

Image Encryption: A New Approach Using Genetic Algorithm

Chinmoy Ghosh¹, Satyendra Nath Mandal²

Dept. of Computer Science and Engineering, Jalpaiguri Govt. Engg. College, Jalpaiguri, West Bengal, India¹

Dept. of Information Technology, Kalyani Govt. Engg. College, Kalyani, Nadia, West Bengal, India²

ABSTRACT: In this paper, a new approach has been applied for Image encryption using genetic algorithm. In genetic algorithm Crossover operation assembles existing genes and mutation operation produces new genes. Here, for each pair of pixels binary value of an image the crossover and mutation are applied to encrypt the image. Different test analysis like correlation, entropy test and histogram analysis is done for verification of the performance of the algorithm.

KEYWORDS: Crossover, Mutation, Most significant Bit, Image Encryption, Genetic algorithm.

I. INTRODUCTION

In the field of cryptography and network security Image encryption is an important research topic due to its huge application in digital communication. Here using some method the Plain text Image is converted to cipher text Image and send it through the communication channel to the receiver. So, the encryption algorithm should be robust enough to protect it from intruder. The author here proposed a new Image encryption method using Genetic algorithm without using any key.

Many authors has proposed different techniques of Image encryption using Genetic Algorithm. Rasul Enayatifar and Abdul Hanan Abdullah [1] in their paper at first they used chaotic function to encrypt a image, then they used genetic algorithm to get the best encrypted image. In their next paper [2] they used a hybrid technique composed of genetic algorithm and chaotic function. In 2012, Aarti Soni, Suyash Agrawal [3] Presented a method for key generation using genetic algorithm & then used AES for image encryption. Some authors has made a comparative study [4-9] on the different methods of Image encryption and reviewed them. The results of the showed that every method has advantages and disadvantages based on their techniques which are applied on images. Rasul Enayatifar and Abdul Hanan Abdullah in their 2014 paper [10] proposed a hybrid model of DNA masking , a genetic algorithm and a logistic map. Here DNA and logistic map functions used to create the number of initial DNA masks and then it applies GA to determine the best mask for encryption. More work on Image encryption by using Genetic algorithm and their performance are presented [11-14] and by other method[15-18].

II. PROPOSED METHOD

In this method Genetic algorithm is applied to each pair of pixel value of Image to be encrypt. At first convert each pixel of a pair to binary array and apply crossover operation on that pair since it is a inter-pixel operation. Here single point crossover technique is applied but the crossover changes every time based on the pair no. After crossover operation Mutation operation is implemented on the remaining bit stream of the each pixel of a particular pair as Mutation operation is Intra-pixel operation as mentioned before.

ALGORITHM:

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 13, October 2016

- Step 1: To read the Image in matrix form.
- Step 2: To take a pair of pixel from beginning and pixel and represents it by equivalent eight bit binary array.
- Step 3: Perform Crossover Operation.
- Step 4: Perform Mutation operation.
- Step 5: Convert each of the binary array to the decimal value taking *right-most bit as a 'Most significant bit'*.
- Step 6: Go to step 2 and repeat up to the last pair of pixel.
- Step 7: Result is an encrypted Image.

A. CROSSOVER

Suppose for an Image the pixels are B1, B2, B3,, Bn . To perform crossover operation from a pair of pixel from beginning and binarize them. The pair no will be used as crossover point (Single point).

- 1st pair of pixel (B1, B2) Crossover point CP= 1
- 2nd pair of pixel (B3, B4) Crossover point CP=2
- 3rd pair of pixel (B5, B6) Crossover point CP=3
-
- Nth pair of pixel Crossover point CP=N

Now binary bit stream from beginning to crossover point for each pixel of a pair (B_i, B_{i+1}) will exchange themselves to perform single point crossover operation. Let first two pixels are B1=116 and B2=170 and fourth pair B7=59 and B8=141.

