Further, the various images are examined to validate our results. The software is developed using MATLAB 7.0 [4]. Clark introduced technique which enables the creation of a complete list of Boolean function inputs in such way that complementing any one of the corresponding truth table positions will increase the nonlinearity of the function. Each truth table position corresponds to a unique function input. To find the list of truth table positions Clark first found the values of Walsh Hadamard transform coefficients. First experiments were done by utilizing hill climbing Techniques on the binary truth tables [5].

3. GENETIC ALGORITHM

A Genetic Algorithm is a searching technique used in computer science to find approximate solutions to optimization problems. GAs are a particular class of evolutionary algorithms that use techniques inspired by evolutionary biology such as inheritance, mutation, natural selection, and recombination (or crossover). Once we have the genetic representation and the fitness function defined, GA proceeds to initialize a population of solutions randomly, and then improve it through repetitive application of mutation, crossover, and selection operators. The GA is a stochastic global search method that mimics the metaphor of natural biological evolution. GA operates on a population of potential solutions applying the principle of survival of the fittest to produce (hopefully) better and better approximations to a solution. At each generation, a new set of approximations is created by the process of selecting individuals according to their level of fitness in the

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

problem domain and breeding them together using operators borrowed from natural genetics. This process leads to the evolution of populations of individuals that are better suited to their environment than the individuals that they were created from, just as in natural adaptation. Individuals, or current approximations, are encoded as strings, chromosomes, composed over some alphabet(s), so that the genotypes (chromosome values) are uniquely mapped onto the decision variable (phenotypic) domain.

4. NEW PROPOSED ALGORITHM

In new proposed technique, our main focus was on two operations that are used in genetic algorithm .i.e. Cross-over and mutation operations. Swapping of bits is done in cross-over operation and mutation is used for another key, in which we subtract swapped key out of 255 bits. The proposed technique is mainly focus on to encrypt digital image, for encrypting digital image we rotate it at 90 degree angle. For ensuring the confidentiality of the image which is send over the network, we use blow fish algorithm. In today's era 488 ways are possible to break the key; in our algorithm 576 possible tries will break the key which ensures the confidentiality of the digital image.

Steps to encrypt digital image

a. 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.

b. (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].

c. (mutation operation)For each vector Vi Do mutation by an 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]

d. Construct an encrypted image from the set of N vector that are produced from the Mutation.

5. RESULTS AND DISCUSSION

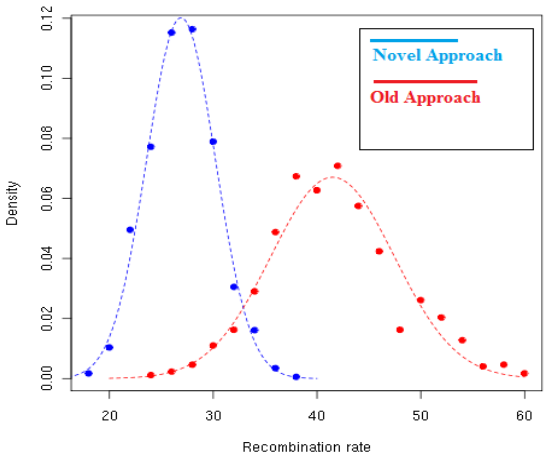

Figure 1: Comparison graph of security

As illustrated in figure 1, on X axis recombination rate of population size is shown and on Y axis Density in chromosomes in shown. The curve of previous technique takes fewer hikes due large number of population size and less complexity. The curve of novel approach takes more hikes due to less population size and high complexity due to increase in bit size

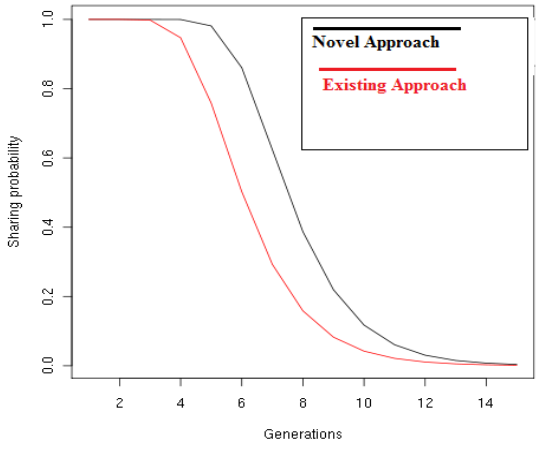

Figure 2: Comparison graph of generations

As illustrated in figure 2, Curve of novel approach is higher as compared with existing approach due to the reason of sharing probability of correctness of sending bits is more as compared to existing technique. This graph is showing probability on y axis and mutation on x axis.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

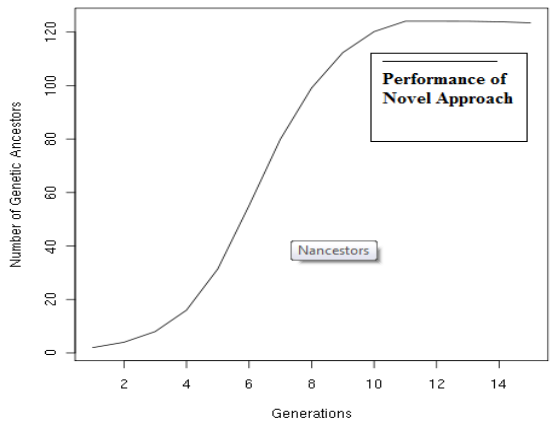

Figure 3: Performance of Novel Approach

As illustrated in figure 4.11, Performance graph of novel approach is shown. The x axis shows the generations and y axis shows the number of genetic ancestors. The curve takes hikes because less number of possible ways is there to decrypt the digital image.

6. CONCLUSION

In this paper, we conclude that genetic algorithm is much vulnerable to security attacks. In this paper, we proposed novel technique through which brute force attacks is prevented. The proposed technique provides extra security to multimedia data which is send over the network. In this work, image is send over the network. The image is encrypted with the proposed algorithm and simulation is performed in MATLAB. The simulation results shows that proposed technique is efficient than existing technique.

REFERENCES

[1] F. Adamo, F. Attivissimo, A. Di Nisio, M. Savino, An Automated visual inspection system for the glass industry,In: Proc. of 16th IMEKO TC4 Symposium, Florence, Italy, Sept. 22–24, 2008.

[2] www.ijera.com Vol. 2, Issue 3, May-Jun 2012, pp.691-694 691 | P a g e Ultrasound Liver Image Enhancement Using Watershed Segmentation Method

[3] JOURNAL OF COMPUTERS, VOL. 7, NO. 4, APRIL 2012Application of Improved Median Filter on Image Processing Rong Zhu School Of Computer Science, Qufu Normal University, Rizhao, Shandong 276826, China zhurongsd@126.com

[4] International Journal of Advances in Engineering Researchhttp://www.ijaer.com/ (IJAER) 2011, Vol. No. 2, Issue No. VI, December ISSN: 2231-5152 COMPARATIVE STUDY OF EDGE DETECTION ALGORITHMS ON THE REMOTE SENSING IMAGES USING MATLAB Harshlata Vishwakarma1,S.K.Katiyar2

[5] H. Cheng and X. Li, "Partial Encryption of Compressed Images and Video," IEEE Transactions on Signal Processing, 48(8), 2000, pp. 2439-2451.