ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A NOVEL CRYPTOGRAPHY APPROACH BASED ON GENETIC ALGORITHM

Prasenjit Kumar Das*, Pradeep Kumar
M.Tech Scholar, Department Of CSE, Manipal University Jaipur, India
Asst. Professor, Department Of CSE, Manipal University Jaipur

ABSTRACT

Images play an important role in our lives. They are used in many applications. Therefore it is always necessary to affirm the integrity and confidentiality of the digital image that are being transmitted. With the progress in data exchange by electronic system, the need of information security has become a necessity. Moreover due to growth of multimedia applications, security becomes an important issue of communication and storage of images. Encryption and Decryption is used to securely transmit data in open networks. The principle goal of designing any encryption and decryption algorithm is to hide the original message and to send non readable text message to the receiver so that secret message communication can take place over the web. The strength of an algorithm depends on the difficulty of cracking the original message. And proper combination of both encryptions that provides confidentiality and hashing which leads to integrity of image transferred provide an ideal alternative.

In this paper, we provide a novel cryptographic approach based on genetic algorithm. Here, blowfish algorithm is used for image encryption and decryption and the Genetic algorithm is used to determine the key for the algorithm, which is an important aspect in any cryptographic algorithm. The approach is expected to provide high level of security to the image with less computational head to improve the image security, proper combination of encryption as well as authentication techniques always presents an ideal alternative.

KEYWORDS: Cryptography, Blowfish Algorithm, Genetic Algorithm, Hashing..

INTRODUCTION

Digital image play an important role in multimedia technology, it becomes more important for the user's to maintain privacy. Evidently, information security is an essential condition in the "modern life" . To protect our data against unauthorized access, from the time immemorial the first choice has always been to use cryptography. Digital images are exchanged over various types of networks. It is often true that a large part of this information is either confidential or private. Encryption is the preferred technique for protecting the transmitted data. There are various encryption systems to encrypt and decrypt image data, however, it can be argued that there is no single encryption algorithm which satisfies the different image types. With rapid growth in the arena of multimedia technology, since digital image has become an important medium of communication, extensive research is still a dynamic process in this field. The effectiveness of the protection through encryption depends on the algorithm applied and as well as on the quality of the 'key' used. If a 'key' is badly designed or haphazardly selected, obviously the protection fails to provide proper security and improper access can be gained on the secured information. The first algorithm in cryptographic system design is the algorithm to generate 'key'. It specifies the manner in which the 'key' is to be chosen. And to provide such security and privacy to the user, image encryption is very important to protect from any unauthorized user access. Image and video encryption have applications in various fields including internet communication, multimedia systems, medical imaging, Tele-medicine and military communication.

Figure 1: Image Encryption

Fig 1 shows a general image encryption process using any image encryption algorithm and resultant encrypted image. Color images are being transmitted and stored in large amount over the Internet and wireless networks, which take advantage of rapid

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

development in multimedia and network technologies. For long time image cryptography plays an important role in the field of security and it is battleground for the mathematicians and scientists, starting from Shannon's that dates back to 1949[1].Several cryptographic algorithms have been proposed up to now like AES, DES,RSA, IDEA etc. Cryptography is a science of information security. It is the art of protecting the data. It stores and transmits the information safely over the insecure medium like Internet by encoding image data into a form non recognizable format with the help of various encryption algorithms and only the intended user will be able to convert it into original text. The process which converts original data into the unreadable form is called encryption process. The encrypted data is called cipher text. The reverse of data encryption is data decryption which converts the cipher text back into the original text. Original text is also called plain text. Cryptology is a combination of Cryptography (encryption) and cryptanalysis (decryption).Cryptography algorithms are classified as: Symmetric (private key) algorithm and asymmetric (public key) algorithm. In symmetric algorithms uses only one key for encrypt the data and same for decrypt the data. Asymmetric key algorithm uses two keys, one is used to encrypt the data and other is used to decrypt the data. Length of Key has an important place in Symmetric key encryption. For the same algorithm, encryption using longer key is hard to cryptanalyze means more secure as compared to the one using shorter key. Asymmetric encryption techniques are almost one-thousand times slower than symmetric techniques as they require more computational processing power [2].