B1 (binary)	0	1	1	1	0	1	0	0
B2 (binary)	1	0	1	0	1	0	1	1

↑
CP=1 since it is first pair

After crossover operation

B1	1	1	1	1	0	1	0	0
B2	0	0	1	0	1	0	1	1

Table-1

B7 (binary)	0	0	1	1	1	0	1	1
B8 (binary)	1	0	0	0	1	1	0	0

↑
CP=4 since it Fourth pair

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 13, October 2016

After crossover operation

B7	1	0	0	0	1	0	1	1
B8	0	0	1	1	1	1	0	0

Table-2


This operation will be applied to the rest of the pair of pixels. In each successive pair of pixels CP is incremented by one. When CP is equal 7 reset it to 1.

B. MUTATION

As mentioned mutation operation is an intra-pixel operation and after crossover it is applied to the rest of the bit of each pair of pixel based on the CP value. Here remaining untouched bit of each pixel is complemented by one's complement method. After crossover operation mutation operation is applied on (B1, B2) and (B7, B8) and the result is as follows.

Before Mutation

B1	1	1	1	1	0	1	0	0
B2	0	0	1	0	1	0	1	1


 Mutation region

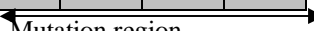
After Mutation

B1	1	0	0	0	1	0	1	1
B2	0	1	0	1	0	1	0	0

Table 3

Before Mutation

B7	1	0	0	0	1	0	1	1
B8	0	0	1	1	1	1	0	0


 Mutation region

After Mutation

B7	1	1	0	0	0	1	0	0
B8	0	0	1	1	0	0	1	1

Table 4

Finally, each of the binary arrays of each pair is converted to decimal by taking right-most bit as 'Most significant bit'. According to this new value of the First pair will be $(11010001_2, 00101010_2) = (209, 42)$. Similarly from Table 4 New value of fourth pair will be $(00100011_2, 11001100_2) = (35, 204)$

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 13, October 2016

III. EXPERIMENTAL ANALYSIS

A. VISUAL ANALYSIS

Experimental analysis shows good performance when it the algorithm has been applied on different types of images. The following figure indicates that the algorithm performs well.




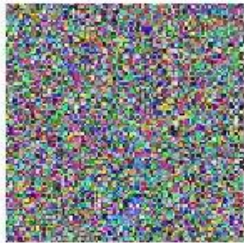


IMAGE NAME	IMAGE	
Train	<p data-bbox="587 792 730 824">Original Image</p> 	<p data-bbox="994 792 1137 824">Encrypted Image</p> 
Tusi	<p data-bbox="555 1099 699 1131">Original Image</p> 	<p data-bbox="962 1099 1106 1131">Encrypted Image</p> 
Lina	<p data-bbox="539 1406 683 1438">Original Image</p> 	<p data-bbox="962 1406 1106 1438">Encrypted Image</p> 

Table 5: Original and Encrypted Images

B. HISTOGRAM ANALYSIS

Histogram describes the statistical characteristics for a particular Image. Histogram analysis of the plain text image and encrypted image of Table 5 has been given below. It demonstrates that it is very hard for an intruder to guess the statistical nature of the image.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 13, October 2016

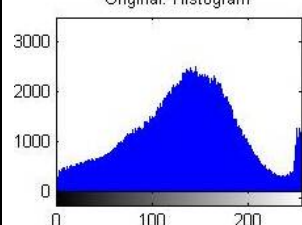
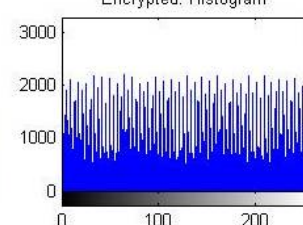
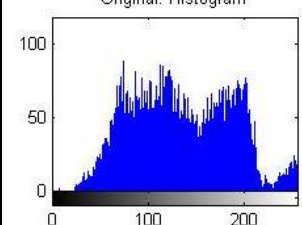
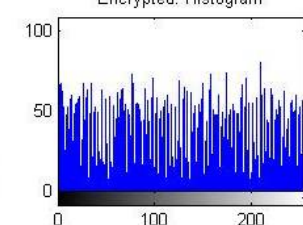
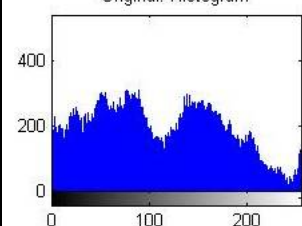
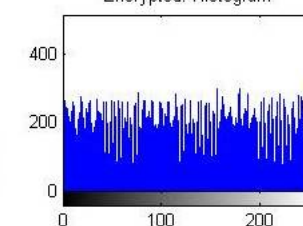
IMAGE NAME	HISTOGRAM	
Train	Original: Histogram 	Encrypted: Histogram 
Tusi	Original: Histogram 	Encrypted: Histogram 
Lina	Original: Histogram 	Encrypted: Histogram 

Table 6: Histogram Analysis

C. CORRELATION COEFFICIENT

The formula to find out Correlation coefficient of an image is

$$r = \frac{COV(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad \text{where}$$

$$COV(x, y) = \frac{1}{N} \sum_{i=1}^N (xi - E(x))(yi - E(y))$$

$$E(x) = \frac{1}{N} \sum_{i=1}^N xi$$

$$D(x) = \frac{1}{N} \sum_{i=1}^N (xi - E(x))^2$$

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 13, October 2016

Here x and y are grey-scale values of two adjacent pixels of an image. The following table shows the correlation coefficient of Original Image and Encrypted Image of Table 5. The RED component of the Particular Image has been considered to find out the correlation coefficient.

NAME	ORIGINAL IMAGE	ENCRYPTED IMAGE
Train	0.7928	0.0035
Tusi	0.9409	0.0232
Lina	0.9828	0.0570

Table 7: Correlation Coefficient

D. ENTROPY ANALYSIS

Entropy defines the statistical measure of randomness which can be used to characterize the texture of the input image. If entropy is low it can be compressed easily whereas high entropy image cannot be compressed as much as low entropy images. It defines by the equation

$$H(m) = \sum p(m_i) \log_2 \frac{1}{p(m_i)}$$

where $p(m_i)$ = Probability of pixel value m_i

The Following table defines the entropy corresponding to Table 5

NAME	ORIGINAL IMAGE	ENCRYPTED IMAGE
Train	7.7956	7.8669
Tusi	7.6402	7.8081
Lina	7.8558	7.9354

Table 8: Entropy

IV. CONCLUSION

The proposed encryption algorithm uses two reproduction operations Crossover and Mutation of Genetic Algorithm to provide good encryption. In this algorithm no key has been used, so the drawback of exchanging key between sender and receiver is eliminated here. Different analytical and visual indicators indicate that the proposed algorithm performs well and can be used effectively in image encryption.

REFERENCES

- [1] Rasul Enayatifar and Abdul Hanan Abdullah, "Image Security via Genetic Algorithm" IPCSIT vol.14 (2011)pp198-203
- [2] Abdul Hanan Abdullah, Rasul Enayatifar, Malrey Lee, "A hybrid genetic algorithm and chaotic function model for image encryption" ELSEVIER, Int. J. Electron. Commun. (AEÜ) 66 (2012)pp 806–816
- [3] Aarti Soni, Suyash Agrawal, "Using Genetic Algorithm for Symmetric key Generation in Image Encryption", IJAR CET, Volume 1, Issue 10, December 2012 pp 137-140
Rajinder Kaur¹, Er.Kanwalprit Singh², Image Encryption Techniques: A Selected Review, IOSR Journal of Computer Engineering (IOSR-JCE), 8727Volume 9, Issue 6, Mar. - Apr. 2013,pp 80-83
- [4] Bharti Ahuja, RashmiLodhi, Different Algorithms used in Image Encryption: A review, International Journal of Computer Science & Engineering Technology (IJCSET), Vol. 4 No. 07, Jul 2013, pp-861-864.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 13, October 2016