RELATED WORK

Image encryption schemes have been increasingly studied to meet the demand for real-time secure image transmission over the internet and through wireless networks [4]. The security of digital image has become more and more important due to rapid evolution of the internet in the digital world. From early 1990s, many researchers have inspected different solutions to image encryption. In 1992 a scheme for two-dimensional data encryption was presented [5]. It is pivoted on the principles and ideas reflected by the specification and development of an image pre-processing language called SCAN language. For the past years several image encryption algorithms have been proposed. These algorithms manipulate the pixels either by using some maps, like two-dimensional baker map or Chaotic Maps , two dimensional chaotic maps or by scattering them according to some chaotic function. An algorithm to hide the original image through simple permutation of the pixels location combined with Boolean XOR operation was proposed in 2003. In 2008 an extension to the Block-Based Image Encryption Algorithm (BBIE) scheme was introduced [6]. It works in combination with Blowfish Encryption algorithm. A new method image encryption algorithm based on hyper-chaos was proposed by Tiegang Gao and Zengqiang Chen ,that uses hyper chaos to encrypt the image .The method is divided into two parts in the first part, total shuffling of the image pixels is take place and in the second part, the shuffled image is encrypted using hyper chaos. Jiun-In Guo and Jui-Cheng Yen have presented an algorithm which was mirror like[7]. In this algorithm there were 7 steps. In the first, 1-D chaotic system is determined and its initial point x (0) and sets k = 0. A new image encryption algorithm based on hyper chaos, 2008 proposed by Tie gang Gao and Zengqiang Chen [8],uses hyper chaos to encrypt the image. The method is divided into two parts. In the first part, total shuffling of the image pixels take place in second part, the shuffling image is encrypted using the hyper chaos. The hyper chaos is used to change the gray values of the image pixels. In the process of farther development in the map based chaotic cipher, in 2006 a scheme was proposed, where an external secret key of 80-bit and two chaotic logistic maps are employed [9].

GENETIC ALGORITHM

A Genetic Algorithm is a searching technique used in computer science to find approximate solutions to optimization problems originated from the studies of cellular automata. Researchers have adopted GA as a solution to optimization in various fields in recent years. GA as solution to optimization problem started gaining popularity towards the end of the last century as used to solve optimization problems in construction. Its intrinsic parallelism facilitates the uses of distributed processing machines, like Distribution Network Planning . Problems which appear to be particularly appropriate for solution by GA include Scheduling and State Assignment Problem. GA approach to Solve Map Color Problem has been examined also. Researchers have shown interest in GA approach to solve scheduling types of problems, like job shop scheduling problem. It can be quite effective to combine GA with other optimization methods. Hybrid GA approach is also being adopted to derive higher quality solutions in relatively shorter time for hard combinatorial real world optimization problems such as Traveling

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

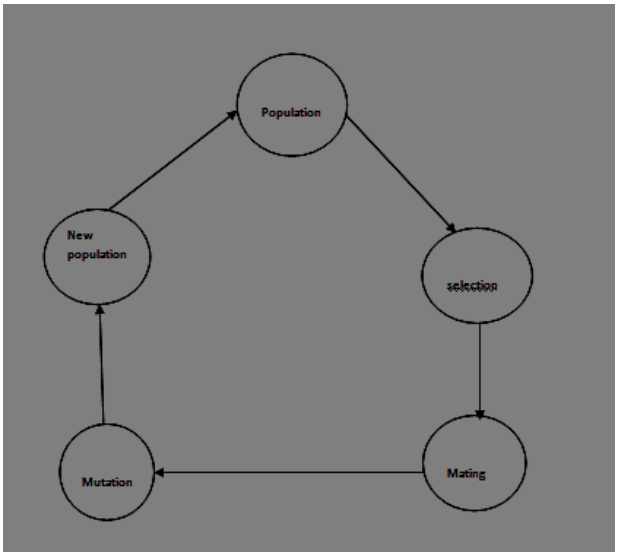
Salesman Problem (TSP). GA goes through three basic operation cycles: Selection, Crossover and Mutation, until stopping criteria is reached.

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

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 another or second chromosome.

Mutation: Mutation is used to maintain genetic diversity from one generation to the next generation of population. It is similar to biological mutation.

In the 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.



.Figure 2: Genetic algorithm

PROPOSED TECHNIQUE

As we know that in any Cryptographic Algorithm key plays an important role, for image encryption, the effectiveness of cipher largely depends on the quality of key. There is no denying the fact that Information Security is profusely endangered unless we are ever alert in respect of the perfect design and impartial selection of the 'key'. The algorithm that has been applied is described below.

1. Choose initial population of 100 chromosomes among 16! options randomly
2. Repeat until termination: (sufficient fitness achieved)
3. Repeat the process for 50 times (populate new generation of 100 offspring)

a. Select 10 randomly selected individuals from population of 100

b. Calculate the fitness of each individual in the population, that is calculated on the basis of the sum of total variation (length of displacement) of each gene

c. Select two chromosome with the best fitness value

d. Breed new generation through crossover and mutation among these two and give birth to two new offspring, and replace the old chromosome with new superior one in the population of the next generation

4. Select the best chromosome in terms of fitness from the final population. This selected chromosome is the 'key' in encryption process. Here, the best chromosome that will heavily affect correlation of the image pixels will be looked for. And so it considered a chromosome of size 16, where each element of the chromosome is an integer indicating the new position of the image pixel within a pixel block of size 16. A trial solution (chromosome) is represented as a string of 16 integers in a random arrangement from 16! Possible options. Each integer in the chromosome exists between 1 and 16. The k-th integer from the left of the chromosome is the new Position assigned to the pixel k, within that chromosome string. Pixels of the chromosome are considered as genes. The fitness function of the chromosomes is calculated on the basis of the sum of total variation (length of displacement) of each gene. In the process of mutation, two genes indicated by two randomly generated positions in a chromosome interchange their place. The objective is to maximize the fitness value so that when the chromosome is applied to shuffle the image pixels, the correlations among the pixels become the least. First break the image into square blocks of the size of chromosome and then applied the chromosome first horizontally and then vertically on each block.

RESULT ANALYSIS

The implementation of the work done on Intel core 2 Duo platforms. Operating system that will be used is Windows 8 and Fedora14. Blowfish encryption algorithm executed by using gcc compiler with readily available code under Linux. The simulation results of image encryption and authentication is done in Matlab 7.5 under windows platform.

The encryption algorithms that are applied on a gray image of size 240 x 240 pixels. And in order to

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

evaluate the impact of the number of blocks on the correlation, different cases have been tested. The initial processing using the pre-encryption technique on the original image generates a transformed image .Each case then produces three other output images; image using the Blowfish algorithm, image using the proposed algorithm (GA), and then image using Blowfish algorithm followed by the proposed algorithm (BlowGA). Here it is tried to analyze the application of GA for image security using a combination of block-based image transformation and encryption techniques.

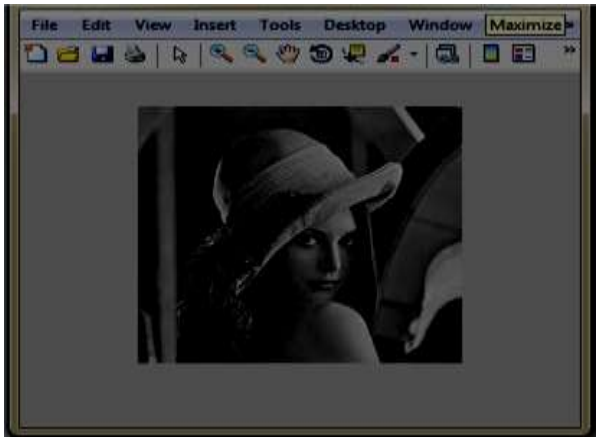


Figure 3: Input Image for Encryption

The input images that are used for the encryption is Lena which is shown above.