- [5] Niraj Kumar, Prof. Sanjay Agrawal, A Technical Review on Symmetric Key Cryptography Algorithm on Images, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 8, August 2013 ,pp1005-1009.
- [6] Komal D Patel, SonalBelani, Image Encryption Using Different Techniques: A Review,International Journal of Emerging Technology and Advanced Engineering ,Volume 1, Issue1, November 2011,pp 30-34.
- [7] Sunil Singh Rathode 1, ChallaSrikar Reddy 2, Sai Praveen Reddy, A Review Of Different Techniques Used In Image Encryption,International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 9, September – 2013, pp2315-2318
- [8] Swati Paliwal and Ravindra Gupta, A Review of Some Popular Encryption Techniques, International Journal of Advanced Research in Computer Science and Software Engineering , Volume 3, Issue 2, February 2013, pp147-149.
- [9] Rasul Enayatifar,AbdulHananAbdullah, IsmailFauziIsnin, “Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence” ELEVIER, Optics and Lasers in Engineering 56(2014) pp 83–93
- [10] Subhajit Das, Satyendra Nath Mandal, Nabin Ghoshal, “Diffusion and Encryption of Digital Image Using Genetic Algorithm” Springer, FICTA, 2014,Volume 327, 2015, pp 729-736
- [11] Dibag Shing, Pooja Rani, Rajesh Kumar, “ To design a Genetic for cryptography to enhance the security”, IJIET, Vol 2, Issue 2, April 2013, pp 380-385.
- [12] Swati Mishra, Siddharth Bali, Public Key Cryptography Using Genetic Algorithm”,IJRTE, ISSN: 2277-3878, Volume-2, Issue-2, May 2013, pp 150-154
- [13] Dr. Poornima G. Naik, “Asymmetric Key Encryption using Genetic algorithm”, IJLTET, Vol. 3 Issue 3 Jan, 2014, pp 118-128
- [14] Taranjit Kaur, Reecha Sharma, TJ-ACA: An Advanced Cryptographic Algorithm forColor Images using Ikeda Mapping,International Journal of Computer Trends and Technology, (IJCTT) - volume4 Issue5,–May 2013,pp 1295-1300.
- [15] Amnesh Goel, Nidhi Chandra, A Technique for Image Encryption with Combination of Pixel Rearrangement Scheme Based On Sorting Group-Wise Of RGB Values and ExplosiveInter-Pixel Displacement, IJ. Image, Graphics and Signal Processing, 2012, 2,pp16-22.
- [16] Somdip Dey, SD-EI: A Cryptographic Technique to Encrypt Images IEEE 2012, International Conference on Cyber security (CyberSec 2012), Malaysia, pp 28-32.
- [17] Somdip Dey, Amalgamation of Cyclic Bit Operation in SD-EI Image Encryption Method: An Advanced Version of SD-EI Method: SD-EI Ver-2, International Journal of Cyber-Security and Digital Forensics (IJCSDF) 1(3):pp2012, 221-225.
- [18] Rafael C. Gonzalez, R.E.Woods, S.L. Eddins, Digital Image Proceasing Using MATLAB, (New Delhi, Tata McGraw Hill Pvt. Ltd, 2010)
- [19] Behrouz A. Forouzan, D. Mukhopadhyay, Cryptography & Network Security, (New Delhi, Tata McGraw Hill Pvt. Ltd, 2013)
- [20] Atul Kahate, Cryptography and Network Security, (New Delhi, Tata McGraw Hill Pvt. Ltd, 2008)

BIOGRAPHY



Chinmoy Ghosh received his B.E (CSE) from North Bengal University and M.Tech (IT Courseware Engineering) from Jadavpur University. At present he is working as Assistant Professor in the Dept. of Computer Science and Engineering at Jalpaiguri Govt. Engg. College, Jalpaiguri, West Bengal. His field of research areas includes cryptography & network security, Genetic Algorithm etc.. He has 2 International Journal Paper in the area of Cryptography.



Satyendra Nath Mandal received his B.Tech & M.Tech degrees in Computer Science & Engineering from university of Calcutta, West Bengal, India. This author is AICTE Career Award for Young Teachers (CAYT) awarded from All India Council for Technical Education (AICTE) on 2010. He is now working as Assistant Professor in Department of Information Technology at Kalyani Govt. Engg. College, Kalyani, Nadia, West Bengal, India. His field of research areas includes cryptography & network Security, fuzzy logic, Artificial Neural Network, Genetic Algorithm etc. He has about 60 research papers in National and International conferences. His eleven research papers have been published in International journals.