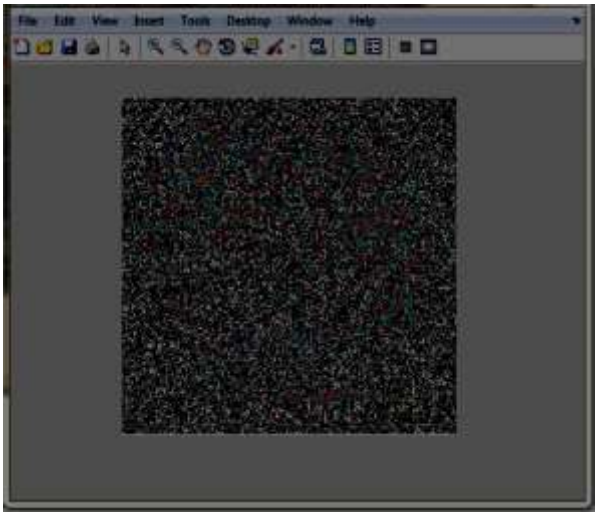


Figure 4: Cipher image Using Blowfish Algorithm

In the above figure the encrypted image is shown after the application of blowfish Encryption Algorithm.

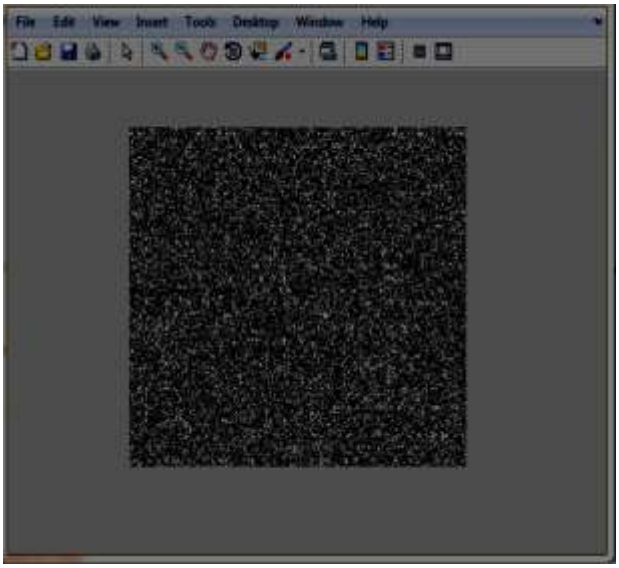


Figure 5: Ciphered image after using GA

The above figure shows the ciphered image after application of both Blowfish and Genetic Algorithm(GA).

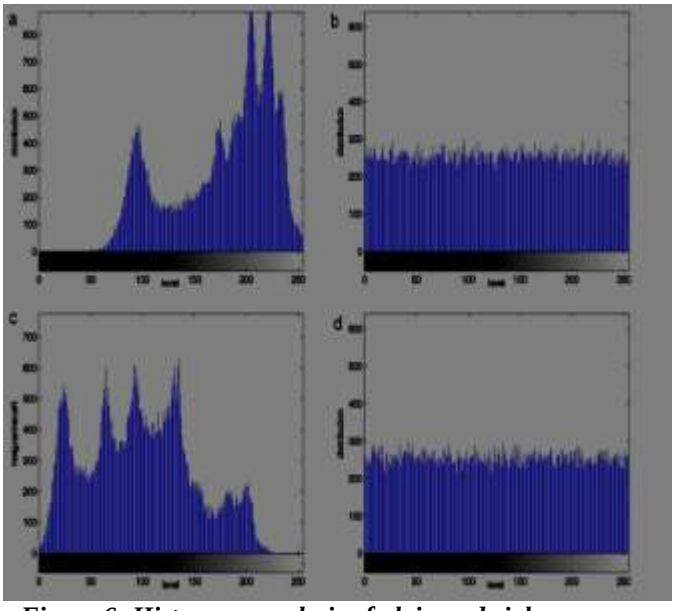


Figure 6: Histogram analysis of plain and cipher image

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

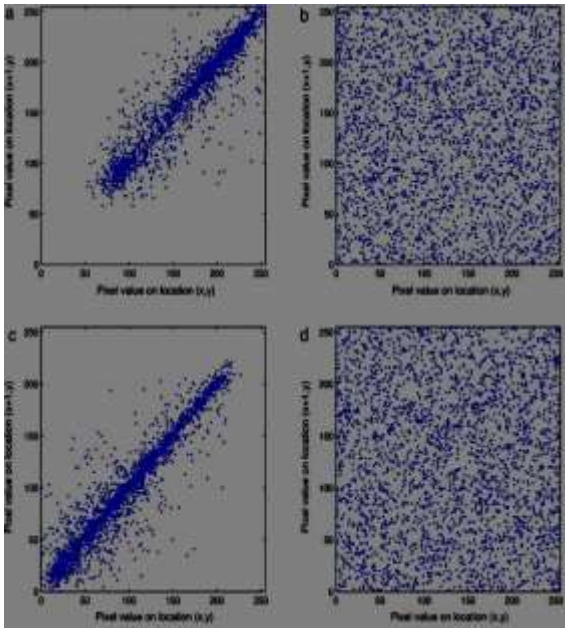


Figure 7: Correlation analysis of plain and cipher image

The above figure show the coefficient correlation of plain and cipher image .

CONCLUSION

Images are important data that always plays an important role in our daily lives. So image security is an always important issue. Everyday new image encryption techniques are evolving, and hence fast and secure image security techniques will always work with high rate of security. And after detail study of many image cryptographic algorithm it is found that the blowfish algorithm use here provide more secure encryption of image compared to any other convention image cryptography algorithms. It also does not have any known security weakness which makes it more suitable to use. The Genetic Algorithm also a searching technique used in computer science to find approximate solutions to optimization problems. Here it is used to generate the key for the encryption algorithm, thus making it an enhanced security mechanism. Since blowfish has not any known security week points so far, this makes it an excellent candidate to be considered as a standard encryption algorithm. Data encryption is a good means of security but it takes time for their operations to be performed which reduces the speed of data transfer and the capabilities of the network. When compared to many commonly used algorithms, the proposed algorithm resulted in the best performance; the lowest correlation and the highest entropy The results obtained for the correlation coefficients and entropies of the images proved the high efficiency of the this method. In the future work we can hashing function. Hash functions are used to check the integrity of the message to ensure that the message has not be altered, compromised or affected by virus.To achieve high level of image security, on a hybrid technique based on image encryption and authentication hashing is used. The technique consists of hash generation of the plain image. The generated hash will be embedded in the image and the entire image is encrypted using combination of blowfish and Genetic algorithm techniques.

REFERENCES

1. Shannon CE "Communication theory of secrecy system," Bell System Technical Journal, Volume 28, pp. 656 – 715, 1949.
2. Shubhangini p Nichat, S.S Sikchi , " Image Encryption Using Hybrid Genetic Algorithm" International Journal of Advanced Research in Computer Science and Software Engineering , Volume 1, Issue 3, January 2013.
3. Amitesh Singh Rajput, Nishcol Mishra, Sanjeev Sharma , "Towards the Growth Of Image Encryption and Authentication Schemes" , IEEE, International Conferences on Advances in Computing, Communications and Informatics,2013.
4. Rajinder kaur, Kanwalpreet Singh, "Comparative Analysis and Implementation of Image Encryption Algorithms", IJCSMC, Volume 2, Issue.4, pp. 170-176,April 2013.
5. N. Bourbakis, C. Alexopoulos, "Picture data encryption using Scan Patterns"; Pattern Recognition, Volume 25, no. 6, pp. 567-581, 1992
6. Syed Ali Naqi Gilani, M. Ajmal Bangash, "Enhanced block based colour image encryption Technique with confusion" in the Proceedings of the 12th IEEE International Multitopic Conference, pp. 200- 206, 2008.
7. Tiegang Gao and Zengqiang Chen, "A new image encryption algorithm based on hyper chaos", science direct, Volume 372, Issue 4, pp 394–400,21 January 2008.
8. Xiaopeng Weia, Ling Guoa, Qiang Zhanga, Jianxin Zhanga, Shiguo Lianb, "A novel color Image encryption algorithm based on DNA sequence operation andhyper-

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

chaotic system",Elsevier, The Journal of Systemsand Software pp 290–299,2012.
9. Jing Qiu , Ping Wang, " An Image Encryption and Authentication scheme", IEEE, Seventh International Conference on Computational Security and Intelligence,pages 784 – 787, 4 Dec. 2011.
10. Jing Qiu , Ping Wang, " An Image Encryption and Authentication scheme", IEEE, Seventh InternationalConference on Computational Security and Intelligence,pages 784 – 787, 4 Dec. 2011.